UNIVERSIDADE DO VALE DO RIO DOS SINOS – UNISINOS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
NÍVEL MESTRADO

André Marcelo Knorst

ALINHAMENTO ESTRATÉGICO ENTRE OBJETIVOS DE NEGÓCIO E SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO (TI): UM ESTUDO NO SETOR DE AUTOMAÇÃO.

São Leopoldo
2010

André Marcelo Knorst

ALINHAMENTO ESTRATÉGICO ENTRE OBJETIVOS DE NEGÓCIO E SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO (TI): UM ESTUDO NO SETOR DE AUTOMAÇÃO.

Dissertação apresentada ao Programa de Pós-Graduação em Administração da Universidade do Vale do Rio dos Sinos como requisito parcial para obtenção do Título de Mestre em Administração.

Orientador: Prof. Dr. Adolfo Alberto Vanti

São Leopoldo

2010

K72a Knorst, André Marcelo.

Alinhamento estratégico entre os objetivos de negócio e segurança da informação no contexto da governança de TI : um estudo no setor de automação / André Marcelo Knorst. – 2009.

153 f. : il. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Administração, 2009.

“Orientador: Prof. Dr. Adolfo Alberto Vanti”.

Catalogação na publicação: Bibliotecário Flávio Nunes, CRB 10/1298

André Marcelo Knorst

ALINHAMENTO ESTRATÉGICO ENTRE OBJETIVOS DE NEGÓCIO E SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO (TI): UM ESTUDO NO SETOR DE AUTOMAÇÃO.

Dissertação apresentada à Universidade do Vale do Rio dos Sinos – Unisinos, como requisito parcial para obtenção do título de Mestre em Administração..

Aprovado em 26/03/2010

BANCA EXAMINADORA

_____

Prof. Dr. José Antônio Valle Antunes Junior - UNISINOS

_____

Prof. Dr. Marcos Antonio de Souza - UNISINOS

_____

Prof. Dr. João Luiz Becker - UFRGS

Prof. Dr. Adolfo Alberto Vanti

Visto e permitida a impressão

São Leopoldo,

Prof. Dra. Yeda Swirski de Souza

Coordenador Executivo PPG em Administração

AGRADECIMENTOS

Ao Orientador Prof. Dr. Adolfo Alberto Vanti, pela paciência e valiosas contribuições para esta dissertação.

Aos professores, colegas e colaboradores da equipe do PPGA/UNISINOS, pelo aprendizado e excelente ambiente acadêmico.

Aos colegas entrevistados, pelos importantes depoimentos e dados fornecidos.

À Coester Automação, por disponibilizar os dados para que esta pesquisa fosse realizada.

Aos meus pais, pelos valores, estímulo e bases para o meu crescimento.

Com especial carinho a Patrícia, pelo amor, companheirismo, apoio e proporcionar um ambiente para dedicação a este trabalho.

Aos meus filhos Pedro e Augusto, pela luz e carinho que serviram de inspiração.

RESUMO

A teoria traz como um problema e uma limitação dos modelos de gestão de TI presentes em grande parte das empresas a abordagem excessivamente operacional envolvendo o tema segurança da informação. Esta visão operacional não leva em consideração elementos estratégicos essenciais em busca das práticas mais adequadas no contexto do negócio. O objetivo desta dissertação é desenvolver e aplicar um *framework* para promover o alinhamento estratégico entre os objetivos de negócio, objetivos de TI e as práticas de segurança da informação. Estas práticas são avaliadas e analisadas no contexto da governança de TI e governança da segurança da informação. Para este fim, foi realizada a integração dos modelos do BSC x COBIT x ISO27002 com a aplicação prática em uma empresa de automação significativamente dependente de sistemas de informação. A integração destes modelos foi com base nos requisitos de segurança confidencialidade, integridade e disponibilidade resultando em um *framework* que possibilita abordar a segurança da informação em todos os níveis organizacionais (estratégico, tático e operacional) através aplicação de quatro (4) instrumentos de coleta de dados. Este *framework* também possibilita realizar uma análise dos dados a partir dos objetivos de TI para o negócio, mapeados a partir dos objetivos de negócio nas perspectivas do BSC.

Palavras-chave: Alinhamento estratégico, Segurança da Informação, Governança de TI, BSC, COBIT, ISO27002.

ABSTRACT

The theory brings up a problem and limitation of IT management models. The models found in most companies used an overly operational approach involving the issue of information security. This operational view does not take into consideration strategic elements essential to search for best practices in the business context. The objective of this thesis is to develop and implement a framework to promote the strategic alignment between business goals, IT goals and information security practices. These practices are assessed and analyzed in the context of IT governance and information security governance. To this end, the study integrated BSC x COBIT x ISO27002 models with practical application in an automation company with significant dependencies on information systems. The integration of these models was based on the security requirements of confidentiality, integrity and availability resulting in a framework that allows it to address information security at all organizational levels (strategic, tactical and operational) through application of four (4) data collection instruments. This framework also enables the performance of data analysis of the IT goals, mapped with the business goals of the BSC perspectives.

Keywords: *Strategic alignment, Information Security, IT Governance, BSC, COBIT, ISO27002.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

AI	Aquisição e Implementação
AQ	Aquisição, desenvolvimento e manutenção de sistemas de informação
BSC	*Balanced Scorecard*
C	Confidencialidade
CA	Controle de Acessos
CCSC	*Commercial Computer Security Centre*
CF	Conformidade
CGTFR	*Corporative Governance Task Force Report*
CMMI	*Capability Maturity Model Integration*
CMU	Universidade Carnegie Mellon
CVM	Comissão de Valores Mobiliários
COBIT	*Control Objectives for Information and related Technology*
D	Disponibilidade
ES	Entrega e Suporte
GA	Gestão de Ativos
GC	Gestão da continuidade do negócio
GI	Gestão de incidentes de segurança da informação
GO	Gerenciamento das operações e comunicações
GTI	Governança de Tecnologia da Informação
I	Integridade
IBGC	Instituto Brasileiro de Governança Corporativa
IEC	*International Electrotechnical Commission*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Standartization Organization*
ITSQC	*Information Technology Services Qualification Center*
ITGI	*Information Technology Governance Institute*
ITIL	*Information Technology Infrastructure Library*
MO	Monitoramento
OI	Organizando a segurança da informação

P&D	Pesquisa e Desenvolvimento
PMI	*Project Management Institute*
PL	Política de segurança da informação
PO	Planejamento e Organização
RH	Segurança em recursos humanos
SA	Segurança física e do ambiente
SEC	*Security and Exchange Comission*
SEI	*Software Engineering Institute*
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

A adoção dos sistemas de informação em maior escala tornou complexa a sua gestão. Frente a esta complexidade e com o objetivo de alinhar as ações de TI ao planejamento estratégico se torna apropriada a utilização de modelos de governança de TI (GTI). Para acompanhar as mudanças nos processos empresariais e principalmente no ambiente tecnológico da informação se faz necessário que estes modelos sejam revistos e evoluam constantemente.

A governança de TI tem por objetivo incorporar uma tecnologia da informação (T)I transparente com objetivos claros e bem definidos. Weill e Ross (2006) a definem como o conjunto de especificações para apoiar decisões e estimular comportamentos desejáveis na utilização da Tecnologia da Informação. Fatores como regulamentações, transparência, segurança, níveis de serviços, terceirização e mercado evidenciam a necessidade de planejar e implantar modelos de Governança de TI. Existem vários modelos de governança de TI com denominações conhecidas no mercado como COBIT, ITIL, ISO/IEC27001 e ISO/IEC27002 sendo que os mesmos apresentam focos distintos, por vezes excessivamente técnicos e individualizados, tanto em níveis organizacionais quanto em áreas específicas. Estas áreas estão relacionadas aos processos organizacionais, aos serviços terceirizados bem como à segurança da informação, foco principal deste estudo. Desta forma, se torna apropriada e necessária a integração entre eles para um alinhamento estratégico capaz de alcançar os diferentes níveis organizacionais e uma gestão mais eficaz.

Entre as questões mais significativas abordadas pela Governança de TI está a segurança da informação devido aos riscos que ela pode representar à organização. A segurança é um dos aspectos que qualificam a informação para tomada de decisão, porém usualmente o tema é tratado no nível operacional nas empresas. Dependendo do grau de importância da TI para o negócio a segurança da

informação deve ser considerada no mais alto nível gerencial (POSTHUMOS e SOLMS, 2004), no plano estratégico da empresa ou mesmo na atuação estratégica (FERNANDEZ e ABREU, 2008) e (ENTRUST, 2009). Já no marco referencial da matriz de Intensidade de Informação de Porter e Miller (1985) é possível analisar o quanto de informação está contido na cadeia de valor (processo) e a quantidade de informação que compõe o produto final conforme figura 1. Desta forma e dependendo da área de negócio, quanto mais intensa a informação para o negócio, maior atenção ela exige no seu gerenciamento em função do também aumento dos riscos de seu uso.

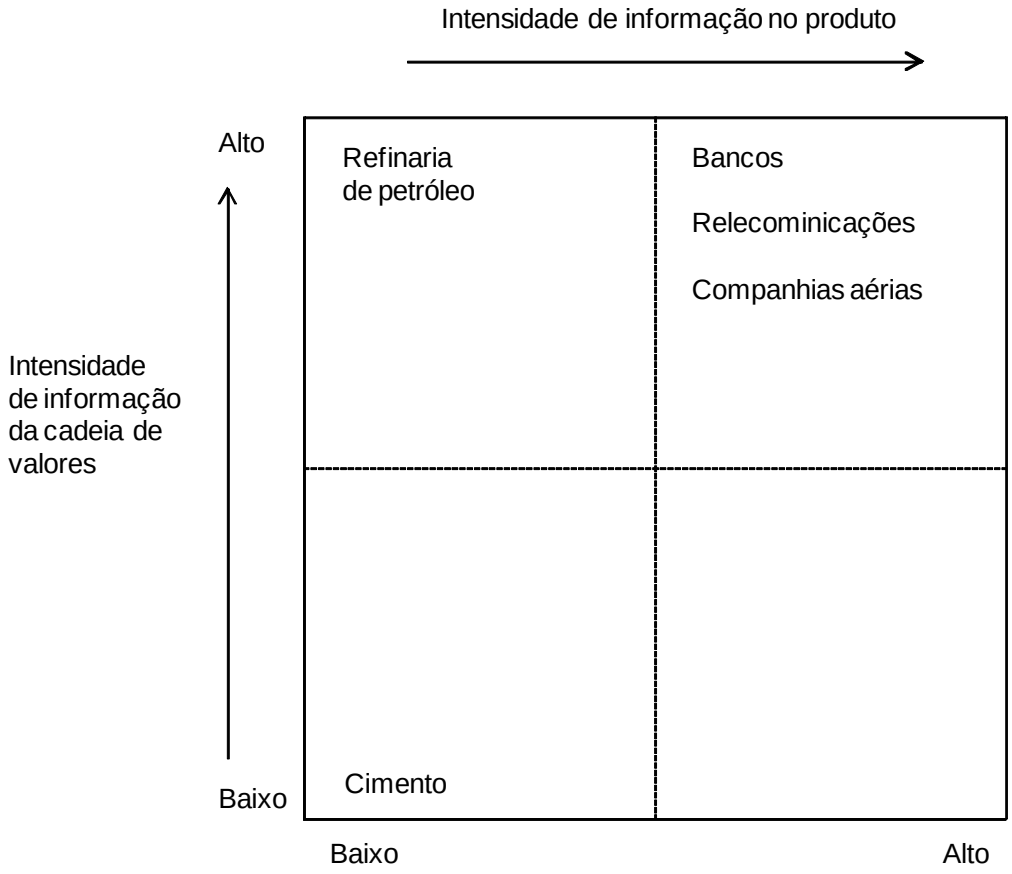


Figura 1: Matriz de intensidade da informação

Fonte: Porter e Miller (1985), pag. 6

A figura 1 indica a posição que empresas que atuam principalmente no mercado de serviços são altamente dependentes de sistemas de informação em seus processos e produtos. A empresa estudada neste trabalho atua no mercado de automação

industrial e se relaciona com esta abordagem, oferecendo produtos e serviços sustentados pela informação como um ativo altamente estratégico.

A segurança da informação possui requisitos básicos para sua manutenção, estes relacionados à confidencialidade, integridade e da disponibilidade (ITGI, 2009), (KWOK e LONGLEY, 1999), (TAYLOR e FRANCIS, 2007) e (SÊMOLA, 2003), (DIAS, 2000), (MOREIRA, 2001). Estes critérios não se restringem somente a sistemas digitais ou de armazenamento, mas a todos os aspectos de proteção de informações e dados. Atualmente as organizações são significativamente dependentes da sua infra-estrutura de TI, fato este associado às oportunidades, benefícios e riscos típicos desta área, faz com que ao se negligenciar os requisitos de segurança se coloque em risco todo o sistema de informação e potencialmente o próprio plano de negócio de uma organização.

A confidencialidade visa manter o sigilo e a privacidade da informação, enquanto que a integridade consiste em protegê-la contra qualquer tipo de alteração sem a autorização do autor, e a disponibilidade tem como objetivo proporcionar o acesso contínuo e interrupto da informação para quem a necessita. Na continuação estes critérios serão aprofundados na fundamentação teórica do trabalho. O tema segurança é tratado por alguns modelos de governança de TI e aprofundado pelas normas – ISO/IEC27001 e ISO/IEC27002. A ISO/IEC27001 propõe um Sistema Integrado de Gestão da Segurança, sendo possível a sua certificação. A ISO/IEC27002, utilizada neste trabalho, complementa a ISO/IEC27001 como um conjunto de boas práticas para a segurança da informação e é o ponto central do problema de pesquisa.

1.1 O problema de pesquisa

Considerando a importância estratégica da informação, a sua segurança e a necessidade de desenvolver modelos que expliquem ou demonstrem o alinhamento entre as políticas de segurança da informação e a estratégia de negócio, foi identificada a seguinte questão problema: Como desenvolver alinhamento estratégico entre objetivos de negócio, objetivos de TI e as práticas de segurança da informação?

Para tal, a segurança da informação foi estudada com base nos requisitos de confidencialidade, integridade e disponibilidade no setor de automação integrando os níveis estratégico, tático e operacional através da integração de BSC x COBIT x ISO/IEC27002. Estes três requisitos são exclusivos para a análise da segurança da informação, porém quando abordados ou mesmo analisados individualmente geram limitada utilidade. Então, cada um desses requisitos é estudado em um alcance que contempla e perpassa o nível operacional (norma de segurança ISO 27002), o nível tático (COBIT) e o nível estratégico (BSC), proporcionando sentido mais eficaz ao processo de governança de TI, ao alinhamento estratégico, bem como ao controle específico dos riscos relacionados à própria segurança da informação

1.2 Objetivos

1.2.1 Objetivo geral

O objetivo geral deste trabalho é desenvolver o alinhamento estratégico entre os objetivos de negócio, objetivos de TI e as práticas de segurança da informação. Estas são avaliadas e analisadas no contexto da governança de TI e segurança da informação em uma empresa do setor de automação.

1.2.2 Objetivos específicos

a) Identificar a relação entre os modelos de governança de TI com características estratégicas, táticas e operacionais envolvendo os requisitos de segurança da informação através do desenvolvimento de um *framework* para esta finalidade;
b) Identificar o grau de maturidade de governança de TI em relação aos processos operacionais no contexto do *framework* desenvolvido, envolvendo os requisitos de segurança da informação e sendo aplicado ao setor de automação;
c) Analisar as práticas de segurança para alinhar as mesmas aos requisitos de negócio e de TI adotadas pelo caso estudado e contemplando os três níveis organizacionais (estratégico, tático e operacional). Essa análise é

contemplada através da integração dos modelos BSC, COBIT e ISO 27002.

1.3 Justificativa

Os gastos em segurança da informação estão em contínuo crescimento para diminuir a vulnerabilidade dos sistemas de informações (ITGI, 2006). Segundo Fernandez e Abreu (2008), as empresas devem tratar a questão de segurança proporcionalmente à importância estratégica que a TI representa para o negócio. Tradicionalmente a segurança da informação em boa parte das empresas é tratada em nível operacional. Porém, atualmente devido alto nível de integração entre sistemas e a importância que a informação exerce, qualquer falha nesta relação pode representar um risco para o sistema de informações da empresa como um todo. Neste sentido garantir um ambiente seguro significa contribuir para a sustentabilidade do negócio.

Entre 2005 e 2008 os incidentes de segurança aumentaram em 320%, percentual este reportado ao CERT.br, conforme representação na Figura 2, o que também remete a importância do tema. No Brasil o CERT.br é mantido pelo NIC.br do Comitê Gestor da Internet Brasileira, o qual é responsável por receber, analisar e responder este tipo de incidentes envolvendo redes conectadas à Internet.

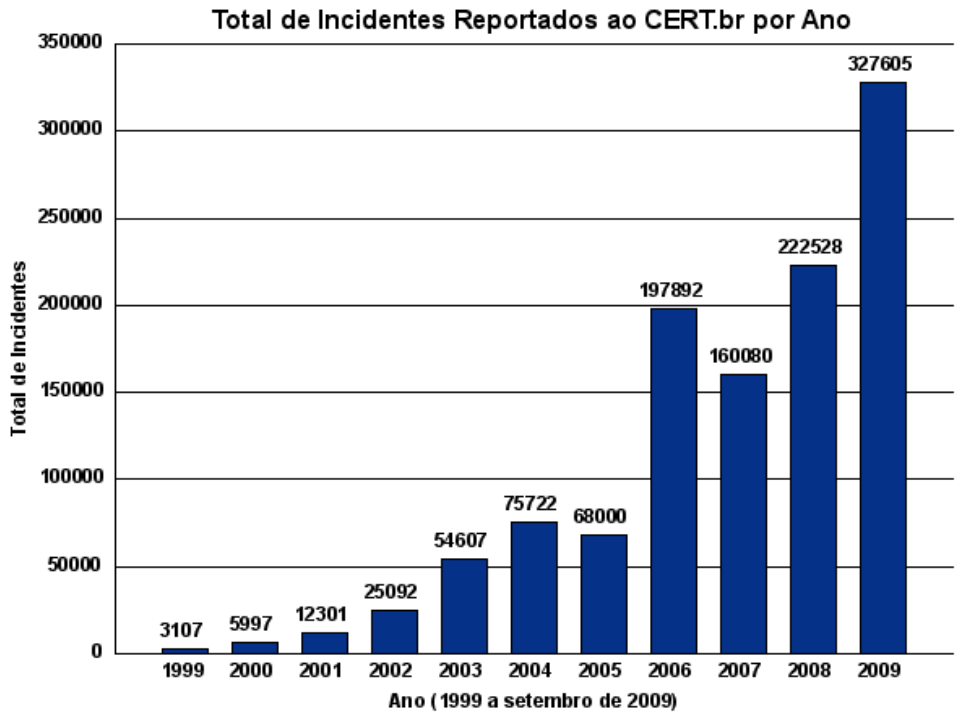


Figura 2: Total de incidentes relatados reportados ao CERT.br por ano
Fonte: CERT.br (2009)

Segundo o CERT.br (2009), este aumento se deve logicamente ao crescimento do uso da Internet. As conseqüências destes incidentes são a indisponibilidade dos sistemas, fraudes, furto de dados confidenciais, corrompimento de bases de dados, entre outras, podendo causar grandes transtornos em nível operacional e estratégico nas empresas.

Nos últimos anos foram realizadas iniciativas em nível acadêmico e empresarial para se estabelecer modelos de governança de TI. No entanto, esses modelos têm focos de atuação diferentes, apresentam limitações e estão em constante evolução para se adequar as contínuas mudanças no ambiente de TI. A abordagem estratégica do tema segurança tem sido preocupação contínua e remete para um conceito incremental e conhecido como governança de segurança da informação. Para Dlamini e outros (2009), as novas pesquisas no campo da segurança da Informação convergem na tentativa de diminuir o *gap* entre governança organizacional, governança de TI e implementações técnicas.

Para que as organizações obtenham sucesso no quesito segurança da informação, os gestores necessitam integrar o tema às operações de negócio tornando necessária a estruturação de um Modelo de Governança da Segurança da Informação como parte da Governança Corporativa. (ENTRUST, 2009). Allen e Westby (2007) analisaram a segurança da informação como um problema da empresa e não somente da área de TI.

A gestão da segurança da informação sustentada por TI deve ser integrada com todos os níveis da organização e alinhada com os objetivos estratégicos. Em um relatório do *Corporate Governance Task Force* é proposto que para proteger melhor a infra-estrutura de TI as organizações devem incorporar a questões de segurança computacional em suas ações de Governança Corporativa (CGTFR, 2004). O BSA *(Business Software Alliance)* sugere que os objetivos de controle contidos na ISO27002 devem ser incorporados e ampliados para o desenvolvimento de um modelo onde segurança da informação que não seja considerada apenas no plano tecnológico, mas parte integrante das melhores práticas corporativas num plano estratégico (BSA, 2003).

O presente trabalho contribui para o plano tecnológico e estratégico com a integração dos modelos BSC x COBIT x ISO/IEC27002, a partir dos princípios do BSC de tradução da estratégia até os termos operacionais de segurança da informação com o desenvolvimento e aplicação de um framework desenvolvido para tal finalidade. Na continuação é apresentado o referencial teórico contemplando os temas Governança Corporativa, Governança de TI, Alinhamento Estratégico e Segurança da Informação.

2 REFERENCIAL TEÓRICO

Nesta dissertação são integrados os modelos BSC x COBIT x ISO/IEC27002 com o objetivo de proporcionar o alinhamento estratégico da segurança da informação com o negócio, ou seja, gerar maior sentido estratégico para a mesma atuando em um contexto de governança de TI. Estes modelos têm focos de atuação em diferentes níveis organizacionais conforme Figura 3.

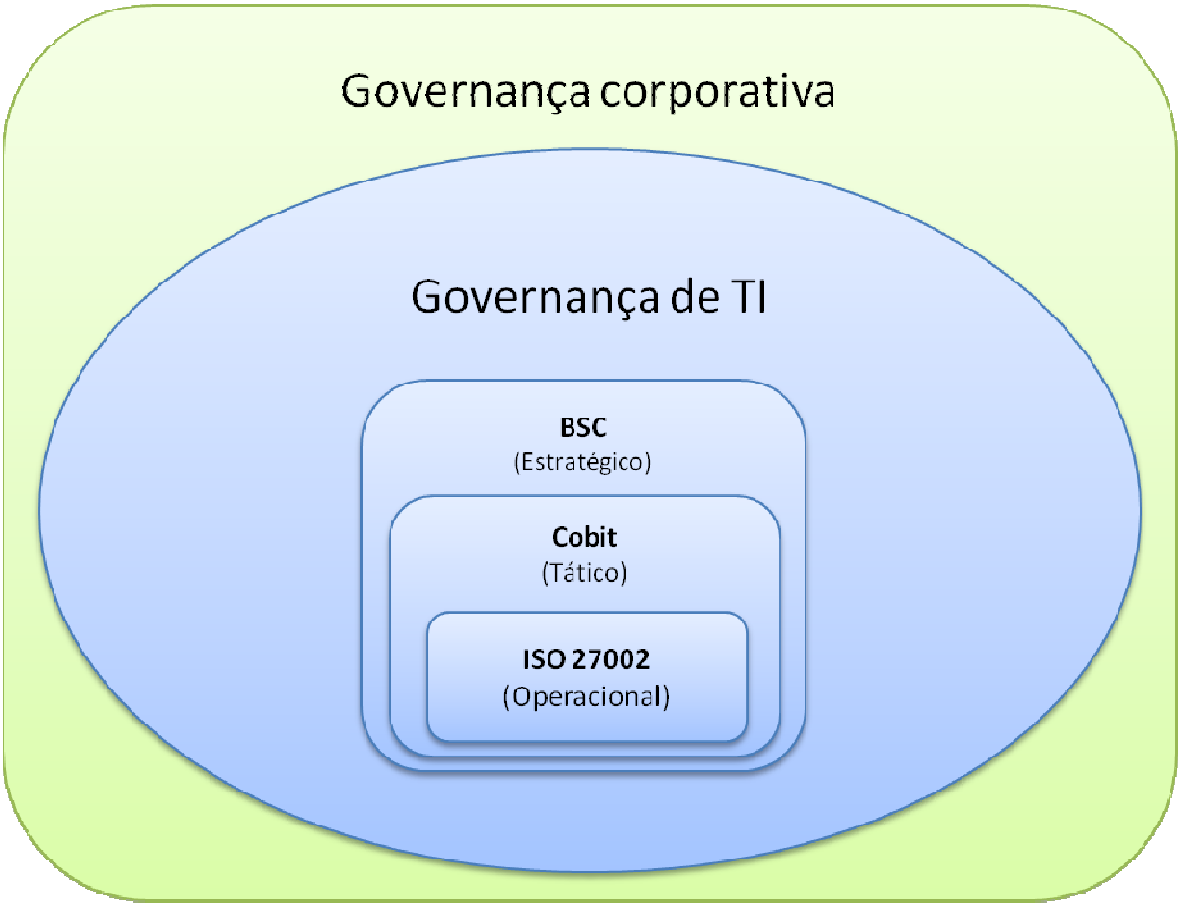


Figura 3 - Abrangência dos modelos de governança
Fonte: Elaborado pelo autor

A governança de TI é parte integrante da governança corporativa e seus modelos BSC, COBIT e ISO/IEC 27002 atuam em diversos níveis organizacionais com focos específicos, como mostrados na Figura 3. Essa atuação dos diferentes modelos é contemplada através de uma série de requisitos, por vezes extremamente operacionais, mas necessária para o alcance efetivo da segurança da informação e da conseqüente diminuição de riscos ao negócio.

2.1 Governança Corporativa (GC)

O termo Governança Corporativa foi criado no início da década de 1990 nos Estados Unidos e na Grã-Bretanha para definir as regras que regem o relacionamento nas organizações, dos interesses de acionistas controladores, acionistas minoritários e administradores. Foi criada nos Estados Unidos em 2002 a

Lei Sarbanes-Oxley (SARBANES-OXLEY ACT, 2002) devido aos eventos relacionados a escândalos financeiros como os das empresas *Enron* e *Worldcom.* A lei objetivou evitar a perda da confiança no mercado financeiro, proporcionar maior transparência às informações e propiciar auditorias preventivas pela *Security and Exchange Comission* (SEC).

No Brasil a Comissão de Valores Mobiliários (CVM) publicou a cartilha denominada “Cartilha Recomendações da CMV” sobre Governança Corporativa em junho de 2002 com orientações relativas a boas práticas de Governança Corporativa (CMV, 2002). Já o Instituto Brasileiro de Governança Corporativa (IBGC) publica desde 1999 e atualmente na 4ª edição o Código de Melhores Práticas de Governança Corporativa cujos princípios são:

Transparência: Os escalões executivos devem prestar as informações necessárias aos acionistas, as partes interessadas e a sociedade em geral.
Eqüidade: O tratamento deve ser justo e igualitário a todos os grupos minoritários, seja do capital ou das demais partes interessadas como colaboradores, clientes, fornecedores ou credores. São totalmente inaceitáveis quaisquer atitudes ou políticas discriminatórias, sob qualquer pretexto.
Prestação de contas: Todas as partes interessadas devem ter tratamento justo por parte dos agentes de Governança Corporativa, preferencialmente dentro dos padrões aceitos internacionalmente.
Responsabilidade Corporativa: É uma visão mais ampla da estratégia empresarial contemplando todos os relacionamentos com a comunidade em que a sociedade atua (IBGC, 2009).

A Governança de Tecnologia da Informação (GTI) é parte integrante da Governança Corporativa (GC) e tem sido objeto de estudo de acadêmicos e profissionais de TI com o objetivo de desenvolver teorias e melhores práticas mais ajustadas ao processo de gestão e ao desenvolvimento de modelos de negócio mais complexos. Neste trabalho são contemplados os modelos de Governança de TI, BSC, COBIT e ISO/IEC27002 e com essa integração destes modelos através de desenvolvimento e aplicação de *framework* específico, foi possível proporcionar uma visão mais ampla da segurança da informação possibilitando uma análise mais

completa da mesma no ambiente organizacional, bem como o seu conseqüente alinhamento estratégico

2.2 Governança de TI (GTI)

A GTI pode ser considerada a forma como as decisões são tomadas e responsabilidades direcionadas para encorajar um comportamento desejável no uso da TI (WEILL e ROSS, 2006). Outra definição diz que a GTI é a parte integrante da governança empresarial e é constituído pelos dirigentes e estruturas organizacionais e processos que asseguram que a organização mantém as práticas de TI para ampliar as estratégias e os objetivos organizacionais (ITGI, 2009). Também, pode ser considerada como a capacidade organizacional exercida pela Diretoria e Gerência Executiva para controlar a formulação e implantação da estratégia de TI e neste caminho, assegurar a fusão do negócio e TI (GREMBERGEN e HAES, 2004).

Uma pesquisa realizada por Weill e Ross (2006) revela que empresas com práticas de governança de TI têm resultados significativamente superiores sobre seus investimentos em tecnologia da informação se comparadas com empresas sem estas práticas. Segundo os autores estas empresas adotam as seguintes práticas em relação a TI:

- Definem as estratégias de negócio e o papel da TI em concretizá-las;
- Mensuram e gerenciam o que se gasta e o que se ganha com a TI;
- Atribuem responsabilidade pelas mudanças organizacionais necessárias para eficiência dos novos recursos de TI;
- Aprendem com cada implementação, tornando-se mais hábeis em compartilhar e reutilizar seus ativos de TI.

Foram desenvolvidos vários modelos tratando o tema GTI com o objetivo de alinhar os objetivos de negócio com os objetivos de TI, como evidenciado no estudo de Dahlberg e Lahdelma (2007) para a terceirização parcial e total deste tipo de serviço. Também o estudo desenvolvido por Fink e Ploder (2008) a partir das referências Tricker (1997); Norfolk (2005) e também a obra de Sheridan et al (2006), gerou um *framework* para análise da GTI aplicado a países de fala germânica.

Com base no perfil e objetivos de negócio, as empresas podem combinar diferentes modelos conforme a sua necessidade, porém em relação à segurança da informação, não há esta disponibilidade referenciada na literatura. Então, o *framework* de integração aqui desenvolvido e aplicado (apresentado no capítulo 5), permite essa combinação quando ocorrer alguma necessidade de envolver o tema de segurança da informação com Objetivos de TI e Objetivos de negócio.

2.3 Modelos de Governança de TI

Na seqüência são apresentados resumidamente alguns dos modelos de GTI mais conhecidos (COBIT, ITIL, eSCM-SP e eSCM-CL, ISO/IEC 27001 e ISO/IEC 27002 e BSC), os quais tendem a uma gestão mais eficaz dos recursos de TI.

O modelo *Control Objectives for Information and related Technology (COBIT)* é focado em controle e auditoria de Tecnologia da Informação. Este propõe que os recursos de TI sejam gerenciados por processo de TI para atingir suas próprias metas, as quais por sua vez estão estreitamente ligadas aos requisitos de negócio. Este modelo foi desenvolvido na década de 90 pelo *Information System Audit and Control Association* (ISACA), (ITGI, 2009) e está detalhado na seqüência, no item 2.4.2.

O modelo *Information Technology Infrastructure Library (ITIL)* reúne um conjunto de recomendações divididas em duas partes: Suporte de Serviços que inclui cinco disciplinas com uma função e acrescido da Entrega de Serviços com mais cinco disciplinas. O objetivo é descrever os processos necessários para gerenciar a infra-estrutura de TI de modo a garantir os níveis de serviços acordados com os clientes internos e externos (MANSUR, 2007). Este modelo foi criado no final dos anos 80 pela *Central Computing and Telecommunications Agency* para o governo britânico.

O modelo *Capability Maturity Model Integration* (CMMI) é aplicado principalmente na gestão de desenvolvimento de software. Foi desenvolvido pelo *Software Engineering Institute* (SEI) da Universidade *Carnegie Mellon* (CMU) em *Pittsburgh* (EUA) por um grupo de profissionais de *software*, sendo que a primeira

versão foi lançada em 1991. O modelo propõe cinco níveis de maturidade dos processos da empresa: Inicial, Repetitivo, Definido, Gerenciável e Otimizado. Estes níveis em escala crescente permitem uma visão evolutiva da maturidade em seus processos organizacionais auxiliando na definição de prioridades e melhorias dos seus processos (SEI, 2008).

O modelo *eSCM-SP/eSCM-CL* foi especificamente desenvolvido para terceirização de serviços de TI, o denominado *outsourcing*. O eSCM é coordenado pelo *Information Technology Services Qualification Center* (ITSQC) e é um modelo para a avaliação e certificação da capacidade em serviços de terceirização de TI com três principais objetivos: 1) Oferecer aos provedores de serviços diretrizes que os auxiliam na melhoria de sua capacidade em uma terceirização; 2) Fornecer aos clientes meios e objetivos para avaliar a capacidade dos provedores de serviços; e 3) Fornecer um padrão que provedores de serviços possam utilizar quando quiserem se diferenciar dos concorrentes, (ITSQC, 2009).

As normas *ISO/IEC 27001 e ISO/IEC 27002* relativa à segurança da informação são de origem britânica. *A British Standard (BS)* 7799 deu origem a ISO/IEC17799, tendo o nome atualizado para ISO/IEC27002 em 2007 e desenvolvida no *Commercial Computer Security Centre (CCSC)* do departamento de indústria e comércio. O CCSC foi criado considerando a atuação em apoiar os fornecedores de produtos de segurança em TI a partir de um conjunto de critérios de avaliação e certificação, bem como para auxiliar os usuários de TI através de um conjunto de código de práticas do usuário.

Os objetivos da norma ISO/IEC27001 é prover um modelo para estabelecer, implantar, operar, monitorar, rever e melhorar um Sistema de Segurança da Informação. A ISO/IEC27002 complementa a ISO/IEC27001 estabelecendo um conjunto de práticas para manter e melhorar a gestão da segurança da informação em uma organização (FERNANDES e ABREU, 2008). Este modelo está detalhado na seqüência, item 2.4.4.

O modelo *Balanced Scorecard (BSC)* foi desenvolvido no início da década de 90 por Kaplan e Norton e constitui um modelo de gestão estratégica baseado em

indicadores financeiros e não-financeiros vinculados à estratégia organizacional e divididos em quatro perspectivas de avaliação: Financeira, Clientes, Processos Internos e Aprendizado e Crescimento.

Posteriormente os autores ampliaram a abordagem de indicadores, incorporando os ativos intangíveis e um mapa estratégico que representa o contexto onde a TI está inserida. A função corporativa pode ser traduzida em um conjunto de prioridades de causa e efeito comunicados a toda organização. Ainda segundo os autores, são princípios das organizações direcionadas para a estratégia: 1) traduzir a estratégia em termos operacionais; 2) alinhar a organização à estratégia; 3) transformar a estratégia em tarefa de todos; 4) converter a estratégia em processo contínuo; e 5) mobilizar a mudança por meio da liderança executiva (KAPLAN e NORTON, 1997). Este modelo é detalhado na seqüência no item 2.4.1.

O BSC é um modelo de alinhamento estratégico que contribui na promoção da governança de TI. Ele é usado neste trabalho com o propósito de realizar uma abordagem e análise ampla do alinhamento entre estratégia de TI e estratégia de negócio.

2.4 Alinhamento Estratégico de Tecnologia da Informação

Um dos principais objetivos da área de TI e da própria GTI é buscar o alinhamento estratégico entre a mesma e a estratégia organizacional, pois estar alinhado estrategicamente significa desenvolver ações que apóiem os objetivos e requisitos do negócio. A dificuldade do alinhamento estratégico nas operações de TI aumenta na medida em que as estratégias empresariais sofrem mudanças. Um dos principais motivos disto é que a TI atua tanto em nível estratégico quanto operacional resultando num quadro complexo de arquiteturas e infra-estruturas em diferentes camadas e níveis organizacionais (FERNANDES e ABREU, 2008).

A TI gera respostas rápidas em um ambiente dinâmico e é capaz de sustentar a estratégia do negócio com eficiência nos processos organizacionais e até mesmo reconfigurar a estratégia da empresa, tornando-se assim mais eficaz como no exemplo da criação de um modelo de negócios baseado em *e-business.* Para isso, o

seu alinhamento deve ser bidirecional, da estratégia de negócio para estratégia de TI e vice versa, conforme Figura 3, (HENDERSON e VENKATRAMAN, 1993).

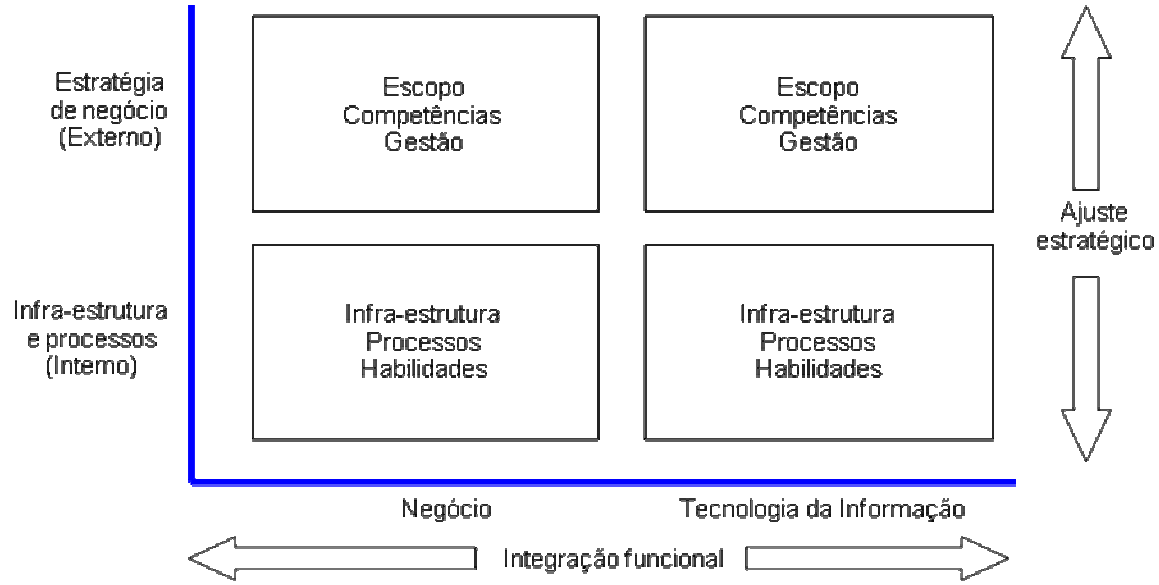


Figura 4: Modelo de Alinhamento Estratégico

Fonte: Adaptado de Henderson & Venkatraman (1993, p.476)

A Figura 4 demonstra a integração estratégica de negócio e de TI. Esta integração não é imediata tendo em vista as inúmeras mudanças organizacionais decorrentes de projetos de TI os quais envolvem questões de poder, política, cultura, entre outras. A integração funcional trata da ligação entre a infra-estrutura e processos organizacionais e infra-estrutura e processos de TI.

Com esta proposta, a GTI propõe dar sustentabilidade ao negócio através do alinhamento estratégico. Para isso a TI deve ter um posicionamento bem definido e consistente em relação às demais áreas da organização, alinhar e priorizar as iniciativas de TI através da iteração com os demais processos organizacionais (FERNANDES e ABREU, 2008). A TI é vista como um dos recursos corporativos que pode apoiar as estratégias em nível operacional, ou direcionar as estratégias em um nível mais alto, apoiando o negócio na obtenção de vantagem competitiva (KAPLAN e NORTON, 1997). Para apoiar os negócios a TI deve apoiar as suas atividades no plano estratégico do negócio, justificando assim seus projetos (MANSUR, 2007).

O ITGI (2009) propõe o alinhamento da TI com a estratégia da organização através de um conjunto de objetivos genéricos de negócio para a TI nas perspectivas do BSC. Estes objetivos por sua vez estão vinculados a objetivos genéricos de TI para o negócio relacionando-os com os processo do COBIT conforme Quadros 1 e 2 na páginas 35 e 36. Para complementar a abordagem de segurança da informação, estes quadros são ampliados nos Quadros 3, 4 e 5 nas páginas 39, 42 e 51, os quais contemplam os requisitos de segurança.

2.4.1 Balanced Scorecard (BSC)

O BSC é um modelo de alinhamento estratégico que contribui para promoção da governança de TI através da mensuração de resultados baseado na estratégia organizacional com o objetivo de estabelecer um equilíbrio entre os indicadores para medição e desempenho nas perspectivas; Financeira, Cliente, Processos Internos e Aprendizado e Crescimento. O modelo inicia com a missão da organização, visão de futuro, definição da estratégia e estabelecimento de ações para apoiar a estratégia. Uma vez definida a visão e o foco estratégico da organização define-se um mapa estratégico que conduz as diretrizes do negócio através de relações causa efeito. Este modelo busca assegurar o alinhamento entre as atividades internas da organização e a proposição de valor para o cliente (KAPLAN e NORTON, 1997).

A função corporativa pode ser traduzida em um conjunto de prioridades em um *scorecard* a ser comunicado para toda a organização deixando clara a missão de todas as unidades dentro da estrutura corporativa. O BSC capacita as empresas a focarem e alinharem suas equipes executivas, unidades de negócio, recursos humanos, TI e recursos financeiros na estratégia organizacional com base em cinco princípios característicos de organizações direcionadas para estratégia:

1. **Traduzir a estratégia em termos operacionais:** a estratégia precisa ser comunicada para todos os níveis da organização, para que possa ser compreendida e operacionalizada por meio da ferramenta dos "mapas estratégicos", que, juntamente com os *balanced scorecards*, indicam como os ativos intangíveis se transformam em resultados financeiros tangíveis;

2. **Alinhar a organização à estratégia:** as organizações focadas na estratégia superam as barreiras relacionadas às diferenças de conhecimentos, linguagem e cultura conectando-se à estratégia por meio de temas e objetivos comuns que permeiam seus *scorecards*;
3. **Transformar a estratégia em tarefa de todos:** os colaboradores devem ser treinados para compreender a estratégia a fim de que possam contribuir a partir das atividades que desenvolvem no cotidiano. Para isso necessitam aprender sobre os componentes estratégicos críticos; segmentação dos clientes, custeio variável e *marketing* de banco de dados. Finalmente é importante vincular ao *balanced scorecard* à remuneração por incentivos, o que aumenta o interesse dos empregados;
4. **Converter a estratégia em processo contínuo:** ao invés de utilizar o orçamento e o plano operacional como ferramenta principal de trabalho na execução de suas atividades gerenciais, deve existir a integração do gerenciamento tático e estratégico em um único processo com a utilização de dois tipos de orçamento: estratégico e operacional. A separação é importante para resguardar as iniciativas de longo prazo das atividades de curto prazo no que tange a resultados financeiros.
5. **Mobilizar a mudança por meio da liderança executiva:** o senso de propriedade e o envolvimento ativo da equipe executiva da organização são fundamentais para que ocorram as mudanças e para que a estratégia seja implementada. Após a mobilização da organização os executivos devem estabelecer um processo de governança para orientar a transição desenvolvendo-se ao longo do tempo um novo sistema gerencial estratégico que institucionaliza os novos valores culturais

A Figura 5 apresenta o modelo proposto pelos autores para tradução da estratégia em termos operacionais.

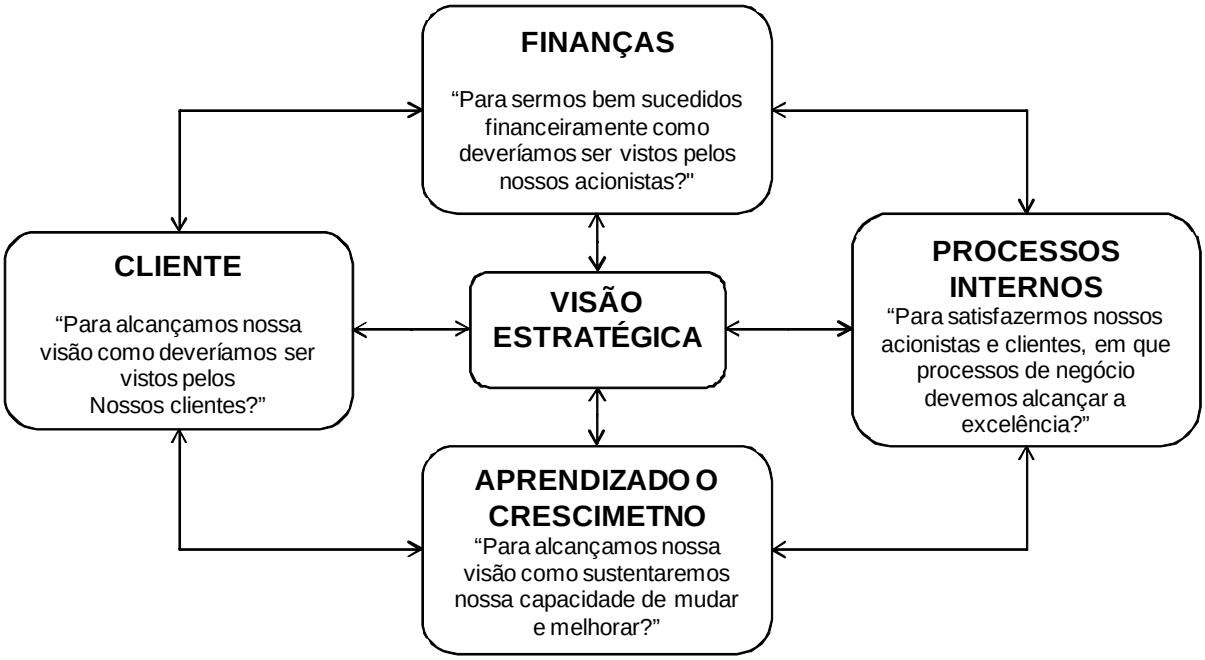


Figura 5: O Balanced Scorecard

Fonte: Kaplan e Norton (1997, p.10)

Os autores esclarecem que cada uma das perspectivas deve estar acompanhada de Objetivos, Indicadores, Metas e Iniciativas. Em cada uma das perspectivas há uma questão primordial a ser respondida e que norteará a criação das iniciativas e demais componentes correlacionados.

O conceito do BSC pode ser aplicado aos processos de TI, desde que siga as perspectivas propostas por esta metodologia e que os objetivos estejam alinhados com a estratégia organizacional, orientação para usuários, excelência operacional e orientação para o futuro (ITGI, 2009). Neste sentido, analisar as práticas envolvendo aspectos de segurança permite avançar na sua compreensão frente à estratégia empresarial.

2.4.2 Control Objectives for Information and related Technology (COBIT)

O COBIT teve sua primeira versão em publicada em 1996 e é mantido atualmente pela *Information Systems Audit and Control Association*. Inicialmente era uma simples orientação para governança de TI e logo foram incorporadas métricas e melhoria de processos, se transformando de fato em um modelo de GTI. O objetivo do COBIT é identificar um relacionamento entre os requisitos de negócio, os

recursos e os processos de TI procurando alinhamento de forma a atender as necessidades da empresa.

Conforme ITGI (2009), o COBIT se relaciona por meio de um conjunto de documentos que caracterizam as melhores práticas e processos de negócios relativos a TI. O modelo divide a função de TI em 34 processos organizados em 4 domínios: Planejamento e Organização (PO), Aquisição e Implementação (AI), Entrega e Suporte (ES) e Monitoramento (MO). A gestão destes processos possibilita a organização a viabilizar a adequação para as necessidades de controle dos ativos do setor. Cada domínio é composto por um conjunto de processos e estes são compostos por atividades. A correta execução destas atividades permite que o processo seja executado e a necessidade do domínio de atingir os objetivos seja alcançada.

A Figura 6 mostra os quatro domínios do COBIT versão 4.1 e os processos que compõem o modelo e o fluxo de interação entre os domínios.

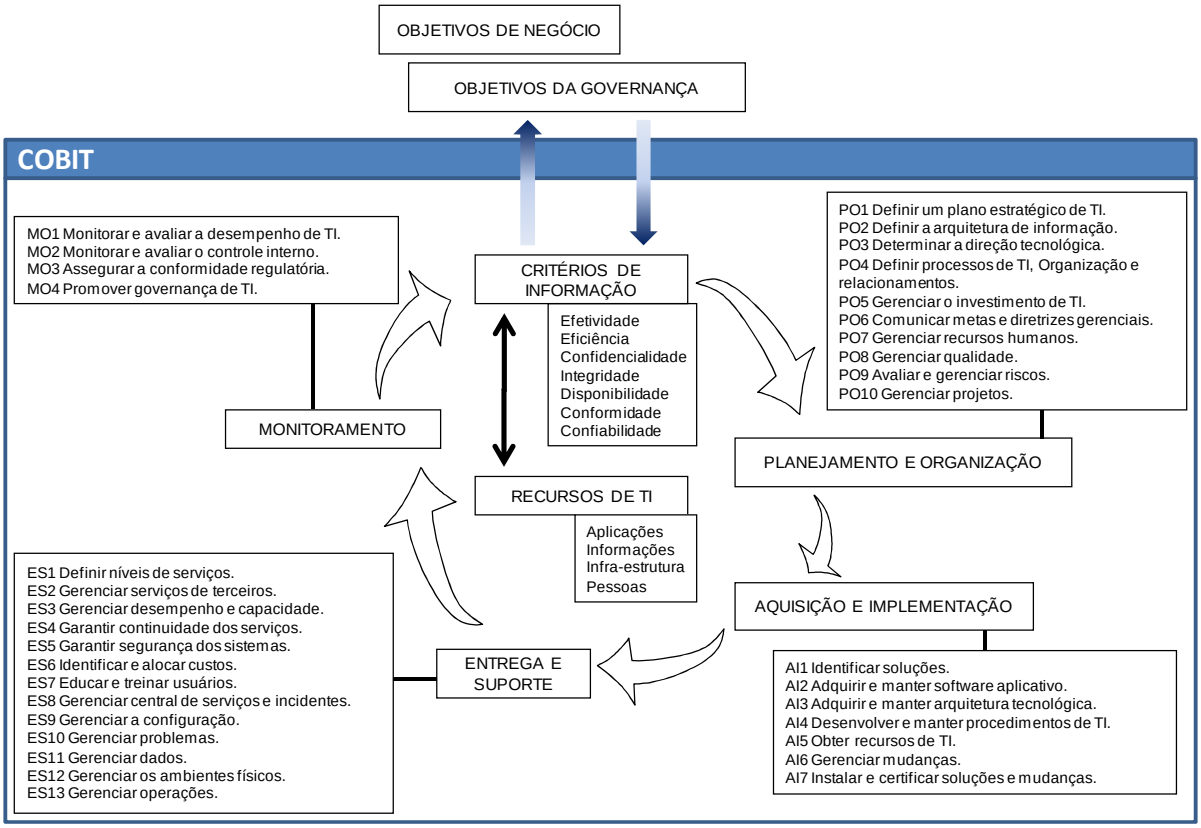


Figura 6: Visão geral do modelo COBIT 4.1
Fonte: ITGI (2009)

Estes 4 domínios estão assim definidos:

Planejamento e Organização (PO): Este domínio descreve o uso de informação e tecnologia para o cumprimento dos objetivos e metas. Ele também propõe que a forma organizacional e a infra-estrutura da TI devem ser consideradas para que se alcance resultados ótimos e para que se gerem benefícios do seu uso.

Aquisição e Implementação (AI): Este domínio atende os requisitos de TI referente à aquisição de tecnologia e implementação nos processos de negócios da organização. Ele também considera o desenvolvimento do plano de manutenção que a empresa adota para prolongar a vida dos sistemas de TI e seus componentes.

Entrega e Suporte (ES): Este atende os aspectos de entrega de tecnologia da informação. Abrange a execução de aplicações dentro do sistema de TI, seus resultados e o suporte dos processos que habilitam a execução de forma eficiente e efetiva. Os processos de suporte também incluem questões de segurança e treinamento.

Monitoramento (MO): O domínio de Monitorar apresenta as necessidades da organização de medir e avaliar se o atual sistema de TI atinge os objetivos para o qual ele foi estruturado. Ele também abrange as questões de estimativa independentemente da efetividade do sistema de TI e sua capacidade de atingir os objetivos de negócio, controlando os processos internos da companhia através de auditorias.

A visão dos domínios se dá em três dimensões. São elas: Processos de TI - processos organizados pelo modelo, Recursos de TI - recursos de TI que os processos utilizam, e Requisitos de Negócio – os quais constituem as informações relativas à qualidade e segurança dos ativos que geram dados para o modelo.

Organizado nessas três dimensões, tem sua representação na Figura 7 a seguir:

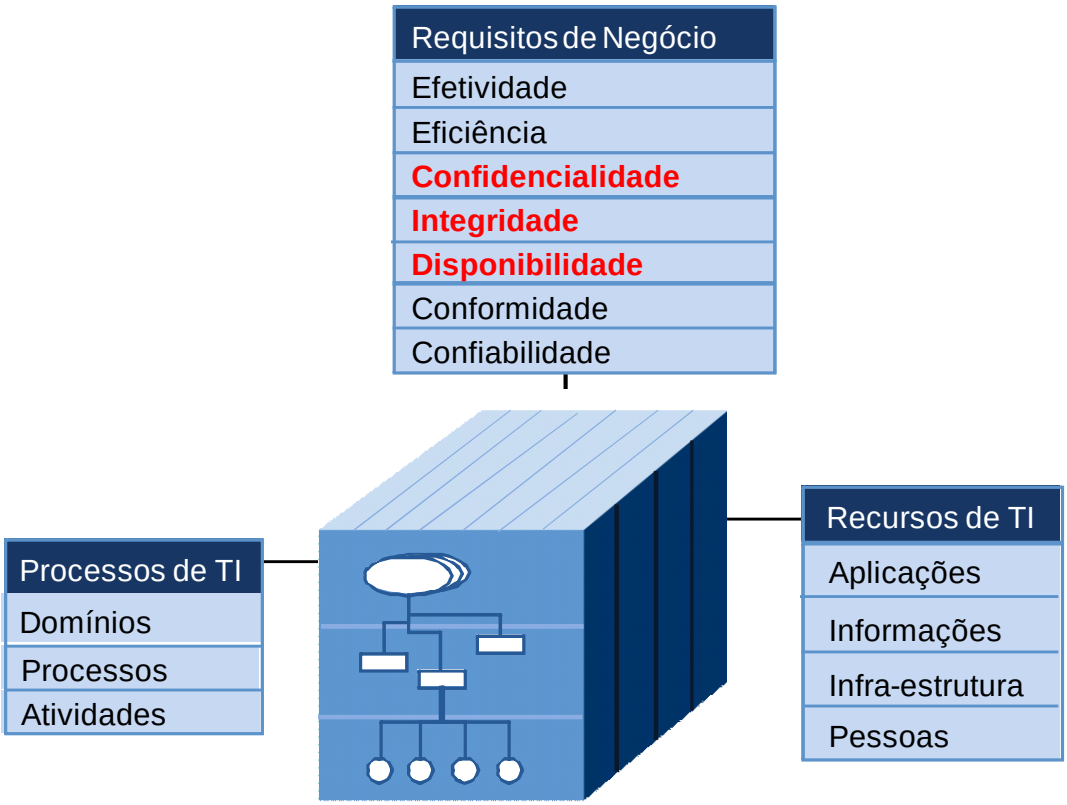


Figura 7: Cubo do Modelo COBIT 4.1

Fonte: ITGI (2009)

Segundo este modelo os requisitos de negócio em relação à informação consistem em:

- **Efetividade:** informação precisa no prazo, na forma e no formato adequado;
- **Eficiência**: prover a informação da forma mais produtiva e econômica;
- **Confidencialidade:** proteção da informação a acessos não autorizados;
- **Integridade:** informação completa, acurada e validada de acordo com os valores e expectativas do negócio;
- **Disponibilidade:** informação disponível para o negócio quando requerida, assim como a salvaguarda dos recursos necessários e capacidades associadas;
- **Conformidade:** cumprimento das leis, contratos e regulamentações;
- **Confiabilidade:** fornecimento de informações precisas e apropriadas aos gestores para tomada de decisão e para prestação de contas sobre finanças e conformidade.

Os requisitos de negócio em relação à segurança da informação descritos nesta dissertação são os de confidencialidade, integridade e disponibilidade, pois estes estão relacionados aos requisitos básicos de segurança.

Os recursos de TI são os tecnológicos, competências técnicas, infra-estrutura física e lógica dos equipamentos e informações geradas a partir das transações de negócios. Esta perspectiva associa-se aos processos de TI ampliados dento do modelo COBIT em 4 domínios. Estes domínios se subdividem em um conjunto de processos que contemplam um grupo de atividades que ao serem executadas remetem a implantação dos controles propostos pelo modelo.

Para verificar o grau de maturidade da empresa em relação aos modelos de governança, podem ser aplicados modelos de verificação de maturidade. Estes modelos são usados para o controle dos processos de TI e fornecem um método eficiente para classificar o estágio da organização de TI originado do CMM.

Esta abordagem CMM é derivada do modelo de maturidade para desenvolvimento de software, *Capability Maturity Model Integration* (CMMI), proposto pelo *Software Engineering Institute* (SEI, 2008). Segundo o modelo de verificação de maturidade *Capability Maturity Model Integration* (CMMI), a governança de TI e seus processos com o objetivo de agregar valor ao negócio através do balanceamento do risco e retorno do investimento são classificados da seguinte forma:

0 - Inexistente: Neste nível não há processos reconhecidos. A organização não tem conhecimento sobre as implicações que a falta do processo pode gerar;

1 - Inicial: Neste nível os processos são esporádicos e desorganizados, não existe documentação e controle algum;

2 – Repetitivo mas intuitivo: Neste nível os processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos;

3 - Definido: Neste nível os procedimentos estão estabelecidos e são cumpridos. Inicio do uso de indicadores para controle;

4 - Gerenciados: Neste nível os processos estão integrados e alinhados. As metas e planos são baseados em dados e indicadores consistentes.

5 - Otimizado: Boas práticas são seguidas e automatizadas com base em resultados de melhoria contínua.

A partir desses níveis foi desenvolvido um roteiro para os processos do COBIT, envolvendo o estágio atual, de desenvolvimento, de padrões internacionais da organização o estágio que a empresa pretende chegar. Este modelo de verificação de maturidade será usado neste trabalho para verificar a maturidade dos processos do COBIT.

2.4.3 Relação BSC x COBIT x Segurança da Informação

O alinhamento da TI à estratégia da organização pode ser obtido através do mapeamento dos objetivos genéricos de negócio para a TI (BSC) com os objetivos genéricos de TI para o negócio (COBIT), isto quando a necessidade alcançar o nível tático, conforme demonstrado no Quadro 1 e complementado no Quadro 2. Porém, quando a necessidade alcançar também o nível operacional, este alinhamento deve ser complementado com outras necessidades, como no caso o alinhamento estratégico com a segurança da informação.

Perspectivas (BSC)		**Objetivos genéricos de negócio para TI Conforme BSC**	**Objetivos genéricos de TI para o negócio conforme Quadro 2 conforme Cobit**
Financeira	F1	Prover bom retorno sobre o investimento de TI	24
	F2	Gerenciar riscos de negócio relacionado a TI	2, 14, 17, 18, 19, 20,21, 22
	F3	Melhorar a transparência e governança corporativa	2, 18
Cliente	C1	Melhorar serviço e orientação ao cliente	3, 23
	C2	Oferecer produtos e serviços competitivos	5, 24
	C3	Estabelecer continuidade e disponibilidade de serviços	10, 16, 22, 23
	C4	Criar agilidade para suportar alterações de requisitos de negócios	1, 5, 25
	C5	Atingir otimização de custo em entregas de serviços	7, 8, 10, 24
	C6	Disponibilizar informações confiáveis e úteis para tomadas de decisões	2, 4, 12, 20, 26
Processos internos	P0	Melhorar e manter funcionalidades dos processos de negócio	6, 7, 11
	P2	Reduzir custos dos processos	7, 8, 13, 15, 24
	P3	Prover adequação com leis, regulamentações e contratos	2, 19, 20, 21, 22, 26,27
	P4	Prover adequação com políticas internas	2, 13
	P5	Gerenciar mudanças no negócio	1, 5, 6, 11, 28
	P6	Melhorar e manter a produtividade operacional	7, 8, 11, 13

		e dos colaboradores	
Aprendizado e crescimento	A1	Gerenciar inovação de produtos e negócios	5, 25, 28
	A2	Identificar e manter pessoas qualificadas e motivadas	9

Quadro 1: Objetivos genéricos de negócio para a TI nas perspectivas do BSC

Fonte: Adaptado ITGI (2009)

O Quadro 1 mostra a integração entre estes objetivos de negócio e de TI sugeridos pelo COBIT nas perspectivas do BSC. Para este trabalho, os objetivos genéricos de TI são uma etapa para o mapeamento do modelo com a finalidade de atingir os objetivos genéricos de negócio, específico para o nível tático.

Assim como para o negócio, o ITG, (2009) sugere 28 objetivos genéricos aplicáveis para a área de TI relacionados aos processos do COBIT conforme Quadro 2.

	Objetivos genéricos de TI para o negócio (BSC)	Processos COBIT
1	Responder aos requisitos do negócio de forma alinhada à estratégia do negócio.	PO1, PO2, PO4, PO10, AI1, AI6, AI7, ES1, ES3, MO1
2	Responder aos requisitos de governança de forma alinhada à alta direção.	PO1, PO4, PO10, MO1, MO4
3	Garantir a satisfação dos usuários finais com bons níveis de serviços.	PO8, AI4, ES1, ES2, ES7, ES8, ES10, ES13
4	Otimizar o uso da informação.	PO2, ES11
5	Criar agilidade de TI.	PO2, PO4, PO7, AI3
6	Definir como os requisitos funcionais e de controle do negócio são traduzidos em soluções automatizadas eficientes e efetivas.	AI1, AI2, AI6
7	Adquirir e manter sistemas de aplicação integrados e padronizados.	PO3, AI2, AI5
8	Adquirir e manter infra-estrutura de TI integrada e padronizada.	AI3, AI5
9	Adquirir e manter competências em TI que atenda à estratégia de TI.	PO7, AI5
10	Garantir satisfação mútua em relacionamento com terceiros	ES2
11	Garantir integração das aplicações com os processos de negócios.	PO2, AI4, AI7
12	Garantir transparência e entendimento dos custos, benefícios, estratégias, política e níveis de serviços de TI.	PO5, PO6, ES1, ES2, ES6, MO1, MO4
13	Garantir uso e desempenho adequados das aplicações e soluções de TI.	PO6, AI4, AI7, ES7, ES8
14	Responder pelos ativos de TI e protegê-los.	PO9, ES5, ES9, ES12, MO2
15	Aperfeiçoar a infra-estrutura e recursos de TI.	PO3, AI3, ES3, ES7, ES9
16	Reduzir defeitos e retrabalho nas entregas de soluções e serviços.	PO8, AI4, AI6, AI7, ES10
17	Garantir o cumprimento dos objetivos de TI.	PO9, ES10, MO2
18	Estabelecer clareza no impacto de riscos do negócio em relação a objetivos e recursos de TI.	PO9
19	Assegurar que informações críticas e confidenciais são inacessíveis a aqueles que não devem ter acesso a elas.	PO6, ES5, ES11, ES12

20	Garantir que as informações de negócio e transações automatizadas são confiáveis.	PO6, AI7, ES5
21	Garantir que os serviços e infra-estrutura de TI resistam a falhas em função de erros, ataques deliberados ou desastres.	PO6, AI7, ES4, ES5, ES12, ES13, MO2
22	Garantir impacto mínimo no negócio no caso de uma interrupção ou anormalidade em um serviço de TI.	PO6, AI6, ES4, ES12
23	Assegurar que os serviços de TI estão disponíveis quando solicitados.	ES3, ES4, ES8, ES13
24	Melhorar a relação custo-eficiência de TI contribuindo com a rentabilidade do negócio.	PO5, ES6
25	Entregar projetos no prazo e nos orçamento previstos, observando padrões de qualidade.	PO8, PO10
26	Manter a integridade da informação e da infra-estrutura.	AI6, ES5
27	Garantir que a TI observe a legislação, regulamentações e contratos.	ES11, MO2, MO3, MO4
28	Garantir que a TI demonstre qualidade de serviços eficiente em relação a seu custo, melhoria contínua e prontidão para futuras mudanças.	PO5, ES6, MO1, MO4

Quadro 2: Objetivos genéricos de TI para o negócio x processos do COBIT

Fonte: ITGI (2009)

Os objetivos do Quadro 2 são a base para a construção de um dos instrumentos para coleta de dados.

Os Quadros 1 e 2 relacionam o alinhamento entre os objetivos de negócio e de TI, sendo que para a análise de segurança da informação os mesmos são ampliados nos Quadros 3, 4 e 5 contemplando o foco de segurança proposto nesta dissertação. Isto significa afirmar que o alinhamento entre negócio e TI necessariamente deve ampliar o enfoque tático (BSC + COBIT) e alcançar também o nível operacional iniciando no nível estratégico. Essa integração nos 3 níveis foi realizada no presente trabalho para atender a segurança da informação.

A integração BSC x COBIT x Requisitos de Segurança da Informação pode ser obtida com o mapeamento dos Objetivos de Negócio e de TI com os Requisitos de Segurança nos seguintes graus:

Primário (P): Impacta diretamente o critério de informação a que se refere.

Secundário (S): Satisfaz parcialmente ou indiretamente o critério de informação a que se refere.

Em branco (-): Pode ser aplicável, entretanto os requisitos são satisfeitos de forma mais apropriada por outro objetivo ou processo.

Para a TI estar alinhada aos Objetivos de Negócio ela deverá associar os seus Objetivos de TI, definir suas metas, medidas, iniciativas e estabelecer suas prioridades. Como o trabalho em questão se propõe a analisar aspectos de segurança serão considerados somente os Objetivos de TI e processos do COBIT envolvendo os Requisitos de Segurança confidencialidade, integridade e disponibilidade. O Quadro 3 apresenta a relação entre os Objetivos genéricos de TI para o Negócio alinhado com os processos do COBIT e os Requisitos de Segurança. Uma vez identificada esta relação é possível verificar o relacionamento entre o BSC, COBIT, ISO/IEC27002.

			Requisitos de segurança		
			Confidencialidade	**Integridade**	**Disponibilidade**
	Objetivo genérico de TI para o negócio (BSC)	**Processos COBIT**			
1	Responder aos requisitos do negócio de forma alinhada à estratégia do negócio.	PO1, PO2, PO4, PO10, AI1, AI6, AI7, ES1, ES3, MO1	-	S	S
2	Responder aos requisitos de governança de forma alinhada à alta direção.	PO1, PO4, PO10, MO1, MO4	-	-	-
3	Garantir a satisfação dos usuários finais com bons níveis de serviços.	PO8, AI4, ES1, ES2, ES7, ES8, ES10, ES13	-	S	S
4	Otimizar o uso da informação.	PO2, ES11	-	P	-
5	Criar agilidade de TI.	PO2, PO4, PO7, AI3	-	S	-
6	Definir como os requisitos funcionais e de controle do negócio são traduzidos em soluções automatizadas eficientes e efetivas.	AI1, AI2, AI6	-	-	-
7	Adquirir e manter sistemas de aplicação integrados e padronizados.	PO3, AI2, AI5	-	-	-
8	Adquirir e manter infra-estrutura de TI integrada e padronizada.	AI3, AI5	-	-	-
9	Adquirir e manter competências em TI que atenda à estratégia de TI.	PO7, AI5	-	-	-
10	Garantir satisfação mútua em relacionamento com terceiros.	ES2	S	S	S
11	Garantir integração das aplicações com os	PO2, AI4, AI7	-	S	S

	processos de negócios.				
12	Garantir transparência e entendimento dos custos, benefícios, estratégias, política e níveis de serviços de TI.	PO5, PO6, DS1, DS2, ES6, MO1, MO4	-	-	-
13	Garantir uso e desempenho adequados das aplicações e soluções de TI.	PO6, AI4, AI7, ES7, ES8	-	-	-
14	Responder pelos ativos de TI e protegê-los.	PO9, DS5, DS9, DS12, MO2	P	P	P
15	Aperfeiçoar a infra-estrutura e recursos de TI.	PO3, AI3, ES3, ES7, ES9	-	-	-
16	Reduzir defeitos e retrabalho nas entregas de soluções e serviços.	PO8, AI4, AI6, AI7, ES10	-	S	S
17	Garantir o cumprimento dos objetivos de TI.	PO9, ES10, MO2	S	S	S
18	Estabelecer clareza no impacto de riscos do negócio em relação a objetivos e recursos de TI.	PO9	P	P	P
19	Assegurar que informações críticas e confidenciais são inacessíveis a aqueles que não devem ter acesso a elas.	PO6, ES5, ES11, ES12	P	P	S
20	Garantir que as informações de negócio e transações automatizadas são confiáveis.	PO6, AI7, ES5	-	P	S
21	Garantir que os serviços e infra-estrutura de TI resistam a falhas em função de erros, ataques deliberados ou desastres.	PO6, AI7, ES4, ES5, ES12, ES13, MO2	-	S	P
22	Garantir impacto mínimo no negócio no caso de uma interrupção ou anormalidade em um serviço de TI.	PO6, AI6, ES4, ES12	-	S	P
23	Assegurar que os serviços de TI estão disponíveis quando solicitados.	ES3, ES4, ES8, ES13	-	-	P
24	Melhorar a relação custo-eficiência de TI contribuindo com a rentabilidade do negócio.	PO5, ES6	-	-	-
25	Entregar projetos no prazo e nos orçamento previstos, observando padrões de qualidade.	PO8, PO10	-	S	-
26	Manter a integridade da informação e da infra-estrutura.	AI6, ES5	-	P	P
27	Garantir que a TI observe a legislação, regulamentações e contratos.	ES11, MO2, MO3, MO4	S	S	-
28	Garantir que a TI demonstre qualidade de serviços eficiente em relação a seu custo, melhoria contínua e prontidão para futuras mudanças.	PO5, ES6, MO1, MO4	-	-	-

Quadro 3: Relação BSC x COBIT x Requisitos de segurança

Fonte: Adaptado ITGI (2009)

Com o quadro apresentado acima, é possível identificar os objetivos de TI e os respectivos processos do COBIT que servem de base para a análise da segurança da informação.

2.4.4 Segurança da Tecnologia da Informação

A informação é um ativo de significativa importância para o negócio e conseqüentemente necessita ser protegida (ISO/IEC27002). Ela é considerada um dos principais patrimônios da empresa e que se encontra sob constante risco (DIAS,

2000). A informação é reconhecida como ativo crítico para a continuidade operacional e sustentabilidade da empresa (SÊMOLA, 2003). Dispor da informação correta, na hora adequada é pré-requisito para uma tomada de decisão ágil e correta. É neste contexto que se destaca a importância dos aspectos relacionados à segurança da informação.

Uma informação segura deve atender três princípios básicos, a confidencialidade, a integridade e a disponibilidade, (ITGI, 2009), (KWOK e LONGLEY, 1999), (FITZGERALD, 2007), (SÊMOLA, 2003), (DIAS, 2000), (MOREIRA, 2001). Os autores também citam outros aspectos como o Não Repúdio, Autenticidade. Porém os mesmos podem ser enquadrados nos três princípios básicos da segurança como segue.

Confidencialidade: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.
Integridade: Toda a Informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
Disponibilidade: Toda a informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

A empresa deve dispor de uma política de segurança da informação associada ao risco que a TI representa para a continuidade do negócio. A política de segurança deve considerar o grau de dependência entre os processos da empresa e os sistemas de informação. Quanto mais dependente a empresa for dos sistemas de informação, maior será o risco das operações a ser comprometido com sistemas vulneráveis, (FERNANDEZ e ABREU, 2008). Apesar de ser independente em sua forma de condução e gestão, o plano de segurança também pode ser adicionado ao plano de TI e à própria estratégia da empresa. De acordo com a ISO/IE27002, os requisitos que devem ser avaliados para se estabelecer a política de segurança são:

- O impacto nos negócios resultantes de uma falha de segurança;

- A probabilidade da ocorrência de falhas, frente às vulnerabilidades encontradas e;
- A seleção dos controles de segurança da informação mais adequados a análise de riscos e vulnerabilidades.

O primeiro requisito é a base para justificativa a relevância deste trabalho sendo que os demais possibilitam um estudo em maior profundidade relacionado a este impacto, pois um incidente pode impedir direta ou indiretamente a organização de cumprir sua missão e de gerar valor para o acionista. Essa perspectiva traz a segurança da informação para um novo patamar, não apenas relacionada em nível tecnológico e de ferramentas necessárias para proteção da informação, mas também como um dos pilares de suporte à estratégia de negócio de uma organização. A gestão da segurança assume, então, um novo significado, pois considera os elementos estratégicos de uma organização.

O modelo COBIT disponibiliza um mapeamento dos requisitos de segurança identificados como três (3) dos sete (7) requisitos de negócio relacionados aos trinta e quatro (34) processos. As medidas de controle para cada processo de TI não satisfazem todos os requisitos de negócio no mesmo grau. Devido a isto o Framework do COBIT define os mesmos três (3) graus de controle:

Primário (P);

Secundário (S); e

Em branco (-)

Os três (3) graus de controle estão representados e aplicados no Quadro 4, da mesma forma que já foram descritos anteriormente.

O fornecimento de uma indicação por processo de TI e domínio, informando qual requisito de negócio/segurança da informação é impactado está evidenciado no Quadro 4. Também é apresentada uma relação para quais recursos de TI são aplicáveis cada um dos processos do COBIT.

Estes são classificados em dois tipos:

1 - Aplicável = (-) e

2 - Não aplicável = (+).

			Requisitos de negócio/ segurança			Recursos de TI			
Domínios COBIT	**Processos COBIT**		**Confidencialidade**	**Integridade**	**Disponibilidade**	**Aplicações**	**Informações**	**Infra-estrutura**	**Pessoas**
Planejamento e Organização	PO1	Definir um plano estratégico de TI.	-	-	-	+	+	+	+
	PO2	Definir a arquitetura de informação.	S	S	-	+	+	-	-
	PO3	Determinar a direção tecnológica.	-	-	-	+	-	+	-
	PO4	Definir processos de TI, Organização e relacionamentos.	-	-	-	-	-	-	+
	PO5	Gerenciar o investimento de TI.	-	-	-	+	-	+	+
	PO6	Comunicar metas e diretrizes gerenciais.	-	-	-	-	+	-	+
	PO7	Gerenciar recursos humanos.	-	-	-	-	-	-	+
	PO8	Gerenciar qualidade.	-	-	-	+	+	+	+
	PO9	Avaliar e gerenciar riscos.	P	P	P	+	+	+	+
	PO10	Gerenciar projetos.	-	-	-	+	-	-	+
Aquisição e implementação	AI1	Identificar soluções.	-	-	-	+	-	+	-
	AI2	Adquirir e manter *software* aplicativo.	-	S	-	+	-	-	-
	AI3	Adquirir e manter arquitetura tecnológica.	-	S	-			+	-
	AI4	Desenvolver e manter procedimentos de TI.	-	S	-	+		+	+
	AI5	Obter recursos de TI.	-	S	S	+	+	+	+
	AI6	Gerenciar mudanças.	-	P	P	+	+	+	+
	AI7	Instalar e certificar soluções e mudanças.	-	S	S	+	+	+	+
Entrega e suporte	ES1	Definir níveis de serviços.	S	S	S	+	+	+	+
	ES2	Gerenciar serviços de terceiros.	S	S	S	+	+	+	+
	ES3	Gerenciar desempenho e capacidade.	-	-	S		+		+
	ES4	Garantir continuidade dos serviços.	-	-	P	+	+	+	+
	ES5	Garantir segurança dos sistemas.	P	P	S	+	+	+	+
	ES6	Identificar e alocar custos.	-	-	-	+	+	+	+
	ES7	Educar e treinar usuários.	-	-	-	-	-	-	+
	ES8	Gerenciar central de serviços e incidentes.	-	-	-	+	-	-	+
	ES9	Gerenciar a configuração.	-	-	S	+	+	+	-
	ES10	Gerenciar problemas.	-	-	S	+	+	+	+
	ES11	Gerenciar dados.	-	P	-	-	+	-	-
	ES12	Gerenciar os ambientes físicos.	-	P	P	-	-	+	-
	ES13	Gerenciar operações.	-	S	S	+	+	+	+
Monitoração e avaliação	MO1	Monitorar e avaliar a desempenho de TI.	S	S	S	+	+	+	+
	MO2	Monitorar e avaliar o controle interno.	S	S	S	+	+	+	+
	MO3	Assegurar a conformidade regulatória.	S	S	S	+	+	+	+
	MO4	Promover governança de TI.	S	S	S	+	+	+	+

Quadro 4: Relação entre os processos COBIT e requisitos de segurança
Fonte: ITGI (2009)

O tema segurança é abordado por seis (6) processos do COBIT em forma primária e dezesseis (16) de forma secundária. Visto que o objetivo deste trabalho é desenvolver alinhamento estratégico entre os objetivos de negócio, os objetivos de TI e as práticas de segurança da informação para avaliar aspectos de segurança em nível operacional, torna-se apropriado a utilização de uma estruturação que especifique os aspectos de segurança. Esta complementação foi então realizada através da ISO/IEC27002 - Técnicas de segurança - Código de prática para a gestão da segurança da informação.

A ISO/IEC27002 tem como objetivo fornecer recomendações para a gestão da segurança da informação para que os departamentos responsáveis possam proporcionar uma base comum para o desenvolvimento de normas de segurança, práticas efetivas de gestão da segurança e prover confiança nos relacionamentos entre as organizações. A norma abrange dez (10) domínios reunidos em trinta e seis (36) grupos que totalizam cento e vinte e sete (127) controles.

Na sequência são apresentados resumidamente os objetivos dos domínios da norma através de capítulos da mesma iniciando número 5, pois os números 1 ao 4 são capítulos introdutórios da norma sendo que (0) é a Introdução, (1) é o Objetivo, (2) corresponde aos Termos e definições, (3) refere-se a Estrutura da norma enquanto que o (4) corresponde à Análise/avaliação e tratamento de riscos.

5 - Política de segurança da informação (PL): Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes;

6 - Organizando a segurança da informação (OI): Gerenciar a segurança da informação dentro da organização bem como manter a segurança dos recursos de processamento da informação que são acessados, processados, comunicados ou gerenciados por partes externas;

7 - Gestão de ativos (GA): Alcançar e manter a proteção adequada dos ativos da organização. Assegurar que a informação receba um nível adequado de proteção;

8 - Segurança em recursos humanos (RH): Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, reduzindo o risco de roubo, fraude e mal uso de recursos. Que os mesmos estejam conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estejam preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos, para reduzir o risco de erro humano e não deixem a organização ou mudem de trabalho de forma desordenada;

9 - Segurança física e do ambiente (SA): Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização. Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização;

10 - Gerenciamento das operações e comunicações (GO): Garantir a operação segura e correta dos recursos de processamento da informação. Minimizar o risco de falhas nos sistemas. Proteger a integridade do *software* e da informação. Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação, bem como garantir a proteção das informações em redes e a proteção da infra-estrutura e de suporte. Prevenir contra divulgação não autorizada, modificação, remoção e destruição dos ativos e interrupções das atividades do negócio. Manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas. Garantir a segurança de serviços de comércio eletrônico e sua utilização segura. Detectar atividades não autorizadas de processamento da informação;

11 - Controle de acessos (CA): Controlar o acesso à informação. Assegurar o acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação. Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação. Prevenir acesso não autorizado aos serviços de rede, bem como

prevenir acesso não autorizado aos sistemas operacionais. Prevenir acesso não autorizado à informação contida nos sistemas de aplicação. Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto;

12 - Aquisição, desenvolvimento e manutenção de sistemas de informação (AQ): Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mal uso de informações em aplicações. Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos. Garantir a segurança de arquivos de sistema. Manter a segurança de sistemas aplicativos e da informação. Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas;

13 - Gestão de incidentes de segurança da informação (GI): Assegurar que fragilidades e eventos de segurança da informação associadas com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação;

14 - Gestão da continuidade do negócio (GC): Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil.

15 - Conformidade (CF): Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação. Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.

Com o objetivo de verificar a conformidade com os domínios da norma, Eloff & Eloff, (2003) propõem quatro níveis de proteção em relação às práticas de segurança. Isso permite que as organizações tenham uma visão geral e verifiquem o atual estágio em que se encontram as práticas possibilitando uma evolução conforme a importância de cada domínio para o negócio como segue:

1 – Proteção inadequada: Não existe nenhum esforço da organização em implementar qualquer um dos controles recomendados para as suas necessidades

específicas. Produtos e equipamentos certificados não têm qualquer influência na classificação das seções neste nível.

2 – Proteção mínima: A organização demonstra o mínimo de esforço na adoção de alguns dos controles recomendados. Produtos e equipamentos certificados não têm qualquer influência na classificação das seções neste nível.

3 – Proteção reativa: A maioria dos controles são implementados e devem satisfazer os requisitos com base procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso.

4 – Proteção adequada: Implementa todos os controles recomendados pelo domínio. Sempre que possível é obrigatório o uso de produtos e equipamentos certificados.

Para uma abordagem estratégica em relação às práticas de segurança é necessário estabelecer uma relação com o BSC porém considerando ambos modelos, tanto BSC quanto a norma. Como há uma distância significativa entre os dois modelos, o modelo tático COBIT pode contribuir efetivamente neste alinhamento entre os três diferentes níveis. Esta relação então se torna possível mapeando as práticas da ISO/IEC 27002 com os processos do COBIT que por sua vez foram mapeados com o BSC no Quadros 1, 2 e 3. Na sequencia é apresentado o mapeamento do COBIT com a ISO/IEC27002.

2.4.5 Integração COBIT x ISO/IEC27002

Para realizar uma integração mais detalhada sobre os aspectos de segurança o ITGI (2009) relaciona os processos do COBIT com as práticas da ISO/IEC27002 conforme Quadro 5. As práticas da ISO/IEC27002 servem como base para elaboração de um dos instrumentos de coleta de dados, as quais iniciam no item 7.1.1 que é relativa à definição da arquitetura da informação

Processos COBIT		Práticas de segurança ISO/IEC27002
PO1 [1]	Definir um plano estratégico de TI.	
PO2	Definir a arquitetura de informação.	7.1.1 Inventário dos ativos.
		7.2.1 Recomendações para classificação.
		10.7.1 Gerenciamento de mídias removíveis.
		10.9.1 Comércio eletrônico.
		10.9.2 Transações on-line.
		11.1.1 Política de controle de acesso.
PO3 [1]	Determinar a direção tecnológica.	
PO4 [1]	Definir processos de TI, Organização e relacionamentos.	
PO5 [1]	Gerenciar o investimento de TI.	
PO6 [1]	Comunicar metas e diretrizes gerenciais.	
PO7 [1]	Gerenciar recursos humanos.	
PO8 [1]	Gerenciar qualidade.	
PO9	Avaliar e gerenciar riscos.	5.1.2 Análise crítica da política de segurança da informação.
		13.1.2 Notificando fragilidades de segurança da informação.
		13.1.1 Notificação de eventos de segurança da informação.
		14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio.
		14.1.2 Continuidade de negócios e análise/avaliação de riscos.
PO10 [2]	Gerenciar projetos.	
AI1 [1]	Identificar soluções	
AI2	Adquirir e manter software aplicativo.	6.1.4 Processo de autorização para os recursos de processamento da informação.
		7.2.1 Recomendações para classificação.
		10.3.2 Aceitação de sistemas.
		10.10.1 Registros de auditoria.
		10.10.5 Registros (*log*) de falhas.
		11.6.2 Isolamento de sistemas sensíveis.
		12.1.1 Análise e especificação dos requisitos de segurança.
		12.2.1 Validação dos dados de entrada.
		12.2.2 Controle do processamento interno.
		12.2.3 Integridade de mensagens.
		12.2.4 Validação de dados de saída.
		12.3.1 Política para o uso de controles criptográficos.
		12.4.3 Controle de acesso ao código-fonte de programa.
		12.5.1 Procedimentos para controle de mudanças.
		12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.
		12.5.3 Restrições sobre mudanças em pacotes de software.
		12.5.4 Vazamento de informações.
		12.5.5 Desenvolvimento terceirizado de software.
		13.2.3 Coleta de evidências.
		15.3.1 Controles de auditoria de sistemas de informação.
		15.3.2 Proteção de ferramentas de auditoria de sistemas de informação.
AI3	Adquirir e manter arquitetura tecnológica.	9.1.5 Trabalhando em áreas seguras.
		9.2.4 Manutenção dos equipamentos.
		10.1.4 Separação dos recursos de desenvolvimento, teste e de produção.
		10.4.2 Controles contra códigos móveis.

[1] Os requisitos de segurança são satisfeitos de forma mais apropriada por outro processo.
[2] Os requisitos de segurança são satisfeitos de forma mais apropriada por outro processo.

		12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.
		12.6.1 Controle de vulnerabilidades técnicas.
AI4	Desenvolver e manter procedimentos de TI.	10.1.1 Documentação dos procedimentos de operação.
		10.3.2 Aceitação de sistemas.
		10.7.4 Segurança da documentação dos sistemas.
		13.2.2 Aprendendo com os incidentes de segurança da informação.
AI5	Obter recursos de TI.	6.1.5 Acordos de confidencialidade.
		6.2.3 Identificando segurança da informação nos acordos com terceiros.
		10.8.2 Acordos para a troca de informações.
		12.5.5 Desenvolvimento terceirizado de software.
AI6	Gerenciar mudanças.	10.1.2 Gestão de mudanças.
		11.5.1 Procedimentos seguros de entrada no sistema (*log-on*).
		11.5.4 Uso de utilitários de sistema.
		11.6.1 Restrição de acesso à informação.
		12.5.3 Restrições sobre mudanças em pacotes de software.
AI7	Instalar e certificar soluções e mudanças.	6.1.4 Processo de autorização para os recursos de processamento da informação.
		8.2.2 Conscientização, educação e treinamento em segurança da informação.
		10.1.4 Separação dos recursos de desenvolvimento, teste e de produção.
		10.3.2 Aceitação de sistemas.
		12.4.3 Controle de acesso ao código-fonte de programa.
		12.5.1 Procedimentos para controle de mudanças.
		12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.
		12.5.4 Vazamento de informações.
ES1	Definir níveis de serviços.	10.2.1 Entrega de serviços.
		10.2.2 Monitoramento e análise crítica de serviços terceirizados.
		10.2.3 Gerenciamento de mudanças para serviços terceirizados.
ES2	Gerenciar serviços de terceiros.	6.2.1 Identificação dos riscos relacionados com partes externas.
		6.2.3 Identificando segurança da informação nos acordos com terceiros.
		8.1.2 Seleção.
		8.1.3 Termos e condições de contratação.
		10.2.1 Entrega de serviços.
		10.2.2 Monitoramento e análise crítica de serviços terceirizados.
		10.8.2 Acordos para a troca de informações.
		10.2.3 Gerenciamento de mudanças para serviços terceirizados.
		12.4.1 Controle de software operacional.
		12.5.5 Desenvolvimento terceirizado de software.
		15.1.4 Proteção de dados e privacidade de informações pessoais.
ES3	Gerenciar desempenho e capacidade.	10.3.1 Gestão de capacidade.
ES4	Garantir continuidade dos serviços.	6.1.6 Contato com autoridades.
		6.1.7 Contato com grupos especiais.
		10.5.1 Cópias de segurança das informações.
		14.1.1 Incluindo segurança da informação no processo de

		gestão da continuidade de negócio.
		14.1.2 Continuidade de negócios e análise/avaliação de riscos.
		14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação.
		14.1.4 Estrutura do plano de continuidade do negócio.
		14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.
ES5	Garantir segurança dos sistemas.	5.1.1 Documento da política de segurança da informação.
		5.1.2 Análise crítica da política de segurança da informação.
		6.1.1 Comprometimento da direção com a segurança da informação.
		6.1.5 Acordos de confidencialidade.
		6.1.2 Coordenação da segurança da informação.
		6.1.8 Análise crítica independente de segurança da informação.
		6.2.1 Identificação dos riscos relacionados com partes externas.
		6.2.2 Identificando a segurança da informação, quando tratando com os clientes.
		6.2.3 Identificando segurança da informação nos acordos com terceiros.
		8.1.1 Papéis e responsabilidades.
		8.2.2 Conscientização, educação e treinamento em segurança da informação.
		8.2.3 Processo disciplinar.
		8.3.1 Encerramento de atividades.
		8.3.3 Retirada de direitos de acesso.
		9.1.6 Acesso do público, áreas de entrega e de carregamento.
		9.2.1 Instalação e proteção do equipamento.
		9.2.3 Segurança do cabeamento.
		10.1.3 Segregação de funções.
		10.4.1 Controles contra códigos maliciosos.
		10.4.2 Controles contra códigos móveis.
		10.6.1 Controles de redes.
		10.7.4 Segurança da documentação dos sistemas.
		10.8.4 Mensagens eletrônicas.
		10.10.1 Registros de auditoria.
		10.10.2 Monitoramento do uso do sistema.
		10.10.3 Proteção das informações dos registros (*log*).
		10.10.4 Registros (*log*) de administrador e operador.
		10.10.5 Registros (*log*) de falhas.
		10.10.6 Sincronização dos relógios.
		11.1.1 Política de controle de acesso.
		11.2.1 Registro de usuário.
		11.2.2 Gerenciamento de privilégios.
		11.2.4 Análise crítica dos direitos de acesso de usuário.
		11.3.1 Uso de senhas.
		11.3.2 Equipamento de usuário sem monitoração.
		11.3.3 Política de mesa limpa e tela limpa.
		11.4.1 Política de uso dos serviços de rede.
		11.4.2 Autenticação para conexão externa do usuário.
		11.4.3 Identificação de equipamento em redes.
		11.4.4 Proteção e configuração de portas de diagnóstico remotas.
		11.4.5 Segregação de redes.
		11.4.6 Controle de conexão de rede.
		11.4.7 Controle de roteamento de redes.
		11.5.1 Procedimentos seguros de entrada no sistema (*log-on*).
		11.5.3 Sistema de gerenciamento de senha.

		11.5.4 Uso de utilitários de sistema.
		11.5.5 Desconexão de terminal por inatividade.
		11.5.6 Limitação de horário de conexão.
		11.6.2 Isolamento de sistemas sensíveis.
		11.7.1 Computação e comunicação móvel.
		11.7.2 Trabalho remoto.
		12.2.3 Integridade de mensagens.
		12.3.1 Política para o uso de controles criptográficos.
		12.3.2 Gerenciamento de chaves.
		12.4.1 Controle de software operacional.
		12.6.1 Controle de vulnerabilidades técnicas.
		13.1.1 Notificação de eventos de segurança da informação.
		13.1.2 Notificando fragilidades de segurança da informação.
		13.2.1 Responsabilidades e procedimentos.
		13.2.3 Coleta de evidências.
		14.1.4 Estrutura do plano de continuidade do negócio.
		15.1.6 Regulamentação de controles de criptografia.
		15.2.2 Verificação da conformidade técnica.
		15.3.1 Controles de auditoria de sistemas de informação.
		15.3.2 Proteção de ferramentas de auditoria de sistemas de informação.
ES5 [1]	Garantir segurança dos sistemas.	
ES6 [1]	Identificar e alocar custos.	
ES7 [1]	Educar e treinar usuários.	
ES8 [1]	Gerenciar central de serviços e incidentes.	
ES9	Gerenciar a configuração.	7.1.2 Proprietário dos ativos.
		7.2.2 Rótulos e tratamento da informação.
		10.7.4 Segurança da documentação dos sistemas.
		11.4.3 Identificação de equipamento em redes.
		12.4.1 Controle de software operacional.
		12.4.2 Proteção dos dados para teste de sistema.
		12.6.1 Controle de vulnerabilidades técnicas.
		12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.
		12.5.3 Restrições sobre mudanças em pacotes de software.
		15.1.5 Prevenção de mau uso de recursos de processamento da informação.
ES10	Gerenciar problemas.	13.2.2 Aprendendo com os incidentes de segurança da informação.
ES11	Gerenciar dados.	9.2.6 Reutilização e alienação segura de equipamentos.
		10.5.1 Cópias de segurança das informações.
		10.7.1 Gerenciamento de mídias removíveis.
		10.7.2 Descarte de mídias.
		10.7.3 Procedimentos para tratamento de informação.
		10.8.1 Políticas e procedimentos para troca de informações.
		10.8.3 Mídias em trânsito.
		10.8.4 Mensagens eletrônicas.
		12.4.2 Proteção dos dados para teste de sistema.
		12.4.3 Controle de acesso ao código-fonte de programa.
		15.1.3 Proteção de registros organizacionais.
ES12	Gerenciar os ambientes físicos.	6.2.1 Identificação dos riscos relacionados com partes externas.
		9.1.1 Perímetro de segurança física.

[1] Os requisitos de segurança são satisfeitos de forma mais apropriada por outro processo

		9.1.2 Controles de entrada física.
		9.1.3 Segurança em escritórios, salas e instalações.
		9.1.4 Proteção contra ameaças externas e do meio ambiente.
		9.1.5 Trabalhando em áreas seguras.
		9.1.6 Acesso do público, áreas de entrega e de carregamento.
		9.2.2 Utilidades.
		9.2.3 Segurança do cabeamento.
		9.2.4 Manutenção dos equipamentos.
		9.2.5 Segurança de equipamentos fora das dependências da organização.
		9.2.7 Remoção de propriedade.
ES13	Gerenciar operações.	9.2.4 Manutenção dos equipamentos.
		10.1.1 Documentação dos procedimentos de operação.
		10.7.4 Segurança da documentação dos sistemas.
MO1	Monitorar e avaliar a desempenho de TI.	10.2.2 Monitoramento e análise crítica de serviços terceirizados.
MO2	Monitorar e avaliar o controle interno.	5.1.1 Documento da política de segurança da informação.
		5.1.2 Análise crítica da política de segurança da informação.
		6.1.8 Análise crítica independente de segurança da informação.
		6.2.3 Identificando segurança da informação nos acordos com terceiros.
		10.2.2 Monitoramento e análise crítica de serviços terceirizados.
		10.10.2 Monitoramento do uso do sistema.
		10.10.4 Registros (*log*) de administrador e operador.
		15.2.1 Conformidade com as políticas e normas de segurança da informação.
		15.2.2 Verificação da conformidade técnica.
		15.3.1 Controles de auditoria de sistemas de informação.
MO3	Assegurar a conformidade regulatória.	6.1.6 Contato com autoridades.
		15.1.1 Identificação da legislação vigente.
		15.1.2 Direitos de propriedade intelectual.
		15.1.4 Proteção de dados e privacidade de informações pessoais.
MO4	Fornecer governança de TI.	5.1.2 Análise crítica da política de segurança da informação.
		6.1.8 Análise crítica independente de segurança da informação.
		10.10.2 Monitoramento do uso do sistema.

Quadro 5: Relação COBIT 4.1 e ISO/IEC27002

Fornte: Adaptado ITGI (2009)

O quadro 5 lista os processos do COBIT relacionados aos os requisitos de segurança de impacto primário e secundário, que por sua vez estão mapeados com as práticas de segurança (em nível operacional) para construir uma parte do mapeamento do modelo de integração entre BSC x COBIT x Segurança da Informação e possibilitar a complementação das três partes ou dos três níveis.

3 MAPEAMENTO DOS MODELOS DE INTEGRAÇÃO BSC X COBIT X ISO/IEC27002

Como apresentado no referencial teórico foi desenvolvida a integração dos modelos do BSC x COBIT x ISO/IEC27002, conforme Figura 3, através dos objetivos genéricos de negócio para TI nas perspectivas do BSC, mapeados com os objetivos genéricos de TI para o negócio propostos pelo ITGI, 2009. Na sequência foi utilizado o mapeamento dos objetivos genéricos de TI para o negócio com os processos do COBIT que envolvem os requisitos de segurança confidencialidade, integridade e disponibilidade que por sua vez permitiu realizar a identificação das práticas de segurança mais apropriadas para a organização, conforme Figura 8. Esta figura representa um *framework* desenvolvido e aplicado pelo próprio autor para realizar o alinhamento entre objetivos de negócio e os de TI (framework integração entre **os** modelos de governança em TI, nível de abrangência e instrumentos de coleta de dados).

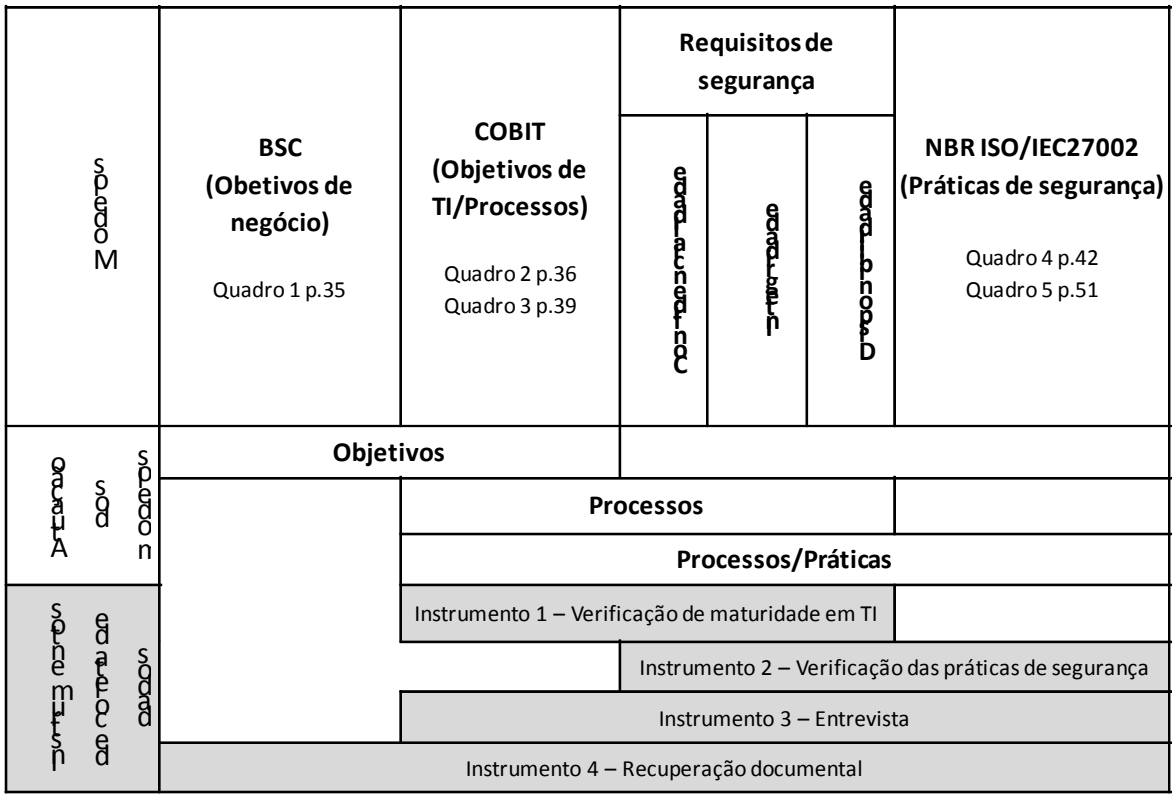


Figura 8: *Framework* de integração entre os modelos de governança em TI, nível de abrangência e instrumentos de coleta de dados.

Fonte: Elaborado pelo autor

A Figura 8 mostra a integração dos modelos e o nível de atuação de cada modelo. Considerando o nível de atuação dos modelos e os requisitos de segurança, foi construído este *framework* para mostrar como os requisitos de segurança são atendidos em cada nível organizacional. O COBIT traz o mapeamento dos objetivos genéricos de TI e processos mapeados com os requisitos de segurança, porém não traz o mapeamento com as práticas de segurança da ISO/IEC27002 a partir das dos objetivos genéricos de TI.

Este mapeamento foi realizado pelo autor possibilitando um enfoque estratégico para o tema segurança quando a abordagem mais técnica e tática se comunica com a abordagem mais estratégica (modelo BSC). Com base neste mapeamento, foram desenvolvidos instrumentos para coleta de dados e aplicar e validar sua estruturação em cada nível como segue:

Instrumento 1 – Verificação de nível de maturidade em TI com a aplicação de um questionário baseado nos processos do modelo COBIT e identificados através do mapeamento juntamente com os requisitos de segurança. Este questionário foi aplicado com a equipe gerencial conforme Quadro 6.

Instrumento 2 – Verificação das práticas de segurança com a aplicação de um questionário baseado nas práticas recomendadas pela ISO/IEC27002 e identificadas através do mapeamento. Este questionário foi aplicado com a empresa terceirizada que presta serviços suporte à rede e servidores e o técnico interno responsável pelo suporte conforme Quadro 7.

Instrumento 3 - Aplicação de uma entrevista com a diretoria responsável pela TI com base nos objetivos genéricos de TI para o negócio, estes sugeridos pelo modelo COBIT e mapeados pelos requisitos de segurança conforme Quadro 8.

Instrumento 4 - Recuperação documental para obter e confirmar informações eventualmente duvidosas ou que não foram respondidas através dos instrumentos 1, 2 e 3.

Assim, como os modelos teóricos BSC, COBIT e ISO, estes instrumentos também têm níveis de alcance distintos quando aplicados, porém a sua combinação ou integração é que proporciona uma análise de dados a partir dos objetivos genéricos de TI para o negócio, conforme Quadro 9. Esta análise permite então uma visão abrangente dos aspectos relacionados a segurança a partir de uma visão de negócio, resultando em um alinhamento especificamente estratégico da segurança da informação, objetivo principal deste trabalho.

A aplicação combinada destes quatro (4) instrumentos possibilita uma compreensão das necessidades e vulnerabilidades no ambiente TI da empresa com uma dimensão estratégica, possibilitando direcionar os recursos de TI de forma alinhada ao modelo de negócio.

A primeira etapa de Coleta de dados através do **Instrumento 1** contemplou os processos do COBIT com impacto primário ou secundário em relação aos requisitos de segurança confidencialidade ou integridade ou disponibilidade. Este instrumento é uma adaptação do COBIT com o CMMI e esta adaptação foi elaborada pelo próprio autor, constituindo parte do *framework* desenvolvido.

Processos COBIT		**Nível de maturidade**					
		0 - Inexistente	**1 - Inicial**	**2 - Repetitivo**	**3 - Definido**	**4 - Gerenciado**	**5- Otimizado**
PO - Organização e planejamento.							
PO1	**Define o planejamento estratégico de TI.** As empresas dispõem de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio						
PO2	**Define a arquitetura da informação.** A empresa documenta a estrutura de TI e sistemas de informação com modelos e dicionário de dados.						
PO4	**Define a organização de TI e seus relacionamentos.** A empresa estabelece a estrutura de RH de TI com cargos, suas responsabilidades e os relacionamentos com as demais áreas da organização.						

PO6	**Comunica as metas e diretrizes gerenciais.** A empresa estabelece e comunica as metas de TI para a equipe e as políticas de TI para a organização.						
PO7	**Gerencia os recursos humanos.** Gerencia o RH de TI com um plano de capacitação e desenvolvimento de pessoal e plano de carreira considerando as necessidades do negócio e as tecnologias utilizadas na empresa. Desenvolve mecanismos de motivação para a equipe de TI.						
PO8	**Gerencia a qualidade.** Mantém de um sistema de gestão da qualidade com documentação dos processos, seleção de fornecedores e melhoria contínua de TI, integrado ao sistema de qualidade da empresa.						
PO9	**Avalia e gerencia os riscos.** Mantém um quadro de gestão de riscos, analisa ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência.						
PO10	**Gerencia os projetos.** Coordena projetos através de um plano mestre com níveis de qualidade, recursos necessários e prazos observando modelos e melhores práticas de mercado.						
AI - Aquisição e Implementação.							
AI1	**Identifica soluções de automação.** Para compra ou desenvolvimento de novas aplicações é realizada uma análise de requisitos, considerando fontes alternativas, análise de viabilidade econômica e tecnológica, análise de risco, custo benefício.						
AI3	**Adquire e mantém a arquitetura tecnológica.** Mantém um plano de manutenção, aquisição e implementação de melhoria da infra-estrutura tecnológica com o objetivo de dar sustentação as aplicações da empresa.						
AI4	**Desenvolve e mantém procedimentos de TI.** Disponibiliza documentação e treinamento os usuários e profissionais de TI para correta utilização dos sistemas e infra-estrutura de TI.						
AI5	**Obtém recursos de TI.** Dispõe de um procedimento para aquisição de recursos necessários de TI, incluindo hardware, software, serviços, pessoas e fornecedores.						
AI6	**Gerenciar mudanças** Avalia e aprova mudanças no ambiente, tanto em equipamentos e arquitetura quanto em sistemas e processos.						
AI7	**Instala e certifica soluções e mudanças.** Antes da entrega de novas soluções de TI (Software, Hardware e Sistemas) são realizados testes apropriados e um acompanhamento pós-implantação.						
DS - Entrega e suporte.							
ES1	**Define níveis e mantém os acordos de níveis de serviços.** Formaliza os níveis de atendimento e internos e externos das soluções TI.						
ES2	**Gerencia os serviços de terceiros.** Acompanha e avalia os serviços contratados.						
ES3	**Gerenciar desempenho e capacidade da TI.** A empresa define e revisa periodicamente os recursos computacionais e garante que não haja escassez de recursos, evitando problemas de desempenho nas aplicações ou desperdício de investimentos.						
ES4	**Garante a continuidade dos serviços.** Assegura a continuidade dos serviços, incluindo sistemas de Backup, manutenção de equipamentos, testes e plano de contingência de hardware e serviços críticos.						
ES5	**Garante a segurança dos sistemas.** A empresa dispõe de políticas de segurança, visa a preservação da confidencialidade, da integridade e da disponibilidade da informação.						
ES7	**Educa e treina os usuários.** A empresa mantém um plano de treinamento de usuários e profissionais de TI						

	para uso eficaz e eficiente dos sistemas de informação.						
ES8	**Gerencia a central de serviços e incidentes.** Existe o registro e controle das solicitações e incidências de TI.						
ES9	**Gerencia a configuração.** A empresa dispõe de um repositório/registro das configurações de hardware e software com o objetivo de minimizar e resolver problemas com mais agilidade.						
ES10	**Gerencia os problemas.** Existe uma metodologia de ações corretivas e preventivas para os problemas de TI.						
ES11	**Gerencia os dados.** Define o ciclo de vida da informação, com definição de prazos para disponibilidade, arquivo morto e descarte de acordo com os requisitos do negócio e da legislação.						
ES12	**Gerencia a infra-estrutura.** Existe uma definição dos requisitos físicos e controle do ambiente físico para os equipamentos de TI, incluindo fatores ambientais, de acesso, instalações entre outros.						
ES13	**Gerenciar operações.** Administra o funcionamento das operações de TI						
ME - Medição e monitoramento.							
MO1	**Monitora e avalia a desempenho de TI.** Utiliza indicadores para monitorar e gerenciar o desempenho dos processos de TI.						
MO2	**Monitora e avalia o controle interno.** Estabelece mecanismos de controle interno dos requisitos da área e monitora a sua execução.						
MO3	**Assegura a conformidade aos requisitos externos.** Estabelece processo de revisão dos requisitos de legislação, contratuais e de negócio.						
MO4	**Fornecer governança de TI.** Estabelece um efetivo modelo de governança, que inclui definição da estrutura organizacional, processos, liderança, perfis e responsabilidades, a fim de garantir que os investimentos estejam alinhados às estratégias da organização.						

Quadro 6: Instrumento de avaliação de maturidade da empresa

Fonte: Adaptado do COBIT e CMMI

Na segunda atividade foi aplicado o **Instrumento 2** para identificar os dados envolvendo a aplicação do questionário com a equipe técnica da empresa para verificar as práticas de segurança dos sistemas de informação.

As práticas verificadas foram referenciadas com base na ISO/IEC27002 conforme Quadro 8, mapeadas através do *framework* de integração dos modelos BSC x COBIT X ISO/IEC27002 considerando os requisitos de segurança confidencialidade, integridade e disponibilidade. Eloff e Eloff (2003) propõe uma classificação das práticas em níveis de proteção identificados como **inadequada, mínima, reativa** e **adequada.**

Após um pré-teste com o técnico de TI foi sugerida a inclusão de uma categoria chamada "***Não aplicável N/A***" conforme Quadro 7. Isso se mostrou adequado, pois a norma sugere algumas práticas que não se aplicam no contexto do negócio. As práticas iniciam no número 5, pois como já descrito anteriormente, os capítulos 1 ao 4 são de introdução da norma.

Prática de segurança	***Proteção***				
	1 – inadequada	2 – Mínima	3 – Reativa	4 – Adequada	Não aplicável
5 - Política de segurança da informação (PL).					
5.1.1 Documento da política de segurança da informação.					
5.1.2 Análise crítica da política de segurança da informação.					
6 - Organizando a segurança da informação (OI).					
6.1.1 Comprometimento da direção com a segurança da informação.					
6.1.2 Coordenação da segurança da informação.					
6.1.4 Processo de autorização para os recursos de processamento da informação.					
6.1.5 Acordos de confidencialidade.					
6.1.6 Contato com autoridades.					
6.1.7 Contato com grupos especiais.					
6.1.8 Análise crítica independente de segurança da informação.					
6.2.1 Identificação dos riscos relacionados com partes externas.					
6.2.2 Identificando a segurança da informação, quando tratando com os clientes.					
6.2.3 Identificando segurança da informação nos acordos com terceiros.					
7 - Gestão de ativos (GA).					
7.1.1 Inventário dos ativos.					
7.1.2 Proprietário dos ativos.					
7.2.1 Recomendações para classificação.					
7.2.2 Rótulos e tratamento da informação.					
8- Segurança em recursos humanos (RH).					
8.1.1 Papéis e responsabilidades.					
8.1.2 Seleção.					
8.1.3 Termos e condições de contratação.					
8.2.2 Conscientização, educação e treinamento em segurança da informação.					
8.2.3 Processo disciplinar.					
8.3.1 Encerramento de atividades.					

8.3.3 Retirada de direitos de acesso.					
9 - Segurança física e do ambiente (SA).					
9.1.1 Perímetro de segurança física.					
9.1.2 Controles de entrada física.					
9.1.3 Segurança em escritórios, salas e instalações.					
9.1.4 Proteção contra ameaças externas e do meio ambiente.					
9.1.5 Trabalhando em áreas seguras.					
9.1.6 Acesso do público, áreas de entrega e de carregamento.					
9.2.1 Instalação e proteção do equipamento.					
9.2.2 Utilidades.					
9.2.3 Segurança do cabeamento.					
9.2.4 Manutenção dos equipamentos.					
9.2.5 Segurança de equipamentos fora das dependências da organização.					
9.2.6 Reutilização e alienação segura de equipamentos.					
9.2.7 Remoção de propriedade.					
10 - Gerenciamento das operações e comunicações (GO).					
10.1.1 Documentação dos procedimentos de operação.					
10.1.2 Gestão de mudanças.					
10.1.3 Segregação de funções.					
10.1.4 Separação dos recursos de desenvolvimento, teste e de produção.					
10.2.1 Entrega de serviços.					
10.2.2 Monitoramento e análise crítica de serviços terceirizados.					
10.2.3 Gerenciamento de mudanças para serviços terceirizados.					
10.3.1 Gestão de capacidade.					
10.3.2 Aceitação de sistemas.					
10.4.1 Controles contra códigos maliciosos.					
10.4.2 Controles contra códigos móveis.					
10.5.1 Cópias de segurança das informações.					
10.6.1 Controles de redes.					
10.6.2 Segurança dos serviços de rede.					
10.7.1 Gerenciamento de mídias removíveis.					
10.7.2 Descarte de mídias.					
10.7.3 Procedimentos para tratamento de informação.					
10.7.4 Segurança da documentação dos sistemas.					
10.8.1 Políticas e procedimentos para troca de informações.					
10.8.2 Acordos para a troca de informações.					
10.8.3 Mídias em trânsito.					
10.8.4 Mensagens eletrônicas.					
10.9.1 Comércio eletrônico.					
10.9.2 Transações on-line.					
10.10.1 Registros de auditoria.					
10.10.2 Monitoramento do uso do sistema.					

10.10.3 Proteção das informações dos registros (*log*).					
10.10.4 Registros (l*og*) de administrador e operador.					
10.10.5 Registros (*log*) de falhas.					
10.10.6 Sincronização dos relógios.					
11 - Controle de acessos (CA).					
11.1.1 Política de controle de acesso.					
11.2.1 Registro de usuário.					
11.2.2 Gerenciamento de privilégios.					
11.2.4 Análise crítica dos direitos de acesso de usuário.					
11.3.1 Uso de senhas.					
11.3.2 Equipamento de usuário sem monitoração.					
11.3.3 Política de mesa limpa e tela limpa.					
11.4.1 Política de uso dos serviços de rede.					
11.4.2 Autenticação para conexão externa do usuário.					
11.4.3 Identificação de equipamento em redes.					
11.4.4 Proteção e configuração de portas de diagnóstico remotas.					
11.4.5 Segregação de redes.					
11.4.6 Controle de conexão de rede.					
11.4.7 Controle de roteamento de redes.					
11.5.1 Procedimentos seguros de entrada no sistema (*log-on*).					
11.5.3 Sistema de gerenciamento de senha.					
11.5.4 Uso de utilitários de sistema.					
11.5.5 Desconexão de terminal por inatividade.					
11.5.6 Limitação de horário de conexão.					
11.6.1 Restrição de acesso à informação.					
11.6.2 Isolamento de sistemas sensíveis.					
11.7.1 Computação e comunicação móvel.					
11.7.2 Trabalho remoto.					
12 - Aquisição, desenvolvimento e manutenção de sistemas de informação (AQ).					
12.1.1 Análise e especificação dos requisitos de segurança.					
12.2.1 Validação dos dados de entrada.					
12.2.2 Controle do processamento interno.					
12.2.3 Integridade de mensagens.					
12.2.4 Validação de dados de saída.					
12.3.1 Política para o uso de controles criptográficos.					
12.3.2 Gerenciamento de chaves.					
12.4.1 Controle de software operacional.					
12.4.2 Proteção dos dados para teste de sistema.					
12.4.3 Controle de acesso ao código-fonte de programa.					
12.5.1 Procedimentos para controle de mudanças.					
12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.					
12.5.3 Restrições sobre mudanças em pacotes de software.					

12.5.4 Vazamento de informações.					
12.5.5 Desenvolvimento terceirizado de software.					
12.6.1 Controle de vulnerabilidades técnicas.					
13 - Gestão de incidentes de segurança da informação (GI).					
13.1.1 Notificação de eventos de segurança da informação					
13.1.2 Notificando fragilidades de segurança da informação.					
13.2.1 Responsabilidades e procedimentos.					
13.2.2 Aprendendo com os incidentes de segurança da informação.					
13.2.3 Coleta de evidências.					
14 - Gestão da continuidade do negócio (GC).					
14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio.					
14.1.2 Continuidade de negócios e análise/avaliação de riscos.					
14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação.					
14.1.4 Estrutura do plano de continuidade do negócio.					
14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.					
15 - Conformidade (CF).					
15.1.1 Identificação da legislação vigente.					
15.1.2 Direitos de propriedade intelectual.					
15.1.3 Proteção de registros organizacionais.					
15.1.4 Proteção de dados e privacidade de informações pessoais.					
15.1.5 Prevenção de mau uso de recursos de processamento da informação.					
15.1.6 Regulamentação de controles de criptografia.					
15.2.1 Conformidade com as políticas e normas de segurança da informação.					
15.2.2 Verificação da conformidade técnica.					
15.3.1 Controles de auditoria de sistemas de informação.					
15.3.2 Proteção de ferramentas de auditoria de sistemas de informação.					

Quadro 7: Instrumento de Requisitos da norma ISO/IEC27002 aplicados para equipe técnica.

Fonte: Adaptado da norma ISO/IEC27002.

Na terceira atividade envolvendo o **instrumento** 3 foi realizada a aplicação de uma entrevista conforme Quadro 8 para obter uma visão gerencial em relação aos objetivos de TI para o negócio e aos aspectos relacionados a segurança da informação. Esta entrevista foi realizada com o diretor administrativo financeiro responsável pela TI.

Os objetivos que foram verificados estão relacionados com os que têm impacto *Primário* ou *Secundário* nos requisitos de segurança, isso contribuindo para a compreensão da segurança da informação na visão da gestão da empresa para

posterior análise e alinhamento estratégico. Com o objetivo de direcionar e proporcionar objetividade para a entrevista foi realizada uma adaptação sugerindo algumas questões para cada objetivo de TI. Para não limitar a investigação, não necessariamente esta entrevista se limitou somente a estas questões.

Objetivo de TI	Questão
1	**Alinhamento entre estratégia de negócio e TI.** • Como a empresa desenvolve o planejamento estratégico? • A gerência de TI participa do planejamento estratégico? • Como a TI desenvolve o seu planejamento estratégico? • O planejamento estratégico de TI é realizado com base no planejamento estratégico da empresa? • A área de TI possui um plano de ação? • A área de TI possui indicadores para avaliar o seu desempenho?
3	**Garantir a satisfação dos usuários finais com bons níveis de serviços.** • Existe um controle das demandas dos usuários com prioridades (D)? • São negociados prazos com os usuários (D)? • Os serviços são entregues nos prazos combinados (D)? • Existe uma iteração com o usuário durante a execução dos serviços (C, I)? • Os serviços entregues atendem os objetivos dos usuários inicialmente propostos (D, I, C)?
4	**Otimizar o uso da informação.** • Os recursos de TI atendem as necessidades dos usuários (D)? • As informações são suficientes para os usuários (D, I, C)? • Existe um modelo com infra-estrutura de TI (I, C)? • São realizadas análises para melhoria dos recursos de TI (D, I, C)?
5	**Criar agilidade de TI.** • As informações são disponibilizadas no tempo certo (D)? • As funções e responsabilidades de TI estão definidas. (D, I, C)? • Como é a estrutura organizacional de TI (D, I, C)? • Os responsáveis pelas atividades de TI são capacitados para suas tarefas (D, I, C)?
10	**Garantir satisfação mútua em relacionamento com terceiros.** • Existem serviços de TI terceirizados? Quais são eles? (D, I, C) • Como são realizadas as contratações de terceiros (D, I, C)? • Existe um procedimento para contratação a de serviços terceirizados, ex, uso de RFP, RFI, visitas a clientes dos fornecedores, etc (D, I, C)? • São estabelecidos contratos com terceiros (C, D, I)? • Os contratos englobam cláusulas de confidencialidade sobre as informações da empresa (C)? • Os contratos estabelecem níveis de serviços a serem entregues (D, I, C)? • Há um processo de revisão conjunta e da melhoria das operações (D, I, C)?
11	**Garantir integração das aplicações com os processos de negócios.** • Como é a documentação dos sistemas (manuais, procedimentos, etc) (D, I, C)? • As aplicações atendem os principais processos de negócio (D)? • Os sistemas são flexíveis para mudanças (D)?
14	**Responder pelos ativos de TI e protegê-los.** • Existem responsáveis pela infra-estrutura de TI (D)? • Quem é responsável pelas aplicações da empresa (D, I)? • Existe e como é realizada a rotina de backup (D, I, C)? • As informações são protegidas por senhas (I, C)? • Existe um plano de manutenção da infra-estrutura de TI (D)?
16	**Reduzir defeitos e retrabalho nas entregas de soluções e serviços.** • São feitas especificações para desenvolvimento de novas soluções (D, I,C)? • São realizados testes adequados antes da entrega das soluções para os usuários (D, I, C)?
17	**Garantir o cumprimento dos objetivos de TI.** • Como são estabelecidos os objetivos de TI? • Existe um plano de ação da TI com prazos e responsáveis (D)?
18	**Estabelecer clareza no impacto de riscos do negócio em relação a objetivos e recursos de TI.** • A TI conhece os riscos potenciais dos sistemas e equipamentos (D, I, C)? • É mantido um quadro de gestão de riscos (D, I, C)?

19	**Assegurar que informações críticas e confidenciais são inacessíveis a aqueles que não devem ter acesso a elas.** • O acesso as informações é através de senhas (C)? • Existe uma política de troca de senhas (C)?
20	**Garantir que as informações de negócio e transações automatizadas são confiáveis.** • Antes das entregas, existe uma rotina de teste de informações (I)? • As informações/relatórios são validadas antes da entrega (I)
21	**Garantir que os serviços e infra-estrutura de TI resistam a falhas em função de erros, ataques deliberados ou desastres.** • Existem mecanismos de contingência nos servidores da empresa (D)? • Existem equipamentos sobressalentes para os usuários (D)? • Existe algum sistema de monitoramento e auditoria dos servidores (D)? • Existe um sistema de antivírus (I, C, D)?
22	**Garantir impacto mínimo no negócio no caso de uma interrupção ou anormalidade em um serviço de TI.** • Como são realizados os serviços de manutenção dos servidores (D)? • Existe um plano de manutenções (D)? • Existe um plano de contingência dos serviços essenciais (D)?
23	**Assegurar que os serviços de TI estão disponíveis quando solicitados.** • Quais são os serviços considerados essenciais (D)? • Existe um serviço para registro de solicitações?
25	**Entregar projetos no prazo e nos orçamento previstos, observando padrões de qualidade.** • Existe uma rotina/metodologia de gestão de projetos de TI (D, I, C)?
26	**Manter a integridade da informação e da infra-estrutura.**
27	**Garantir que a TI observe a legislação, regulamentações e contratos.** • Os gestores de TI conhecem as legislações aplicáveis ao negócio?
D – Disponibilidade, **I –** Integridade, **C -** Confidencialidade	

Quadro 8: Instrumento de Questões para entrevista.

Fonte: Adaptado do ITGI

Na quarta e última etapa de Coleta de dados foi realizada a recuperação documental através da aplicação do **Instrumento 4**. O objetivo desta etapa foi de confirmar informações eventualmente conflitantes ou que não tenham sido identificadas pelos três instrumentos anteriores. Nesta análise documental foram considerados:

1 - Documentos de planejamento estratégico;

2 - As políticas de RH e TI;

3 – Os procedimentos de processos organizacionais e de TI;

4 – As atas de reuniões estratégicas e gerenciais;

5 - Os quadros de indicadores;

6 - Os mecanismos de acompanhamento de planos de ação e de indicadores;

7 - Os relatórios de auditoria ISO9000;

8 - Os contratos com terceiros e documentação técnica da área de TI.

Tendo em vista os objetivos apresentados nesta dissertação, a análise dos resultados foi realizada através do instrumento apresentado no Quadro 9. Nesta análise foram considerados os objetivos genéricos de TI com **impacto primário** ou **secundário** nos requisitos de segurança Confiabilidade (C), Integridade (I) e Disponibilidade (D).

<table>
<tr><td colspan="5">Objetivo genérico de tecnologia da informação (TI):</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td>Objetivo genérico de negócio:</td><td>Mapeados</td><td>Não mapeados</td><td>Domínios da Norma</td><td>C, I, D</td></tr>
<tr><td colspan="5">Documentação analisada:</td></tr>
<tr><td colspan="5">Respostas da entrevista:</td></tr>
<tr><td colspan="5">Práticas de segurança:</td></tr>
</table>

Quadro 9: Instrumento de análise de resultados da aplicação dos modelos de GTI

Fonte: Elaborado pelo autor

4 CASO DE ESTUDO

O estudo foi realizado em uma empresa de automação localizada em São Leopoldo, RS com 46 anos de atuação de mercado. A empresa tem como missão fornecer soluções para automação de válvulas e é pioneira na fabricação de atuadores elétricos no Brasil.

Em 2007 a empresa conquistou o prêmio de empresa inovadora segundo os critérios da Financiadora de Estudos e Projetos do Governo Federal (FINEP).

O caso se mostrou apropriado para resposta à questão problema e atendimento dos objetivos, pois os aspectos de segurança da informação relacionados aos produtos e serviços oferecidos pela empresa são de significativa à importância estratégica. Isso é devido ao fato que a empresa está se tornando muito dependente de sistemas de informação e qualquer pequeno problema de segurança da informação pode ocasionar resultados preocupantes ao próprio modelo de negócio desenvolvido pela mesma e até mesmo à cadeia de valores que a mesma está inserida.

Este tipo de empresa é muito dinâmica em sua atuação devido às mudanças continuadas que o mercado internacional impõe ao processo de aprimoramento tecnológico.

4.1 O Setor de Automação Industrial

A automação de processos industriais envolve uma extensa cadeia de atividades que se inicia na pesquisa científica e termina na entrada em operação da unidade produtiva. A evolução tecnológica do setor é constante e não há duas plantas iguais e, portanto, sua automação dificilmente é passível de padronização. Os sistemas legados são diferentes e requerem sempre adaptações para compatibilizar equipamentos, aplicativos e infra-estrutura de comunicação, novos

com os existentes. Isso faz com que as atividades relativas à automação de processos industriais demandem mão de obra de elevada qualificação e investimentos em pesquisa e desenvolvimento. O Quadro 10 mostra as principais empresas no mercado nacional ligadas à automação industrial. De acordo com a Associação Brasileira da Indústria Elétrica e Eletrônica (Abinee), o faturamento do setor em 2007 foi de R$ 3,1 bilhões.

EMPRESA	LINHA DE PRODUTOS
Altus	CLPs e soluções completas
Atan	Provedor de *software* e soluções completas
Atos	CLPs e soluções completas
BCM	CLPs e outros dispositivos de controle
Coester	Atuadores de válvulas
Ecil	Dispositivos de controle para sistemas elétricos
Elipse	Software supervisório (SCADA)
Novus	Dispositivos de controle
Presys	Dispositivos de controle
Sense	Sensores
Smar	Dispositivos de controle e soluções completas
Trisolutions	Provedor de *software* e soluções completas
WEG	Inversores de freqüência e soluções completas

Quadro 10: Principais fabricantes nacionais ligados a automação industrial
Fonte: BNDES Setorial 2008, Rio de Janeiro, n. 28, p. 218

4.2 Empresa pesquisada: Coester Automação S.A.

Conforme o manual da qualidade da empresa, a COESTER foi fundada em 1963 e se dedicava inicialmente a equipamentos de comunicação para empresas e escritórios. Em meados da década de 60, a partir do 1º Plano de Construção Naval Brasileiro a empresa direcionou suas atividades para projetos e fabricação de Sistemas de Controle para Navios. Atualmente mais de 350 navios são equipados com sistemas da empresa entre os quais as 4 corvetas da Marinha de Guerra Brasileira. Em 1975 a empresa projetou e forneceu os primeiros atuadores elétricos fabricados no Brasil em um consórcio MCC (Michelleto, Coester, Comtei).

O consórcio terminou em 1980, quando a empresa passou a produzir sua própria linha de atuadores. Em 1977 foi adquirido o controle acionário da METAÚRGICA ALPAIR S.A, em São Leopoldo o que ocasionou a mudança da COESTER de Porto Alegre para São Leopoldo e na centralização de todas as atividades em uma única planta.

No final dos anos 80 devido ao colapso do setor naval brasileiro, a COESTER diversificou suas atividades para compensar a perda quase total de seu principal mercado. Em 1997, foi implementado um processo de reestruturação e terceirização. A partir desta reestruturação, o foco de atividade da empresa passou a ser o de AUTOMAÇÃO industrial. Atualmente a empresa conta com 100 colaborados em sua força de trabalho e tem representações comerciais em todo o país. A empresa também esta em fase de implantação de um programa de internacionalização e com isso mantém atividades comerciais com a Argentina, Chile, Colombia, Equador, México, Perú e Venezuela.

Também pertencem ao GRUPO COESTER:

- AEROMÓVEL BRASIL S/A: empresa que conduz o projeto do AEROMÓVEL, tecnologia de transporte.
- COESTER PESQUISAS E PARTICIPAÇÕES LTDA, holding do grupo.

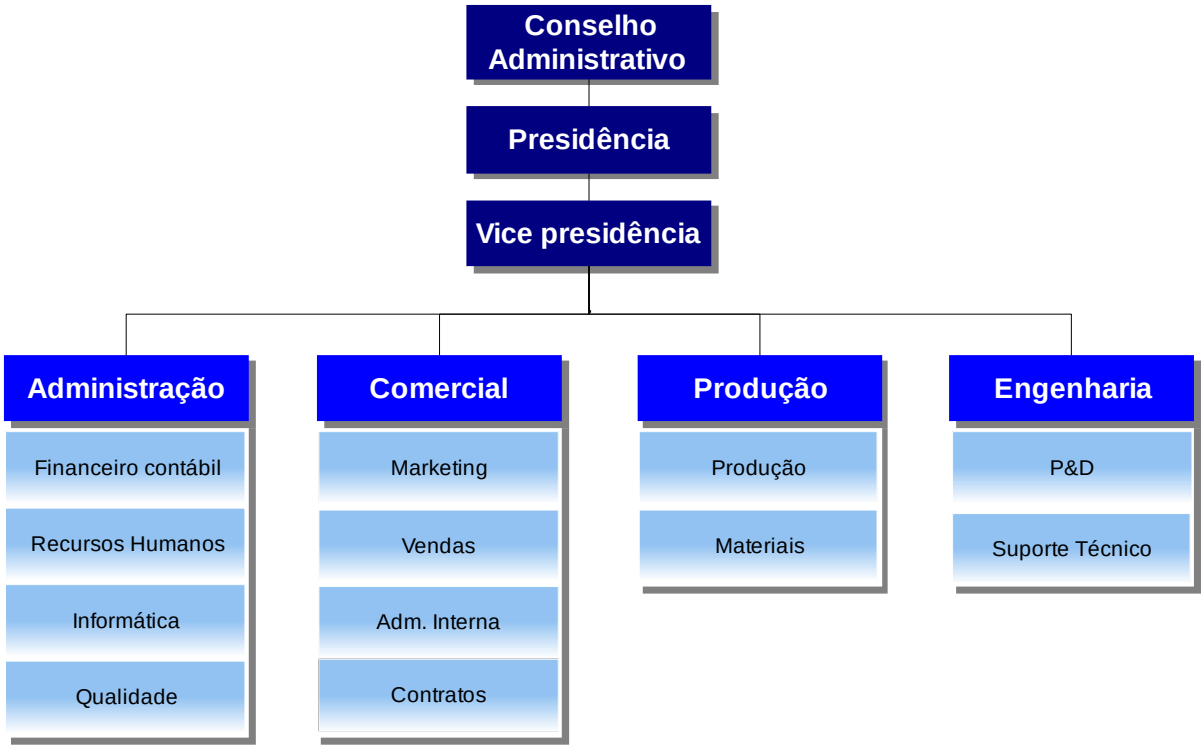


Figura 9: Organograma da empresa estudada

Fonte: Planejamento estratégico da empresa

Como requisito do mercado de automação os produtos e soluções comercializados pela empresa demandam um alto esforço e constantes investimentos em Pesquisa e Desenvolvimento para atingir um grau de inovação em produto intrínseco deste mercado.

Com isso a segurança da informação principalmente em proteção dos dados das áreas comercial, projetos e produção passa a ser um requisito estratégico. Atualmente a empresa dispõe de recursos de TI e sistemas de informação distribuídos em todas as áreas da organização. Com o objetivo de se tornar mais competitiva nos anos de 2006 e 2007 a empresa passou por um processo de implantação de ERP.

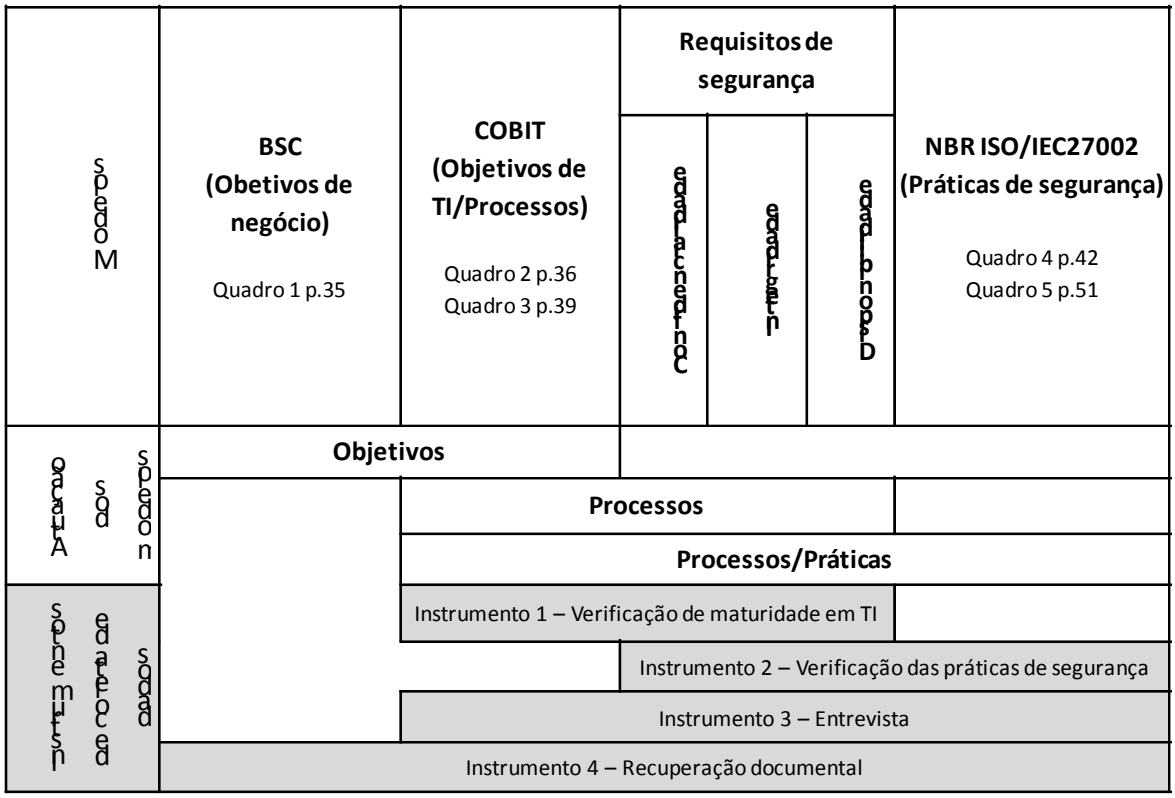
4.3 Coleta de dados

A coleta de dados compreendeu 4 etapas que seguiram o *framework* desenvolvido que integra os três níveis organizacionais, estratégico, tático e

operacional. Estas etapas estão descritas na continuação já com os resultados encontrados.

Etapa 1: Avaliação dos níveis de maturidade dos processos de TI

A primeira etapa desenvolvida foi a aplicação do **instrumento 1,** a aplicação de um questionário baseado nos processos do modelo COBIT envolvendo aspectos de segurança com a equipe gerencial para avaliar o grau de maturidade da empresa. Na continuação é reapresentado o *framework* de integração dos modelos com a finalidade de posicionar o instrumento de avaliação do grau de maturidade da empresa estudada, instrumento este representado na figura 8. Esse *framework* também é reapresentado anteriormente a aplicação de cada um dos outros instrumentos.



O questionário foi aplicado a quatro gestores, são eles; o Diretor Administrativo, o Diretor Industrial, o Diretor Comercial e o Gerente de P&D. Esta escolha ocorreu em função das atividades estratégicas desenvolvidas na empresa por estes profissionais, assim como a abrangência dos mesmos em todos os processos principais da empresa. Primeiramente foi realizado um pré-teste com o diretor Administrativo que sugeriu um texto complementar explicando cada processo do COBIT.

Os gráficos com os resultados da aplicação dos questionários para verificar o grau de maturidade podem ser observados nas Figuras 9, 10, 11, 12 e 13 a seguir.

O primeiro gráfico de maturidade referente ao modelo COBIT foi respondido pelo Diretor Administrativo, conforme representação na continuidade.

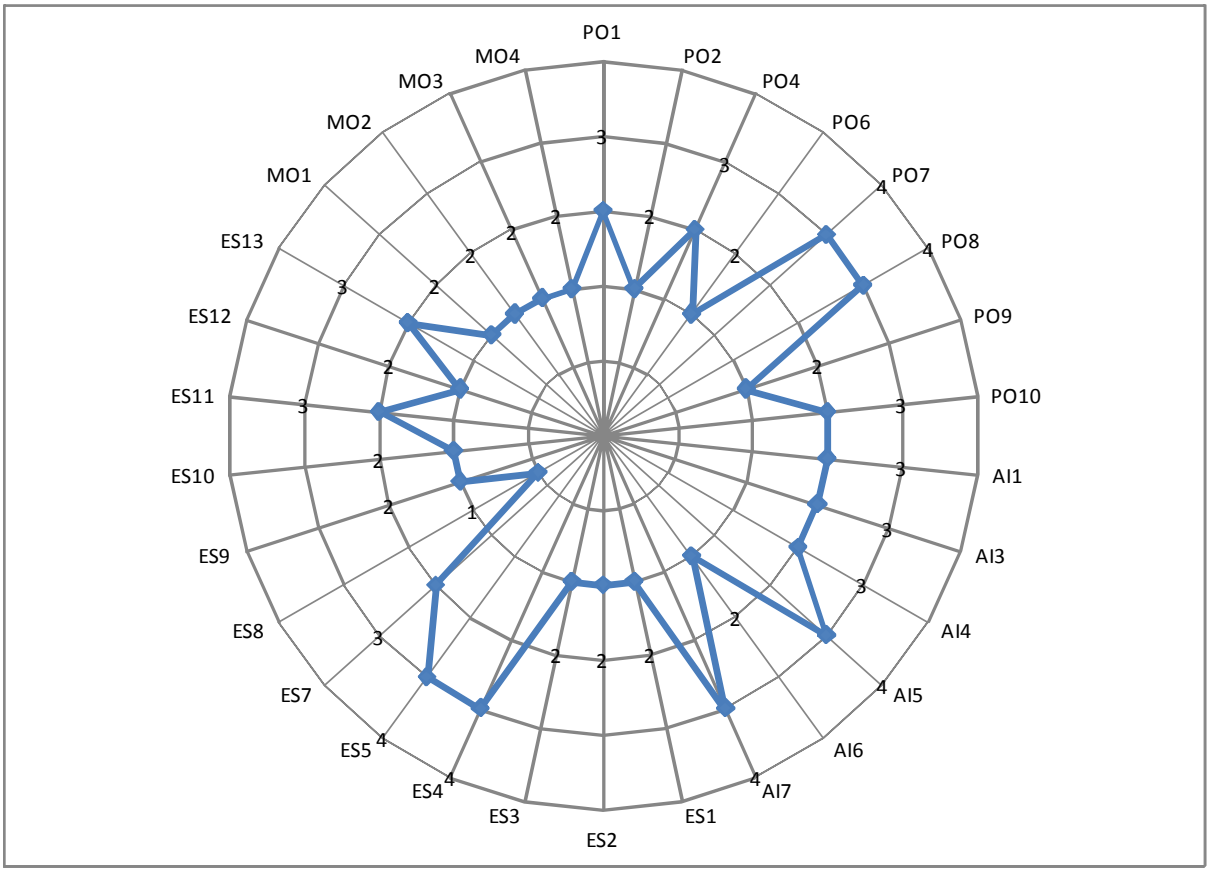


Figura 10: Maturidade da empresa em relação aos processos COBIT – Diretor administrativo

Este gráfico anteriormente representado evidencia os resultados do nível de maturidade da empresa em relação aos processos do COBIT, aplicado junto ao Diretor Administrativo. Com ele é possível visualizar que o nível de maturidade mais

significativo encontrado é o nível que representa o processo de PO 07 - Gerenciar recursos humanos, PO8 - Gerenciar qualidade, AI5 - Obter recursos de TI, AI7- Instalar e certificar soluções e mudanças, ES4 - Garantir continuidade dos serviços e ES5 - Garantir segurança dos sistemas.

O segundo gráfico de maturidade referente ao modelo COBIT foi respondido pelo Diretor Industrial, conforme representação na continuidade.

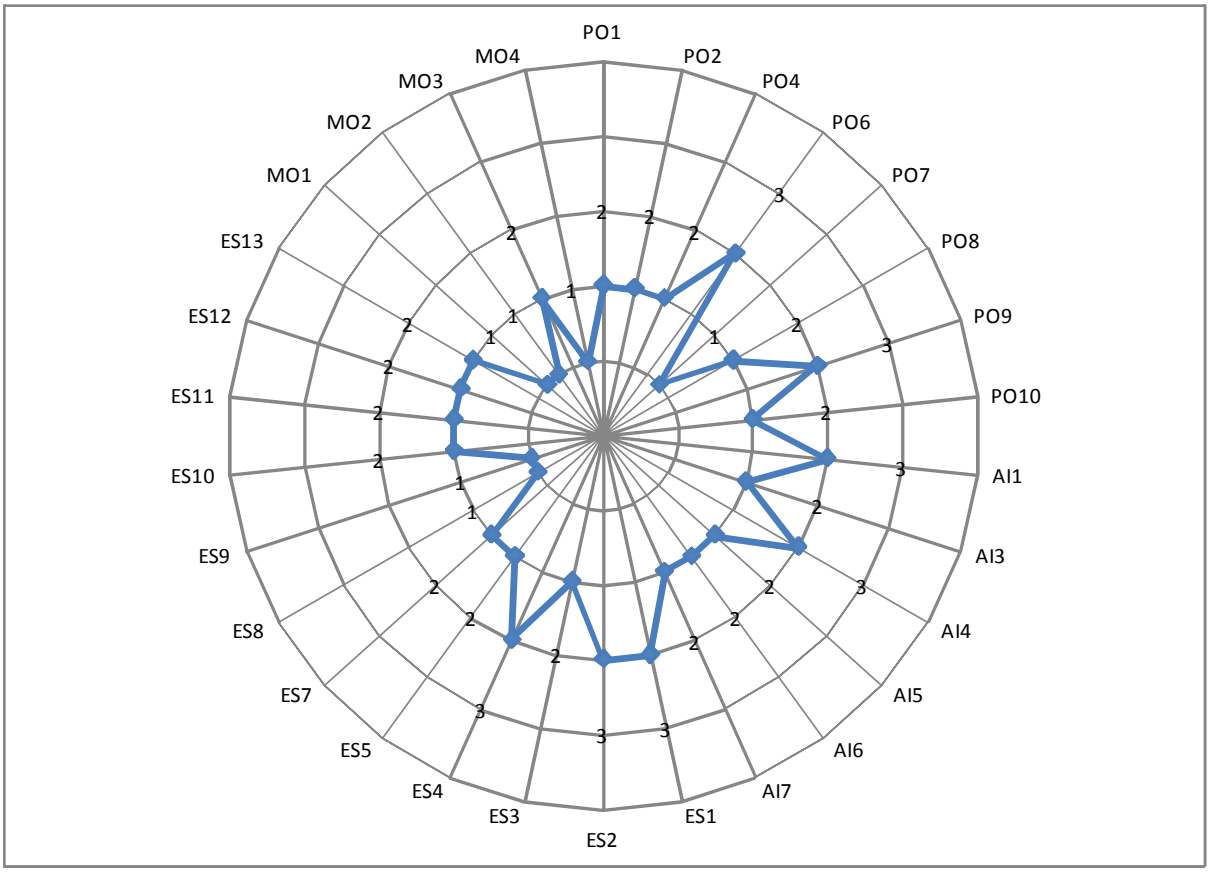


Figura 11: Maturidade da empresa em relação aos processos COBIT – Diretor industrial

Com o gráfico é possível identificar que os processos com maior significância ou maior maturidade do ponto de vista do diretor industrial são PO6 - Comunicar metas e diretrizes gerenciais, PO9 - Avaliar e gerenciar riscos, AI1 - Identificar soluções, AI4 – Desenvolver e manter procedimentos de TI, ES1 – Definir níveis de serviços, ES2 – Gerenciar serviços de terceiros e ES4 - Garantir continuidade dos serviços.

O terceiro gráfico de maturidade referente ao modelo COBIT foi respondido pelo diretor comercial, conforme representação na continuidade.

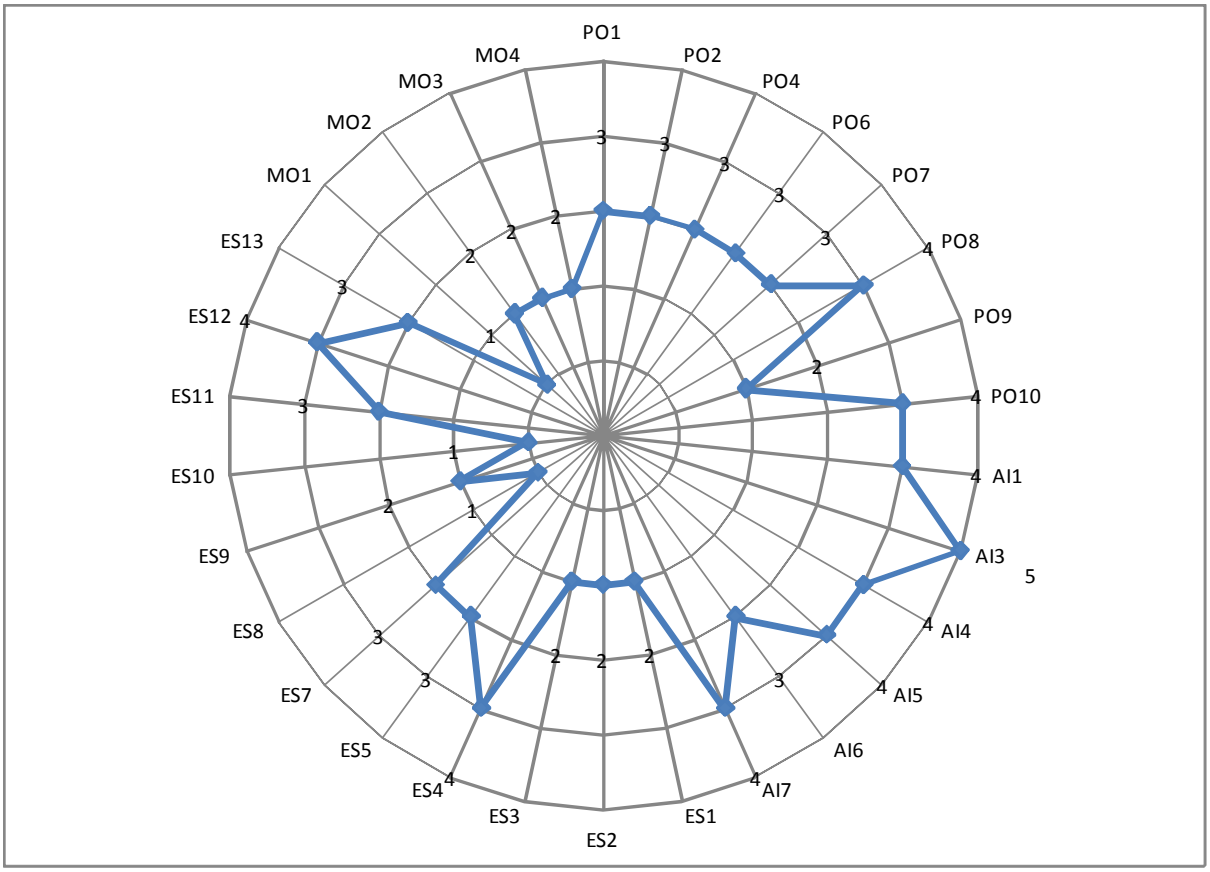


Figura 12: Maturidade da empresa em relação aos processos COBIT – Diretor comercial

O gráfico permite conhecer que os processos com maior maturidade do ponto de vista do diretor comercial são PO8 - Gerenciar qualidade, PO10 - Gerenciar projetos, AI1 - Identificar soluções, AI4 – Desenvolver e manter procedimentos de TI, AI5 - Obter recursos de TI, AI7 - Instalar e certificar soluções e mudanças, ES8 - Gerenciar central de serviços e incidentes e ES12 - Gerenciar os ambientes físicos.

O quarto gráfico de maturidade referente ao modelo COBIT foi respondido pelo gerente de P&D, conforme representação na continuidade.

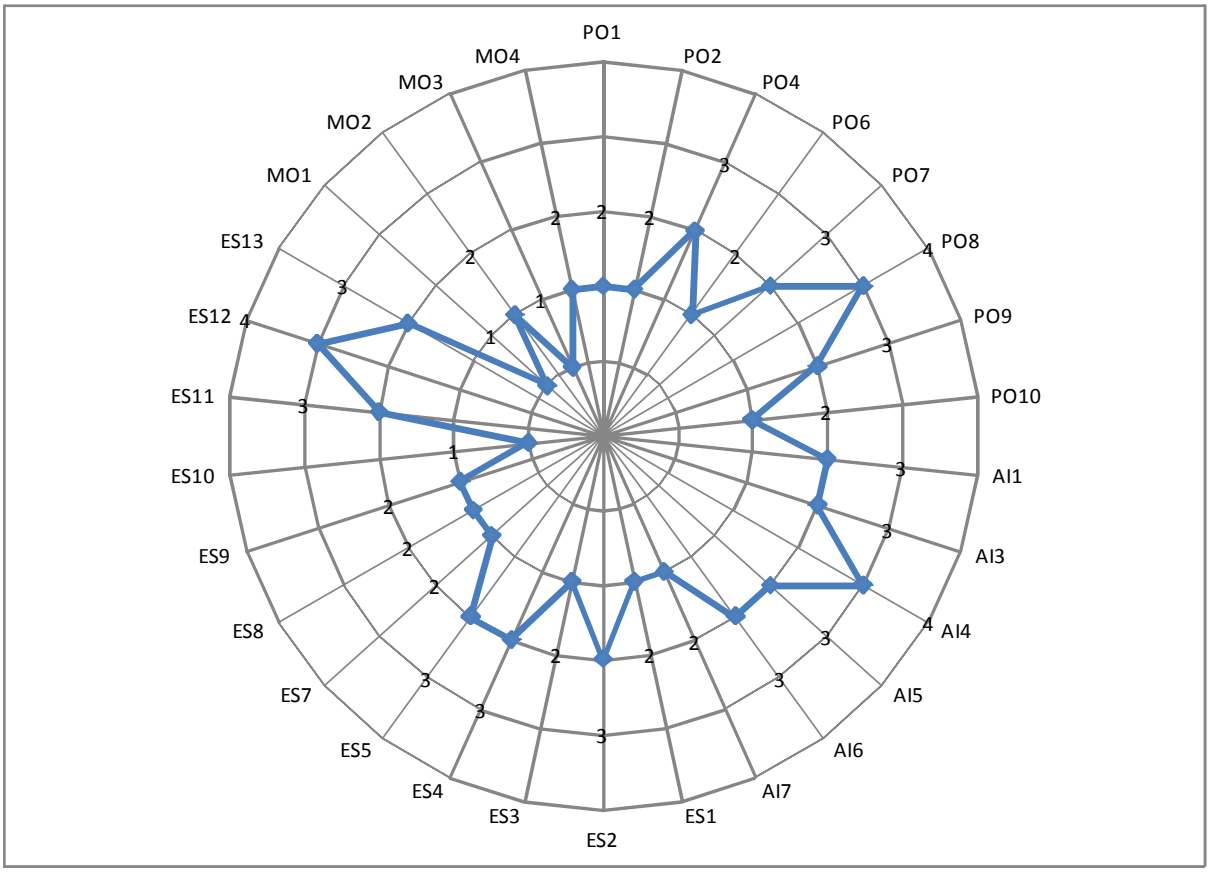


Figura 13: Maturidade da empresa em relação aos processos COBIT – Gerente de P&D

O gráfico mostra que os processos com maior maturidade do ponto de vista do gerente de P&D são PO8 - Gerenciar qualidade, AI4 - Desenvolver e manter procedimentos de TI e ES12 - Gerenciar os ambientes físicos.

O quinto gráfico representa a média dos resultados da maturidade da empresa referente ao modelo COBIT, conforme representação na continuidade.

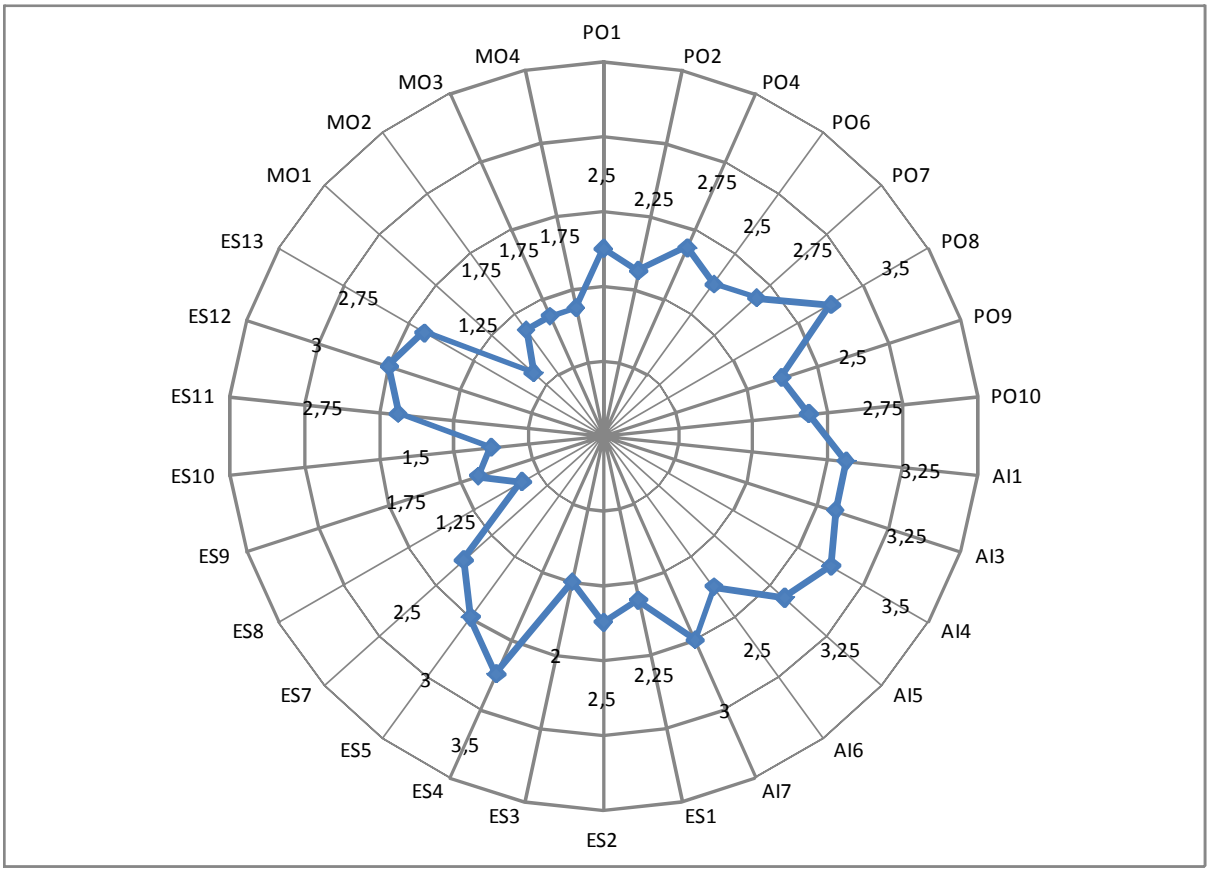


Figura 14: Maturidade da empresa em relação aos processos COBIT – Média

A média do nível de maturidade permite compreender que os processos de TI da empresa estuda possuem 29 processos e que separados por 5 níveis o alcance dos mesmos corresponderam os resultados conforme apresentados na continuação.

Maturidade dos processos em nível Inicial:

ES8 - Gerenciar central de serviços e incidentes
Resultado = 1,25

MO1 - Monitorar e avaliar a desempenho de TI
Resultado = 1,25

ES10 - Gerenciar problemas
Resultado = 1,5

ES9 - Gerenciar a configuração
Resultado = 1,75

MO2 - Monitorar e avaliar o controle interno
Resultado = 1,75

MO3 - Assegurar a conformidade regulatória
Resultado = 1,75

MO4 - Promover governança de TI
Resultado = 1,75

A maturidade dos processos em nível repetitivo, mas intuitivo foram identificados e caracterizados na empresa estudada conforme segue:

ES3 - Gerenciar desempenho e capacidade
Resultado = 2

ES1 - Definir níveis de serviços
Resultado = 2,25

PO2 - Definir a arquitetura de informação
Resultado = 2,25

AI6 - Gerenciar mudanças
Resultado = 2,5

ES2 - Gerenciar serviços de terceiros
Resultado = 2,5

ES7 - Educar e treinar usuários
Resultado = 2,5

PO1 - Definir um plano estratégico de TI
Resultado = 2,5

PO6 - Comunicar metas e diretrizes gerenciais
Resultado = 2,5

PO9 - Avaliar e gerenciar riscos
Resultado = 2,5

ES11 - Gerenciar dados
Resultado = 2,75
ES13 - Gerenciar operações
Resultado = 2,75

PO10 - Gerenciar projetos
Resultado = 2,75

PO4 - Definir processos de TI, Organização e relacionamentos
Resultado = 2,75

PO7 - Gerenciar recursos humanos
Resultado = 2,75

Em relação à maturidade dos processos em nível Definido foram identificados os seguintes resultados:

AI7 - Instalar e certificar soluções e mudanças
Resultado = 3

ES12 - Gerenciar os ambientes físicos
Resultado = 3

ES5 - Garantir segurança dos sistemas
Resultado = 3

AI1 - Identificar soluções
Resultado = 3,25

AI3 - Adquirir e manter arquitetura tecnológica
Resultado = 3,25

AI5 - Obter recursos de TI
Resultado = 3,25

AI4 - Desenvolver e manter procedimentos de TI
Resultado = 3,5

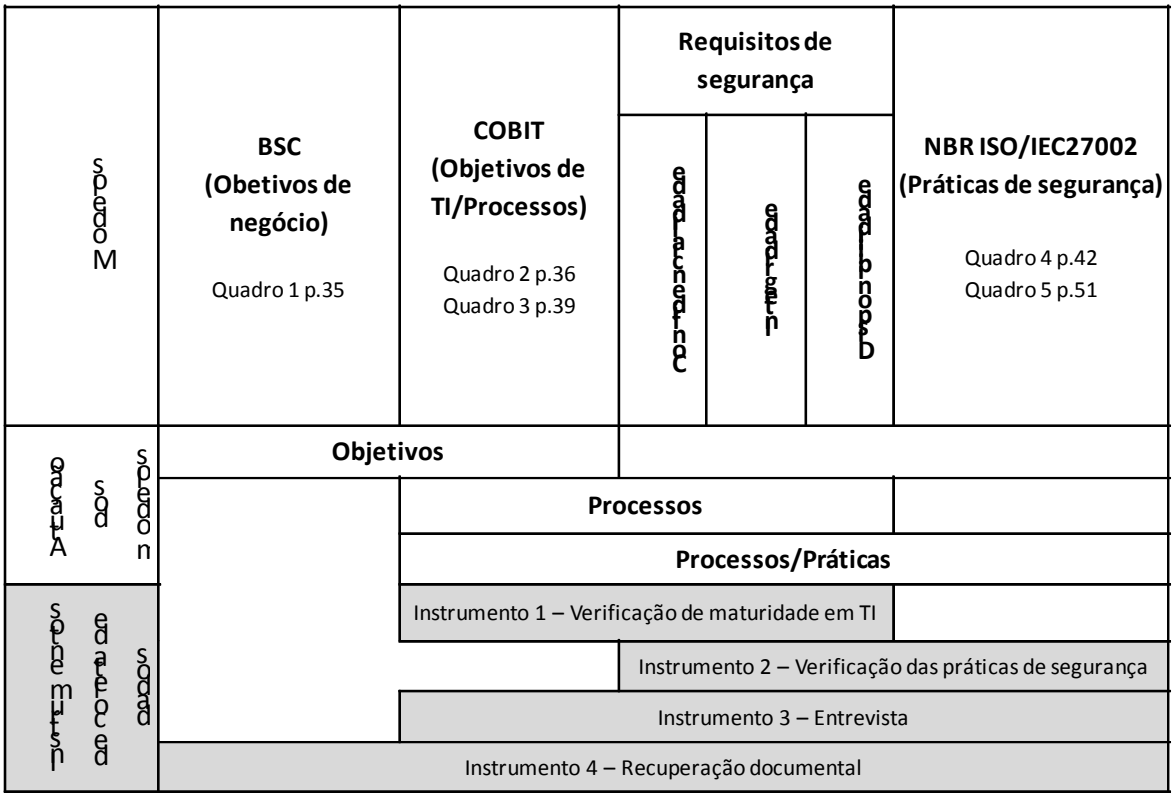
ES4 - Garantir continuidade dos serviços
Resultado = 3,5

PO8 - Gerenciar qualidade
Resultado = 3,5

A análise deste resultado é realizada posteriormente para cada objetivo de TI.

Etapa 2: Verificação do nível de proteção das práticas de segurança

A segunda etapa foi a aplicação do **instrumento 2**, questionário para verificar o nível de proteção das práticas de segurança recomendadas pela ISO/IEC27002. Este instrumento foi aplicado ao técnico interno responsável pelo suporte e a empresa terceirizada que fornece serviços de suporte a rede e servidores da empresa. Para uma melhor interpretação das práticas foi enviado juntamente com o questionário a norma ISO/IEC27007.

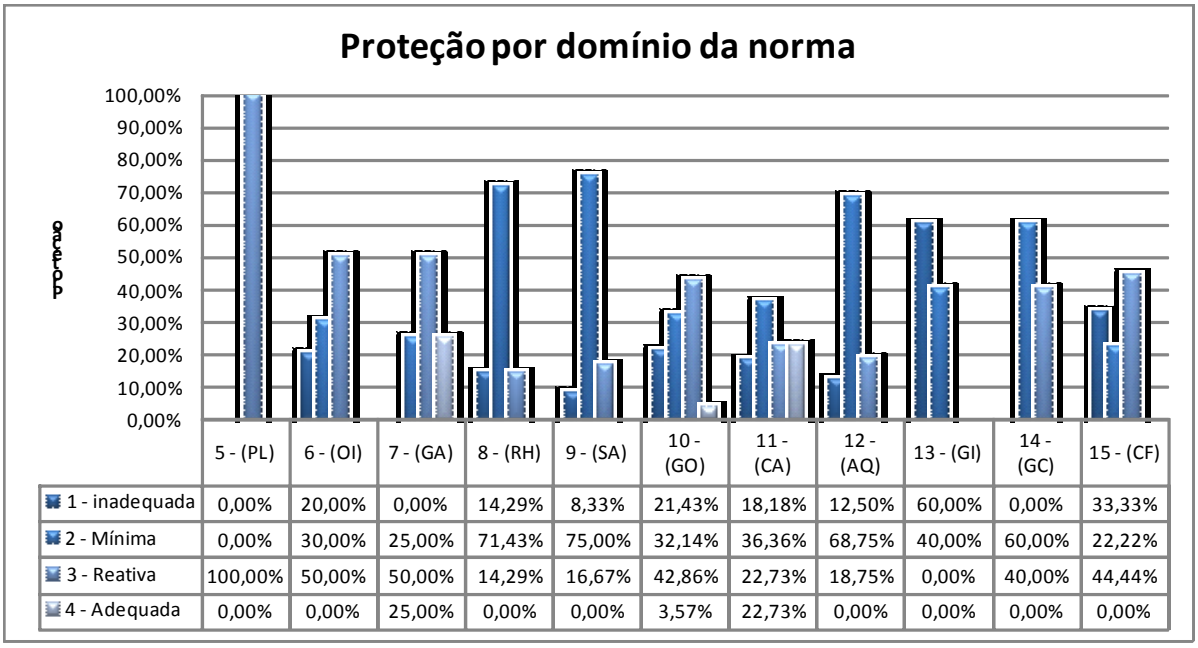


Os gráficos com os resultados por domínio da norma dos questionários podem ser observados nas Figuras 14, 15 e 16 a seguir. As respostas dos questionários podem ser observadas no Anexo B.

Domínios da norma (mantido início no item 5 devido que o intervalo de 1 a 4 é somente introdutório):

5 - (PL) - Política de segurança da informação.
6 - (OI) - Organizando a segurança da informação.
7 - (GA) - Gestão de ativos.
8 - (RH) - Segurança em recursos humanos.
9 - (SA) - Segurança física e do ambiente.
10 - (GO) - Gerenciamento das operações e comunicações.
11 - (CA) - Controle de acessos.
12 - (AQ) - Aquisição, desenvolvimento e manutenção de sistemas de informação.
13 - (GI) - Gestão de incidentes de segurança da informação.
14 - (GC) - Gestão da continuidade do negócio.
15 - (CF) – Conformidade.

O primeiro gráfico se refere ao grau de proteção referente às práticas da norma ISO/IEC 27002 e foi respondido pelo técnico interno responsável pelo suporte. Este profissional está habilitado para gerencia e identificar qualquer questão envolvendo a parte técnica de segurança da informação. Esses resultados estão representados na continuidade.



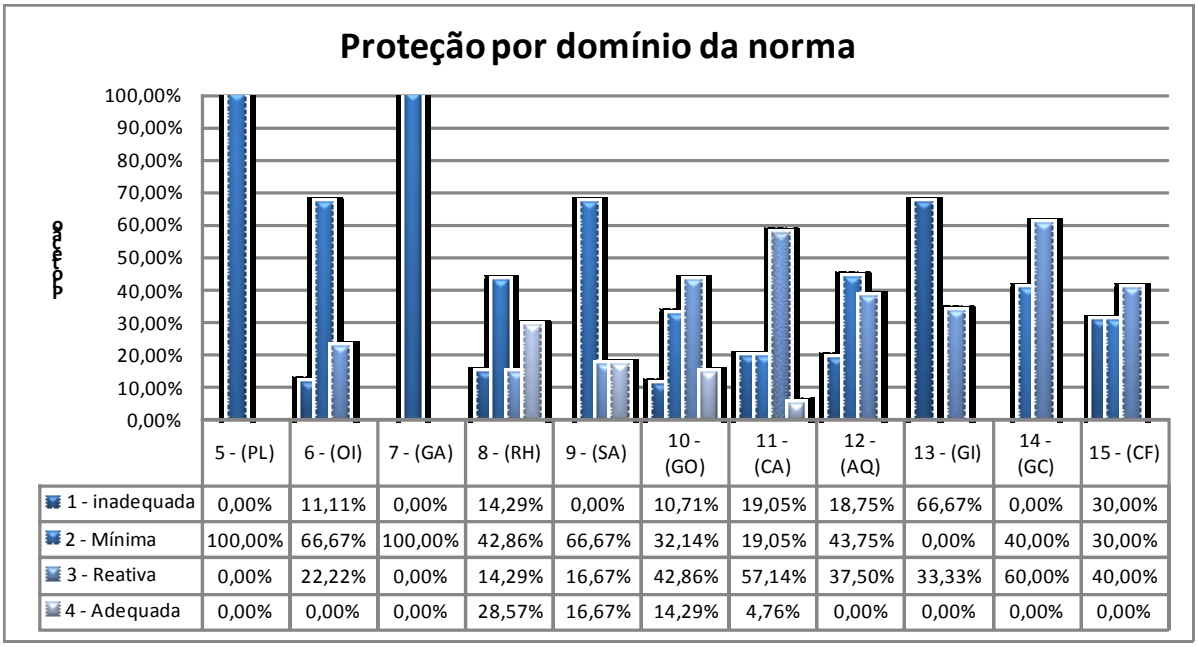
	5 - (PL)	6 - (OI)	7 - (GA)	8 - (RH)	9 - (SA)	10 - (GO)	11 - (CA)	12 - (AQ)	13 - (GI)	14 - (GC)	15 - (CF)
1 - inadequada	0,00%	20,00%	0,00%	14,29%	8,33%	21,43%	18,18%	12,50%	60,00%	0,00%	33,33%
2 - Mínima	0,00%	30,00%	25,00%	71,43%	75,00%	32,14%	36,36%	68,75%	40,00%	60,00%	22,22%
3 - Reativa	100,00%	50,00%	50,00%	14,29%	16,67%	42,86%	22,73%	18,75%	0,00%	40,00%	44,44%
4 - Adequada	0,00%	0,00%	25,00%	0,00%	0,00%	3,57%	22,73%	0,00%	0,00%	0,00%	0,00%

Figura 15: Proteção dos domínios da ISO/IEC 27002 na empresa pesquisada – Técnico interno

Como a proposta deste trabalho é de realizar uma abordagem estratégica da segurança, os resultados da aplicação deste instrumento serão analisados na sequencia a partir dos objetivos de TI para o negócio.

O segundo gráfico do grau de proteção referente as práticas da norma ISO/IEC 27002 foi respondido pela empresa terceirizada que fornece serviços de suporte a rede e servidores da empresa, conforme representação na continuidade.

Essa empresa terceirizada fornece serviços de suporte a rede e servidores e conhece profundamente os aspectos técnicos envolvendo a segurança.

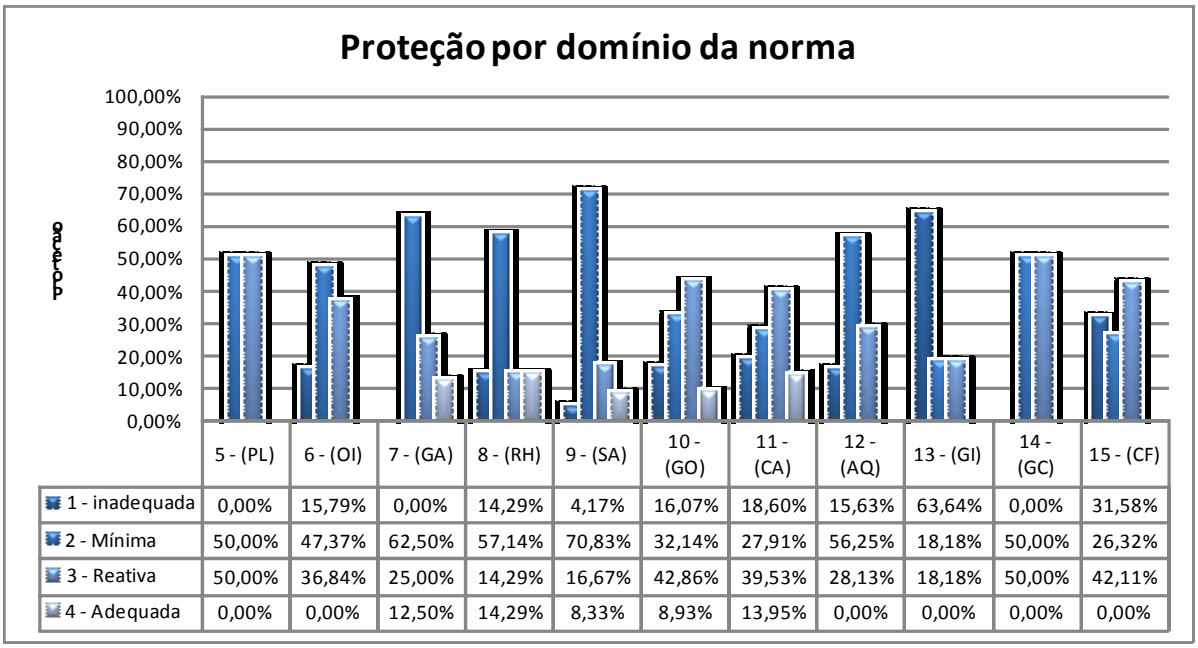


	5 - (PL)	6 - (OI)	7 - (GA)	8 - (RH)	9 - (SA)	10 - (GO)	11 - (CA)	12 - (AQ)	13 - (GI)	14 - (GC)	15 - (CF)
1 - inadequada	0,00%	11,11%	0,00%	14,29%	0,00%	10,71%	19,05%	18,75%	66,67%	0,00%	30,00%
2 - Mínima	100,00%	66,67%	100,00%	42,86%	66,67%	32,14%	19,05%	43,75%	0,00%	40,00%	30,00%
3 - Reativa	0,00%	22,22%	0,00%	14,29%	16,67%	42,86%	57,14%	37,50%	33,33%	60,00%	40,00%
4 - Adequada	0,00%	0,00%	0,00%	28,57%	16,67%	14,29%	4,76%	0,00%	0,00%	0,00%	0,00%

Figura 16: Proteção dos domínios da ISO/IEC 27002 na empresa pesquisada – Empresa terceirizada.

Como a proposta deste trabalho é de realizar uma abordagem estratégica da segurança, os resultados da aplicação deste instrumento serão analisados na sequencia a partir dos objetivos de TI para o negócio.

O terceiro gráfico representa a média do grau de proteção referente as práticas da norma ISO/IEC 27002 da empresa, conforme representação na continuidade.

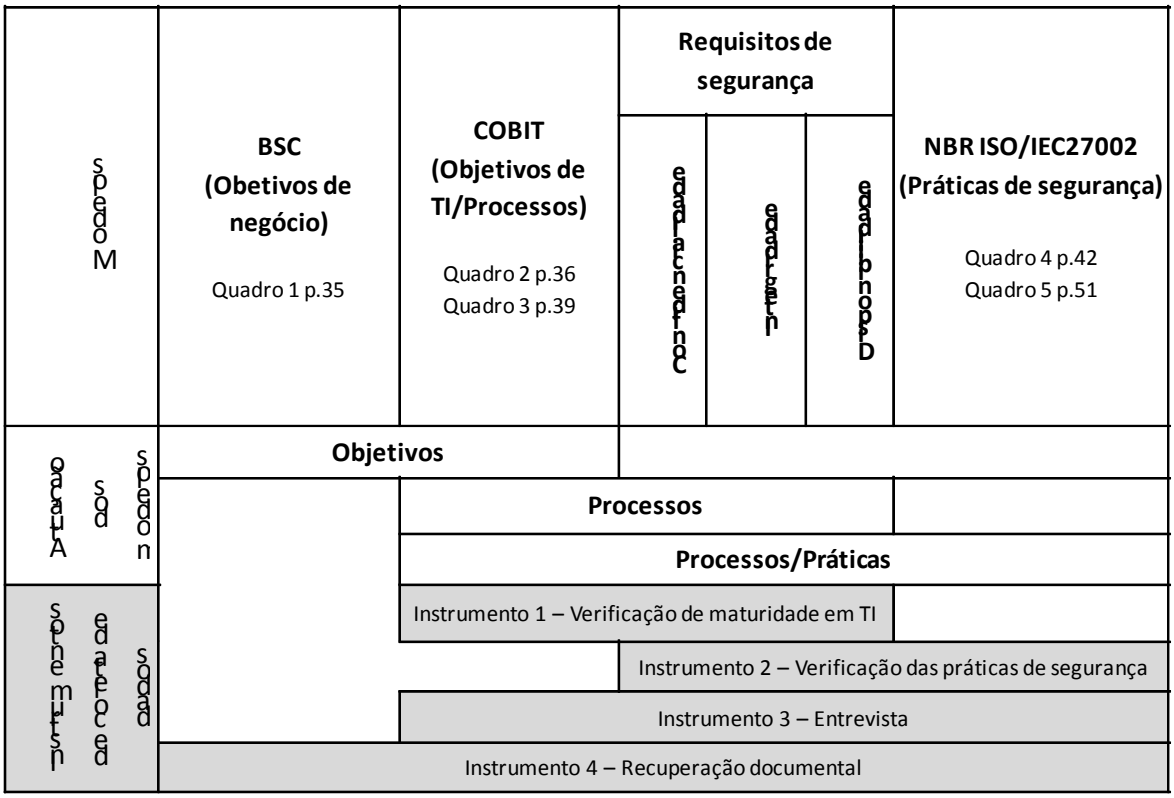


	5 - (PL)	6 - (OI)	7 - (GA)	8 - (RH)	9 - (SA)	10 - (GO)	11 - (CA)	12 - (AQ)	13 - (GI)	14 - (GC)	15 - (CF)
1 - inadequada	0,00%	15,79%	0,00%	14,29%	4,17%	16,07%	18,60%	15,63%	63,64%	0,00%	31,58%
2 - Mínima	50,00%	47,37%	62,50%	57,14%	70,83%	32,14%	27,91%	56,25%	18,18%	50,00%	26,32%
3 - Reativa	50,00%	36,84%	25,00%	14,29%	16,67%	42,86%	39,53%	28,13%	18,18%	50,00%	42,11%
4 - Adequada	0,00%	0,00%	12,50%	14,29%	8,33%	8,93%	13,95%	0,00%	0,00%	0,00%	0,00%

Figura 17: Proteção dos domínios da ISO/IEC 27002 na empresa pesquisada - Média

Etapa 3: Visão gerencial da segurança da informação

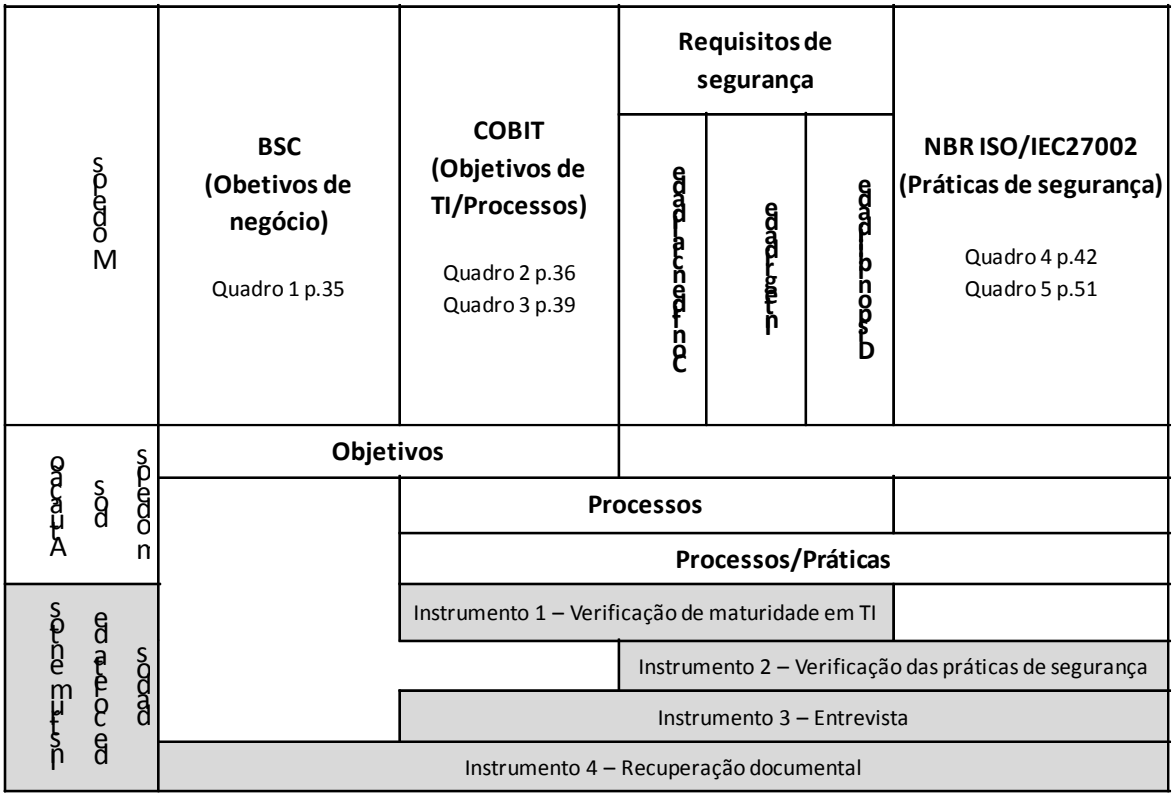
A terceira etapa da coleta de dados foi através do instrumento 3, entrevista com o diretor administrativo, responsável pela TI com base nos objetivos genéricos de TI para o negócio sugeridos pelo COBIT que envolvem os requisitos de segurança. O objetivo da entrevista foi de obter uma visão gerencial em relação à governança de TI e à segurança da informação. Na continuação é reapresentado o *framework* que posiciona este instrumento.



Com o objetivo de se familiarizar com o tema e tornar a entrevista mais produtiva, foram enviados com antecedência a relação dos objetivos. A transcrição da entrevista pode ser verificada no Anexo A.

A quarta e última etapa refere-se à **recuperação documental** para confirmar e obter informações que eventualmente levantaram dúvidas ou não foram respondidas através dos instrumentos anteriores. Os documentos analisados podem ser verificados no caderno de anexos.

O *framework* apresentado na continuação posiciona este instrumento para melhor compreensão do leitor e para o avanço da aplicação dos mesmos conforme a proposição deste trabalho.



Por motivos de confidencialidade alguns documentos não foram liberados como anexos pela empresa. Foram verificados os seguintes documentos com os propósitos.

a) Análise da Infra-Estrutura de TI.
   Propósito: Identificação da infra-estrutura de TI da empresa, arquitetura lógica e física da rede e equipamentos.
b) Atas do Time de Coordenação estratégico e operacional.
   Propósito: Verificar como é o processo decisório da empresa e interligação com o plano estratégico da empresa.
c) Contrato de desenvolvimento do configurador.
   Propósito: Verificar que requisitos e como a empresa realiza a gestão com as terceirizadas.
d) Contrato de manutenção de software SAP.

Propósito: Verificar que requisitos e como a empresa realiza a gestão com as terceirizadas.

e) Contrato Intranetworks.

Propósito: Verificar que requisitos e como a empresa realiza a gestão com as terceirizadas.

f) Controle de documentos (po_016).

Propósito: Identificar como a empresa mantém o controle de versões, distribuição e aprovação de documentos relacionados as políticas de TI.

g) Controle de registros da qualidade (po_015).

Propósito: Verificar como a empresa mantém a guarda, backup e a proteção de registros manuais e eletrônicos.

h) Critérios para seleção de fornecedores de TI.

Propósito: Verificar que requisitos e como a empresa realiza a gestão com as terceirizadas.

i) Dicas de uso dos sistemas de informação (it_064).

Propósito: Verificar como é o processo de treinamento e conscientização dos seus colaboradores sobre aspectos relacionados à segurança da informação.

j) Inventário de hardware.

Propósito: Verificar a quantidade e tipo de equipamento, certificados ou não que a empresa utiliza em sua infra-estrutura e que são importantes para a segurança.

k) Manual CRM SAP.

Propósito: Verificar como e que manuais a empresa disponibiliza para os seus colaboradores.

l) Manual da qualidade.

Propósito: Identificar, verificar como é a gestão e estrutura da empresa.

m) Manual de Inventário SAP.

Propósito: Verificar como e que manuais a empresa disponibiliza para os seus colaboradores.

n) Manual do colaborador (mn_014).

Propósito: Verificar se existem princípios de segurança sendo tratados em outros documentos que não sejam de TI.

o) Medição e monitoramento de processos (ep_018).

Propósito: Verificar quais processos, entradas e saídas e a interpelação dos processos e políticas da empresa.

p) Painel de Indicadores.
   Propósito: Verificar a disponibilidade de indicadores de TI.
q) Perfil de uso dos sistemas de informação (it_056).
   Propósito: Verificar como é tratado o acessos a informações confidenciais.
r) Plano de ação de TI:
   Propósito Verificar como o plano de ação de TI se relaciona com os objetivos da empresa. Verificar como é o processo decisório em TI, Verificar como são tratados os assuntos envolvendo a segurança da informação.
s) Plano de metas 2009.
   Propósito: Verificar se existe inter-relação entre os planos de TI e plano de metas da empresa.
t) Plano de treinamento 2009.
   Propósito: Verificar como é o processo de treinamento e conscientização dos seus colaboradores sobre aspectos relacionados à segurança da informação.
u) Plano Estratégico (ep_017).
   Propósito; Verificar se existe inter-relação entre os planos de TI e plano de metas da empresa.
v) Política de Backup.
   Propósito: Verificar como a empresa mantém a guarda, backup e a proteção de registros eletrônicos.
w) Política de uso dos sistemas de informação (ep_039)
   Propósito: Verificar quais e se a empresa adota políticas de segurança da informação.
x) Relatórios de atendimentos de suporte.
   Propósito: Verificar como a empresa se relaciona com as terceirizadas
y) Relatório de auditoria BRTUV.
   Propósito: Verificar se o sistema da qualidade da empresa integra os processos relacionados a TI.
z) Sistema de gestão de pessoas com base em competências (po_035).
   Propósito: Verificar como é o processo de treinamento e conscientização dos seus colaboradores sobre aspectos relacionados à segurança da informação.

Com a aplicação deste instrumento conclui-se toda a coleta de dados. Na continuação então inicia-se o capítulo de Análise dos Dados com base nos objetivos genéricos de TI.

4.4 Análise dos dados com base nos objetivos genéricos de TI

Para facilitar as análises dos dados, os resultados foram primeiramente estruturados por processos do COBIT com as práticas de segurança consolidadas e posteriormente analisadas por objetivo de TI. Esta organização da estruturação do processo do COBIT com as práticas de segurança consolidadas podem ser verificadas no Anexo D.

Não foram realizadas as análises dos objetivos cujos requisitos de segurança não são mapeados pelo COBIT. São eles:

- Responder aos requisitos de governança de forma alinhada à alta direção (Objetivo de TI 2);
- Definir como os requisitos funcionais e de controle do negócio são traduzidos em soluções automatizadas eficientes e efetivas (Objetivo de TI 6);
- Adquirir e manter sistemas de aplicação integrados e padronizados (Objetivo de TI 7);
- Adquirir e manter infra-estrutura de TI integrada e padronizada (Objetivo de TI 8);
- Adquirir e manter competências em TI que atenda à estratégia de TI (Objetivo de TI 9);
- Garantir transparência e entendimento dos custos, benefícios, estratégias, política e níveis de serviços de TI (Objetivo de TI 12);
- Garantir uso e desempenho adequados das aplicações e soluções de TI (Objetivo de TI 13);
- Aperfeiçoar a infra-estrutura e recursos de TI (Objetivo de TI 15);
- Melhorar a relação custo-eficiência de TI contribuindo com a rentabilidade do negócio (Objetivo de TI 24);

- Garantir que a TI demonstre qualidade de serviços eficiente em relação a seu custo, melhoria contínua e prontidão para futuras mudanças (Objetivo de TI 28).

A seguir são apresentados os quadros de coleta de dados e as análises por objetivo genérico de TI com o tipo de impacto Primário ou Secundário nos requisitos de segurança.

<table>
<tr><td colspan="5">Objetivo de TI 1 - Responder aos requisitos do negócio de forma alinhada à estratégia do negócio</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">C4, P5</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">OI, GA, RH, GO, CA, AQ</td><td rowspan="2">I, D</td></tr>
<tr><td>PO2, AI6, AI7, ES1, ES3, MO1</td><td>PO1, PO4, PO10, AI1</td></tr>
<tr><td colspan="5">Documentação analisada:
- Plano Estratégico.
- Plano de metas 2009.
- Política de uso dos sistemas de informação.
- Inventário de hardware.
- Análise da Infra-Estrutura de TI
- Perfil de uso dos sistemas de informação.
- Manual do colaborador.
- Manual da qualidade.
- Atas do TC estratégico e TC operacional.
- Plano de ação de TI.</td></tr>
<tr><td colspan="5">Respostas da entrevista:
- A empresa mantém um processo formal de planejamento estratégico com a participação da TI.
- São estabelecidas metas para a empresa e para os setores.
- A TI tem um conjunto de metas e um plano de ação.
- A TI dispõe de indicadores para o acompanhamento das metas do setor.
- Existem reuniões regulares para o acompanhamento das metas.
- Existem revisões do planejamento estratégico durante sua execução.</td></tr>
</table>

Práticas de segurança:
- A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários.
- A informação não é classificada por nível de confidencialidade.
- A empresa mantém um inventário de ativos de software e hardware.
- As informações são protegidas por senhas, porém não é mantida uma política de senhas segura.
- Não há uma gestão de mudanças de sistemas e infra-estrutura. Este processo ocorre informalmente.
- O processo de aquisição dos recursos operacionais é realizado em conjunto com o setor de informática, a decisão é por parte dos setores e a especificação técnica é de informática. A liberação de recursos para aquisição de equipamentos rede e serviços comuns a empresa é do setor administrativo.
- Não existe um processo formal para seleção, avaliação e monitoramento de fornecedores de TI.
- São mantidos contratos com os terceirizados.
- São realizadas reuniões de análise crítica com os terceirizados dos serviços considerados críticos.
- Não são realizados treinamentos sobre a segurança da informação.
- É realizada a separação dos recursos de desenvolvimento, testes e produção, porém não existem procedimentos documentos.
- O desenvolvimento de sistemas realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente.
- A empresa possui boa capacidade e disponibilidade de sistemas, porém o hardware é obsoleto e não é de procedência confiável.

Quadro 11: Coleta de dados: Objetivo de TI 1

Análise dos dados relacionada ao Objetivo 1 - Alinhar a estratégia de TI com a estratégia de negócio.

Assegurar o alinhamento de TI a estratégia de negócio é o objetivo principal da governança de TI. Para isso, a TI deve estar integrada ao processo de planejamento estratégico da organização. O Alinhamento de TI não é um conjunto específico de funcionalidades tecnológicas, mas a capacidade organizacional de alavancar a tecnologia para diferenciar suas operações de seus competidores (HENDERSON e VENKATRAMAN, 1993).

No caso analisado os processos do COBIT estão entre Repetitivo e Definido, o monitoramento e avaliação do desempenho de TI está em estágio inicial. Foi possível verificar que a empresa mantém um processo formal de planejamento estratégico com uma metodologia própria e revisões sistemáticas que o tornam dinâmico e capaz de se adaptar frente às oportunidades e necessidades da empresa, tanto internas quanti externas. A TI participa ativamente deste processo no qual possui as principais metas definidas. Estas metas são traduzidas em planos de ações como forma de buscar o alinhamento a estratégia da empresa.

No contexto da segurança da informação ela se torna efetiva quando passa a ser sistêmica fazendo parte da cultura organizacional e é tratada em todos os níveis da organização. Assim assuntos relativos à segurança devem estar presentes nos fóruns executivos da empresa até os níveis operacionais (ALLEN e WESTBY, 2007). Na empresa estudada a segurança é tratada essencialmente em nível operacional através de ações isoladas do setor de TI.

Constatou-se que não há uma preocupação efetiva da direção da empresa em relação a segurança. Desta forma não é possível afirmar que a segurança da informação faça parte da cultura da organizacional. A empresa mantém um processo de gestão que permite traduzir a estratégia em termos operacionais estabelecido. Assim, se a empresa incorporasse assuntos relativos a segurança em suas pautas estratégicas, certamente alcançaria bons níveis de segurança.

<table>
<tr><td colspan="5">Objetivo de TI 3 - Garantir a satisfação dos usuários finais com bons níveis de serviços</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">C1</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">OI, RH, SA, GO, AQ, GI, CF</td><td rowspan="2">I, D</td></tr>
<tr><td>AI4, ES1, ES2, ES10, ES13</td><td>PO8, ES7, ES8,</td></tr>
<tr><td colspan="5">Documentação analisada:
- Critérios para seleção de fornecedores de TI.</td></tr>
</table>

- Contrato Intranetworks. - Contrato de manutenção de software SAP. - Perfil de uso dos sistemas de informação. - Inventário de hardware. - Plano de ação de TI. - Contrato configurador.
Respostas da entrevista: - Existe um controle das demandas/tarefas de TI. - Os prazos das demandas de TI nem sempre são negociados. - Os prazos das demandas de TI raramente são cumpridos. - Existe iteração com os usuários. - Não existe um método para verificar se os objetivos dos projetos e demandas foram bem atendidos.
Práticas de segurança - O desenvolvimento de sistemas é realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente. - São mantidos contratos com os terceirizados. - Não existe um processo formal para seleção, avaliação e monitoramento de fornecedores de TI. - São mantidos contratos com os terceirizados incluindo cláusulas de confidencialidade da informação. - São implementadas reuniões de análise crítica com os terceirizados dos serviços considerados críticos. - São mantidos alguns manuais de sistemas, porém estão desatualizados. - A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000. - Não existe um processo formal para seleção, avaliação e monitoramento de fornecedores de TI. - A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por colaborador de acordo com suas atividades e responsabilidades. - A empresa mantém políticas e recomendações de uso dos sistemas de informação para os usuários. - A empresa não mantém um banco de conhecimentos com os incidentes. Reativamente são tomadas ações para que os incidentes não se repitam. - A manutenção dos equipamentos operacionais é realizada de forma reativa.

Quadro 12: Coleta de dados: Objetivo de TI 3

Análise dos dados do Objetivo 3 - Garantir a satisfação dos usuários finais com bons níveis de serviços

A inovação na área de tecnologia tem ciclos curtos e com isso as organizações estão cada vez mais dependentes dos sistemas de informação, o que torna um ambiente cada vez mais complexo para sua gestão. Assim, garantir a satisfação dos usuários com a solução de problemas em tempo hábil e oferecer recurso com a relação custo x benefício adequada é um desafio constante para a TI.

Os dados coletados mostram que os processos estão entre Repetitivo e Definido e a gestão de problemas se encontra em nível Inicial. Na empresa as iniciativas que levam a uma satisfação dos usuários estão em um estágio inicial. Os sistemas são desenvolvidos internamente e externamente, sendo que a adoção de técnicas e boas práticas para seleção e qualificação de fornecedores são mínimas. Os chamados de usuários são atendidos e encaminhados para solução juntamente com empresas terceirizadas, o que torna a resposta na solução de problemas em tempos relativamente pequenos, pois são tratados por profissionais especializados.

A TI se preocupa basicamente em atender as demandas do dia a dia e não desenvolve um trabalho preventivo. Também não existe a implementação de técnicas para gestão de projetos, isto colaboraria no cumprimento de prazos e consequentemente uma maior satisfação dos clientes internos.

Objetivo de TI 4 - Otimizar o uso da informação				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
C6	Mapeados	Não mapeados	GA, SA, GO, CA, AQ, CF	I

	PO2, ES11	-		
Documentação analisada: - Análise da Infra-Estrutura de TI - Inventário de hardware - Política de Backup. - Política de uso dos sistemas de informação. - Perfil de uso dos sistemas de informação. - Controle de registros da qualidade				
Respostas da entrevista: - A empresa passou recentemente por um processo de implantação de ERP - Aumentou a necessidades de recurso de TI - Os recursos de TI estão adequados as necessidades da empresa - Pouca disponibilidade de informação para tomada de decisão. - Os sistemas de informação estão mais desenvolvidos em nível operacional - Oportunidade de melhoria dos sistemas para o nível estratégico - A infra-estrutura de TI esta mapeada e documentada - Existem reuniões de análise de melhorias para tratar de assuntos relacionados a rede da empresa.				
Práticas de segurança: - A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários. - A informação não é classificada por nível de confidencialidade. - As informações são protegidas por senhas, porém não existe uma política de senha segura. - Não existem procedimentos para descarte de informações e equipamentos que contenham informações. - Não existem procedimentos para troca de informações. - A empresa mantém um inventário de ativos de software e hardware.				

Quadro 13: Coleta de dados: Objetivo de TI 4

Análise dos dados: Objetivo 4 - Otimizar o uso da informação

Em função do papel estratégico da informação e os investimentos expressivos na área de TI, reduzir os custos, melhorar o desempenho e o desempenho dos ativos de tecnologia e da área de TI como um todo pode ser considerado um fator de vantagem competitiva.

Foi possível verificar na empresa estuda que os processos se encontram no nível Repetitivo, mas Intuitivo. São disponibilizadas políticas de TI documentadas que entre outros objetivos visam o uso eficiente dos recursos de TI. Acompanhando as tendências em necessidades de recursos de TI, nos últimos anos a empresa aumentou a quantidade de sistemas de informações inclusive com a implantação de um ERP. Apesar da expansão das tecnologias e dos sistemas de informação não foi possível verificar um aumento proporcional nos em Recursos Humanos o que justifica o uso ineficiente dos sistemas de informação principalmente para tomada de decisão. Foi possível verificar ações isoladas da área de TI para melhoria da infra-estrutura e sistemas, porém isso não é uma preocupação explicita da gestão da empresa, tanto que os investimentos em valores na área de TI são desconhecidos.

<table>
<tr><td colspan="5">Objetivo de TI 5 - Criar agilidade de TI</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">C2, C4, P5, A1</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">GA, SA, GO, CA, AQ</td><td rowspan="2">I</td></tr>
<tr><td>PO2, AI3</td><td>PO4, PO7</td></tr>
<tr><td colspan="5">Documentação analisada:
- Política de uso dos sistemas de informação.
- Sistema de gestão de pessoas com base em competências.
- Plano Estratégico.
- Análise da Infra-Estrutura de TI.
- Inventário de hardware.
- Política de uso dos sistemas de informação.
- Perfil de uso dos sistemas de informação.
- Controle de projeto.
- Manual da qualidade</td></tr>
</table>

Respostas da entrevista: - Disponibilidade da informação on-line - A empresa dispõe de política de RH. - No organograma a TI esta subordinada ao setor administrativo. - As responsabilidades de TI estão definidas. - A empresa mantém um plano de treinamento com base nas necessidades definidas no planejamento estratégico.
Práticas de segurança: - A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários. - A informação não é classificada por nível de confidencialidade. - As informações dos setores de pesquisa e desenvolvimento são tratadas como as demais informações. - A empresa realiza análise crítica da segurança da informação em nível operacional. - É realizada a separação dos recursos de desenvolvimento, testes e produção, porém não há procedimentos documentados. - A empresa mantém um inventário de ativos de software e hardware. - Não existe um plano de manutenção dos equipamentos que executam serviços críticos, porém existe um plano de contingenciamento destes equipamentos.

Quadro 14: Coleta de dados: Objetivo de TI 5

Análise dos dados: Objetivo 5 - Criar agilidade de TI

As estratégias de negócios devem refletir as decisões que alinhadas aos recursos corporativos auxiliam as organizações a manter contato com seu ambiente (PORTER, 1989). Para reagir rapidamente em um ambiente de constantes mudanças as empresas precisam de uma infra-estrutura de TI flexível.

A infra-estrutura precisa balancear a necessidade de custos acessíveis para atender aos atuais requisitos de negócio e de flexibilidade para suportar futuras demandas. A dificuldade da TI em reagir às mudanças de requisitos de negócio pode comprometer as ações estratégicas da empresa. Proporcionar um ambiente de TI capaz de reações rápidas pressupõe estar sensível as mudanças, conhecer a sua infra-estrutura de sistemas, incluído hardware, software, processos e RH.

Na empresa os processos estão definidos entre Repetitivo e Definido. Como a TI participa das reuniões estratégicas as mudanças nos requisitos de negócio podem ser rapidamente percebidas e comunicadas para o nível operacional. Além disso, a empresa dispõe de mecanismos formais como políticas de TI para auxiliar na tarefa de comunicar mudanças no ambiente da empresa. Também foi possível verificar a existência de documentação com o mapeamento da infra-estrutura de TI em relação a equipamentos e serviços considerados críticos, porém esta documentação não trata de maneira clara o mapeamento dos sistemas que a empresa dispõe. Neste objetivo fica claro que a empresa é ágil para adaptar a infra-estrutura de TI. Porém pode encontrar dificuldades em adaptar os novos sistemas por falta de documentação destes sistemas.

<table>
<tr><td colspan="5">Objetivo de TI 10 - Garantir satisfação mútua em relacionamento com terceiros</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">C3, C5</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">OI, RH, GO, AQ, CF</td><td rowspan="2">C, I, D</td></tr>
<tr><td>ES2</td><td>-</td></tr>
<tr><td colspan="5">Documentação analisada:
- Contrato Intranetworks.
- Contrato de manutenção de software SAP.
- Contrato configurador.
- Contrato de prestação de serviços Elite.
- Critérios para seleção de fornecedores de TI.
- Política de uso dos sistemas de informação.
- Manual do colaborador.
- Controle de projeto.
- Inventário de hardware.
- Análise da Infra-Estrutura de TI.</td></tr>
<tr><td colspan="5">Respostas da entrevista:
- São terceirizados os serviços de Impressão, manutenção da rede e consultoria para ERP.
- São mantidos contratos com cláusulas de confidencialidade com as terceirizadas.
- Para novas contratações são realizados avaliações dos fornecedores, porém não</td></tr>
</table>

existe um procedimento documentado. - Não existem acordos de níveis de serviços. - São realizadas reuniões para melhoria dos serviços com os terceirizados.
Práticas de segurança: - Não existe um processo formal para avaliação e monitoramento de fornecedores de TI. - São mantidos contratos com os terceirizados incluindo cláusulas de confidencialidade da informação. - São implementadas reuniões de análise crítica com os terceirizados dos serviços considerados críticos. - A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por colaborador de acordo com suas atividades e responsabilidades. - O desenvolvimento de sistemas realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente.

Quadro 15: Coleta de dados: Objetivo de TI 10

Análise dos dados do Objetivo 10 - Garantir satisfação mútua em relacionamento com terceiros

Alguns dos fatores que conduzem as empresas a terceirizar estão relacionados à necessidade de manter foco no negócio, ao aumento da complexidade de infra-estrutura, à necessidade de especialização, às rápidas mudanças tecnológicas e obsolescência acelerada, (FERNANDES e ABREU, 2008). A terceirização como alternativa torna necessária uma gestão de terceiros que precisa garantir a satisfação entre contratante e contratado. Para isso é fundamental que se estabeleçam os objetivos e as regras que irão nortear a parceria.

Na pesquisa foi possível verificar que a maturidade do processo do COBIT envolvendo gestão de terceiro esta em fase Repetitivo, mas Intuitivo. A empresa adota a prática de terceirizar alguns serviços seguindo a tendência apontada por Fernandes e Abreu (2008). Para isso são mantidos contratos com os parceiros e estabelecidos alguns níveis de serviços incluindo cláusulas de confidencialidade da informação.

Apesar de existirem contratos de terceirização, a empresa não implementa o procedimentos para contratação e avaliação de fornecedores de TI. Com isso, o risco de contratar empresas que não venham atender os objetivos para qual a terceirização se propõe é relativamente alto. Isso justifica o atraso e a insatisfação verificada em alguns projetos de TI como o ERP e configurador de produtos considerados como estratégicos para o negócio.

<table>
<tr><td colspan="5">Objetivo de TI 11 - Garantir integração das aplicações com os processos de negócios</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">P1, P5, P6</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">OI, GA, RH, GO, CA, AQ, GI</td><td rowspan="2">I, D</td></tr>
<tr><td>PO2, AI4, AI7</td><td>-</td></tr>
<tr><td colspan="5">Documentação analisada:
- Relatório de auditoria BRTUV
- Análise da Infra-Estrutura de TI
- Política de Backup
- Manual CRM SAP
- Manual de Inventário SAP
- Plano de ação de TI
- Política de uso dos sistemas de informação
- Perfil de uso dos sistemas de informação
- Manual da Qualidade
- Medição e monitoramento de processos</td></tr>
<tr><td colspan="5">Respostas da entrevista:
- É mantida documentação dos sistemas, porém desatualizada.
- Sistemas subutilizados.
- Sistemas flexíveis para mudanças</td></tr>
<tr><td colspan="5">Práticas de segurança:
- A empresa mantém políticas e recomendações de uso dos sistemas de informação para os usuários.
- Não são realizados treinamentos sobre a segurança da informação.
- A empresa mantém políticas de controle de acesso documentadas por tipo de</td></tr>
</table>

informação e grupos de usuários. - A informação não é classificada por nível de confidencialidade. - A empresa mantém um inventário de ativos de software e hardware. - São mantidos alguns manuais de sistemas, porém estão desatualizados. - A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000. - O processo de aquisição dos recursos operacionais é realizado em conjunto com o setor de informática, a decisão é por parte dos setores e a especificação técnica é de informática. A liberação de recursos para aquisição de equipamentos rede e serviços comuns a empresa é do setor administrativo. - É realizada a separação dos recursos de desenvolvimento, testes e produção, porém não existem procedimentos documentos. - O desenvolvimento de sistemas realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente.

Quadro 16: Coleta de dados: Objetivo de TI 11

Análise dos dados do Objetivo 11 - Garantir integração das aplicações com os processos de negócios

As organizações estão atuando cada vez mais em uma gestão orientada por processos, sendo esta também uma diretriz da norma ISO9000:2008. As empresas que buscam a certificação nesta norma se obrigam a gestão orientada a processos e desenvolver mecanismos de integração e melhoria contínua. O uso adequado dos sistemas de informação proporciona a integração dos processos de forma ágil e eficiente resultando em diminuição de custos.

Na empresa estudada os processos de TI estão posicionados entre os níveis Repetitivo e Definido. A empresa é certificada ISO9000:2008 e com isso tem os processos principais mapeados. Para que a TI possa contribuir na integração dos processos já estabelecidos, necessariamente ela deve se adaptar a estes processos.

Foram identificas várias ferramentas de apoio como políticas de TI e documentação dos sistemas e infra-estrutura, porém esta documentação não esta integrada ao sistema da qualidade da empresa. A implementação de sistema tipo

ERP possibilitou o aumento da capacidade de integração dos processos, porém a empresa julga que os sistemas de informação estão subutilizados. Neste sentido, é possível concluir que a integração das aplicações com os processos de negócio tende a evoluir.

<table>
<tr><td colspan="5">Objetivo de TI 14 - Responder pelos ativos de TI e protegê-los</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">F2</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">PL, OI, GA, RH, SA, GO, CA, AQ, GI, GC, CF</td><td rowspan="2">C, I, D</td></tr>
<tr><td>PO9, ES5, ES9, ES12, MO2</td><td>-</td></tr>
<tr><td colspan="5">Documentação analisada:
- Análise da Infra-Estrutura de TI
- Inventário de hardware
- Política de Backup
- Plano Estratégico
- Política de uso dos sistemas de informação
- Manual do colaborador
- Sistema de gestão de pessoas com base em competências
- Controle de projeto</td></tr>
<tr><td colspan="5">Respostas da entrevista:
- A responsabilidade pela infra-estrutura de TI é da própria TI.
- Existe pouca autonomia sobre os recursos de TI pelos demais setores.
- Não existe uma manutenção preventiva dos equipamentos.
- É mantida rotina de backup.
- Informações protegidas por senhas.
- Redundância de servidores</td></tr>
<tr><td colspan="5">Práticas de segurança:
- A coordenação da segurança da informação é realizada pela TI. Não existe a participação da direção da empresa em assuntos relacionados à segurança da informação.
- A empresa mantém políticas de controle de acesso e recomendações de uso por tipo de informação e grupos de usuários incluindo processos disciplinares.
- A empresa dispõe de um controle para elaboração e revisão de documentos</td></tr>
</table>

conforme requisitos da ISO9000.

- Não existe um fórum específico para tratar a segurança da informação.

- A empresa realiza análise crítica da segurança da informação em nível operacional, porém não de forma independente e com a participação da direção da empresa.

- As informações são protegidas por senhas, porém não existe uma política de senha segura.

- Não estão previstos nas políticas de TI diretrizes sobre remoção de ativos.

- A empresa não usa criptografia de dados.

- São realizadas auditorias eventuais nos sistemas da empresa em busca de uso indevido dos recursos de TI.

- Não é implementado um processo de ações corretivas e preventivas para a segurança da informação

- O acesso por terceiros aos sistemas e informações da empresa não é tratado nas políticas de segurança. Os acessos remotos são realizados utilizando VPN. Porém não identificados os riscos relacionados com partes externas.

- Não estão previstos nas políticas de segurança práticas de desconexões por inatividades.

- Os acessos remotos são realizados utilizando VPN.

- A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por colaborador de acordo com suas atividades e responsabilidades.

- Não são realizados treinamentos sobre a segurança da informação.

- A empresa dispõe de um inventário de ativos de hardware e software com um plano de contingência dos serviços críticos, porém não são realizados testes e auditorias para verificar a disponibilidade em casos de desastres.

- A empresa dispõe de antivírus, porém não dispõe de sistema de detecção de intrusos.

- Os servidores estão protegidos fisicamente em uma sala de servidores com controle de acesso.

- Não há proteção para os equipamentos de rede e estações de trabalho.

- Os problemas relacionados à infra-estrutura de rede da empresa são tratados de forma reativa e não segue padrão recomendado. Os equipamentos e rede não são certificados.

- A manutenção dos equipamentos operacionais é realizada de forma reativa.

- Os contratos com terceiros incluem acordos de confidencialidade da informação.

Quadro 17: Coleta de dados: Objetivo de TI 14

Análise dos dados do Objetivo 14 - Responder pelos ativos de TI e protegê-los

A proteção dos ativos de tecnologia da informação adquire uma posição estratégica para as organizações, tanto pelo alto valor associado quanto pelos impactos negativos do seu comprometimento.

Os processos do COBIT estão posicionados entre os níveis Inicial e o Definido. Foi verificado que a empresa mantém mapeados pelo setor de TI os principais ativos da empresa quanto a *software* e *hardware* com planos de contingência dos serviços e equipamentos considerados críticos. A responsabilidade pelos ativos é distribuída entre o setor de TI e demais setores da organização, ficando responsabilidade do setor de TI os ativos considerados críticos. O plano de contingência considera um tempo tolerável de indisponibilidade por tipo de serviço. Em casos de desastre, isso possibilita uma disponibilidade dos sistemas em um espaço menor e conhecido de tempo.

Analisando a documentação é possível observar que o grau de inovação é apontado como um dos principais diferenciais competitivos da empresa. Partindo deste requisito de negócio a proteção adequada dos projetos de pesquisa e desenvolvimento representa um fator importante para a empresa. Foi possível observar que mesmo existindo políticas de uso e guarda das informações elas não seguem suficientemente as boas práticas recomendadas pela norma IEC/ISO 27002. Desta forma, é possível concluir que o atual modelo de proteção de dados pode representar um risco para informações consideradas confidenciais.

Objetivo de TI 16 - Reduzir defeitos e retrabalho nas entregas de soluções e serviços				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
C3	Mapeados	Não mapeados	OI, RH, GO, CA, AQ, GI	I, D

	AI4, AI6, AI7, ES10	PO8		

Documentação analisada:

- Análise da Infra-Estrutura de TI
- Contrato Intranetworks
- Relatório de atendimento Intranetworks
- Plano de ação de TI
- Política de uso dos sistemas de informação
- Sistema de gestão de pessoas com base em competências
- Plano de Treinamento 2009

Respostas da entrevista:

- São realizados testes antes da entrega das soluções

Práticas de segurança:

- A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários.
- A empresa mantém políticas e recomendações de uso dos sistemas de informação para os usuários.
- Não são realizados treinamentos sobre a segurança da informação.
- A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000.
- São mantidos alguns manuais de sistemas, porém estão desatualizados.
- As informações são protegidas por senhas, porém não é mantida uma política de senhas segura.
- Não há uma gestão de mudanças de sistemas e infra-estrutura. Este processo ocorre informalmente.
- O processo de aquisição dos recursos operacionais é realizado em conjunto com o setor de informática, a decisão é por parte dos setores e a especificação técnica é de informática. A liberação de recursos para aquisição de equipamentos rede e serviços comuns a empresa é do setor administrativo.
- O desenvolvimento de sistemas é realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente.
- É realizada a separação dos recursos de desenvolvimento, testes e produção, porém não existem procedimentos documentos.
- A empresa não mantém um banco de conhecimentos com os incidentes. Reativamente são tomadas ações para que os incidentes não se repitam.

Quadro 18: Coleta de dados: Objetivo de TI 16

Análise dos dados do objetivo 16 - Reduzir defeitos e retrabalho nas entregas de soluções e serviços

Diminuir o os defeitos e retrabalho em qualquer processo empresarial significa redução de custos. Isto se torna especialmente crítico quando envolve sistemas de informação por ser um recurso utilizado em nível estratégico, tático e operacional. Para que haja uma redução de defeitos e retrabalhos em TI é preciso que: (1) haja um bom entendimento dos requisitos de usuários, (2) seja desenvolvida documentação de projetos de sistemas, (3) sejam realizados testes apropriados antes das entregas e que, finalmente, (4) haja uma mão de obra qualificada para o desenvolvimento de soluções.

Os dados demonstram que na empresa os processos estão entre os níveis Repetitivo e Definidos, salvo pela gestão de problemas que se encontra em nível inicial. A empresa possui um plano de desenvolvimento e treinamento de colaboradores com o objetivo de qualificar a sua mão de obra. Também foi possível observar um alto grau de qualificação dos colaboradores em função da exigência do negócio por estar competindo no mercado de automação que requer um bom nível de inovação em produto.

A equipe é formada em mais de 70% por engenheiros, eletrotécnicos ou mão de obra que necessita de especialização em cursos técnicos o que também foi verificado na equipe de TI. Em relação à documentação de projetos de sistemas não foi possível verificar nada consistente. As soluções são desenvolvidas e contratadas sem realizar um estudo aprofundado dos requisitos dos usuários. Neste quesito, o processo que se mostra melhor estruturado é em relação a mudanças na infra-estrutura de rede que segundo a documentação analisada passa por um processo relativamente rigoroso na entrega de soluções com o objetivo de minimizar o impacto aos serviços dos usuários.

Objetivo de TI 17 – Garantir o cumprimento dos objetivos de TI				
BSC	**Processos COBIT**		**ISO/IEC27002**	
F2	Mapeados	Não mapeados	PL, OI, GO, GI, GC, CF	C, I, D

	PO9, ES10, MO2	-		
Documentação analisada: - Análise da Infra-Estrutura de TI - Plano de metas 2009 - Plano de ação de TI - Atas do TC estratégico e TC operacional - Plano Estratégico - Política de uso dos sistemas de informação.				
Respostas da entrevista: - São estabelecidos objetivos e metas de TI - É mantido um plano de ação para o acompanhamento do atendimento das metas.				
Práticas de segurança: - A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários e documentação com recomendações de uso dos sistemas de informação. - A empresa realiza análise crítica da segurança da informação em nível operacional. O assunto não é tradado pela direção da empresa. - A empresa mantém um plano de contingenciamento para os serviços considerados críticos para o negócio. - São realizadas auditorias eventuais para verificar o uso dos sistemas de informação. - A empresa não implementa um processo de ações corretivas e preventivas para a segurança da informação. - A empresa não mantém um banco de conhecimentos com os incidentes. Reativamente são tomadas ações para que os incidentes não se repitam.				

Quadro 19: Coleta de dados: Objetivo de TI 17

Análise dos dados: Objetivo 17 - Garantir o cumprimento dos objetivos de TI

Foi verificado que os processos estão definidos entre o nível Inicial e Repetitivo. Para atender a este objetivo o departamento de TI da empresa mantém políticas de TI e um plano de ação com revisões regulares. O plano de ação e TI é

derivado do plano estratégico o que faz com que ele seja visto e cobrado pela direção.

Não foi possível verificar ações específicas que evidenciem a preocupação da direção da empresa com a segurança da informação. A segurança é tratada basicamente em nível operacional e assim, a empresa dispõe de um processo relativamente bem estruturado para incorporar assuntos relativos à segurança da informação.

<table>
<tr><td colspan="5">Objetivo de TI 18 - Estabelecer clareza no impacto de riscos do negócio em relação a objetivos e recursos de TI</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">F2, F3</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">PL, GI, GC</td><td rowspan="2">C, I, D</td></tr>
<tr><td>PO9</td><td>-</td></tr>
<tr><td colspan="5">Documentação analisada:
- Plano Estratégico
- Política de uso dos sistemas de informação
- Perfil de uso dos sistemas de informação
- Atas do TC estratégico e TC operacional
- Plano de ação de TI</td></tr>
<tr><td colspan="5">Respostas da entrevista:
- A empresa identifica os principais riscos e mantém um mapa para gestão com um plano de redundância.</td></tr>
<tr><td colspan="5">Práticas de segurança:
- A empresa mantém um plano de contingenciamento para os serviços considerados críticos para o negócio.
- A empresa realiza análise crítica da segurança da informação em nível operacional. O assunto não é tradado pela direção da empresa.</td></tr>
</table>

Quadro 20: Coleta de dados: Objetivo de TI 18

Análise dos dados do Objetivo 18 - Estabelecer clareza no impacto de riscos do negócio em relação a objetivos e recursos de TI

Em relação à gestão de riscos para o negócio envolvendo a TI, o processo do COBIT está em nível Inicial e foi possível evidenciar que o assunto é tratado basicamente em nível operacional. Não foi possível encontrar evidências nos objetivos e requisitos de negocio identificados no planejamento estratégico e atas de reuniões estratégicas em relação a riscos envolvendo a TI. Com isso fica evidente que a empresa necessita a melhorar em relação à gestão de riscos e segurança da informação como um todo.

<table>
<tr><td colspan="5">Objetivo de TI 19 - Assegurar que informações críticas e confidenciais são inacessíveis a aqueles que não devem ter acesso a elas</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">F2, P3</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">PL, OI, RH, SA, GO, CA, AQ, GI, GC, CF</td><td rowspan="2">C, I, D</td></tr>
<tr><td>ES5, ES11, ES12</td><td>PO6</td></tr>
<tr><td colspan="5">Documentação analisada:
- Política de uso dos sistemas de informação
- Perfil de uso dos sistemas de informação
- Dicas de uso dos sistemas de informação
- Manual do colaborador
- Plano de ação de TI</td></tr>
<tr><td colspan="5">Respostas da entrevista:
- Informações protegidas por senhas.
- Informações são classificadas por grupo para acesso.</td></tr>
<tr><td colspan="5">Práticas de segurança:
- A coordenação da segurança da informação é realizada pela TI. Não existe a participação da direção da empresa em assuntos relacionados a segurança da informação.
- A empresa mantém políticas de controle de acesso e recomendações de uso por tipo de informação e grupos de usuários incluindo processos disciplinares.
- As informações são protegidas por senhas, porém não existe uma política de senha segura.
- Não existe um fórum específico para tratar a segurança da informação.
- A empresa realiza análise crítica da segurança da informação em nível</td></tr>
</table>

operacional.

- Não são realizados treinamentos sobre a segurança da informação.

- A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por colaborador de acordo com suas atividades e responsabilidades.

- A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000.

- São realizadas auditorias eventuais nos sistemas da empresa em busca de uso indevido dos recursos de TI.

- O acesso por terceiros aos sistemas e informações da empresa não é tratado nas políticas de segurança.

- A empresa dispõe de antivírus, porém não dispõe de sistema de detecção de intrusos.

- As informações são protegidas por senhas, porém não existe uma política de senha segura.

- A empresa dispõe de um inventário de hardware com identificação dos equipamentos.

- A infra-estrutura de rede da empresa é tratada de forma reativa e não segue padrão recomendado. Não é certificada.

- A empresa não usa criptografia de dados.

- Não esta prevista nas políticas de segurança práticas de desconexões por inatividades.

- Os acessos remotos são realizados utilizando VPN.

- Não existem procedimentos para descarte de informações e equipamentos que contenham informações.

- Os servidores estão protegidos fisicamente em uma sala de servidores com controle de acesso.

- Não há proteção para os equipamentos de rede e estações de trabalho.

- A manutenção dos equipamentos operacionais é realizada de forma reativa. Para equipamentos que executam serviços críticos existe um plano de contingenciamento.

- Não estão previstos nas políticas de TI diretrizes sobre remoção de ativos.

- Não existem procedimentos para troca de informações.

- Os acessos remotos são realizados utilizando VPN. Porém não identificados os riscos relacionados com partes externas.

- Os contratos com terceiros incluem acordos de confidencialidade da informação.

Quadro 21: Coleta de dados: Objetivo de TI 19

Análise dos dados do Objetivo 19 - Assegurar que informações críticas e confidenciais são inacessíveis a aqueles que não devem ter acesso a elas

Este objetivo é o princípio da confidencialidade e os processos do COBIT estão posicionados no nível denominado Definidos. As informações são protegidas por usuário, grupos de usuários e tipo de informações, porém a informação não é classificada por nível de confidencialidade.

Apesar da proteção por senhas, não são adotadas políticas de senhas seguras, assim a quebra destas por diversas técnicas se torna fácil. Isso é uma evidência de que a preocupação não é tratada como prioridade e consequentemente acaba por adotar práticas obsoletas. Esta prática certamente questiona significativamente toda segurança da informação e principalmente o princípio da Confidencialidade. Na empresa estudada, a confidencialidade da informação também é tratada em algumas políticas de TI que repassam as responsabilidades para os usuários através da aplicação de processos disciplinares.

Outras formas para garantia do sigilo e confidencialidade da informação são praticadas por iniciativa da equipe de TI como auditoria análise de registros e uso de antivírus. Isto minimiza os riscos de acesso não autorizado dos sistemas por ataques externos. Neste sentido, fica claro que os processos estão estabelecidos e são implementados, porém a rigorosidade em relação à segurança poderia melhorar.

<table>
<tr><td colspan="5">Objetivo de TI 20 - Garantir que as informações de negócio e transações automatizadas são confiáveis</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">F2, C6, P3</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">PL, OI, RH, SA, GO, CA, AQ, GI, GC, CF</td><td rowspan="2">I, D</td></tr>
<tr><td>ES5</td><td>PO6, AI7</td></tr>
<tr><td colspan="5">Documentação analisada:
- Política de uso dos sistemas de informação
- Dicas de uso dos sistemas de informação</td></tr>
</table>

- Plano de ação de TI
Respostas da entrevista: - São realizados testes antes da entrega das soluções. - Os relatórios e sistemas são validados pelos usuários.
Práticas de segurança: - A empresa realiza análise crítica da segurança da informação em nível operacional. - A empresa mantém políticas de controle de acesso e recomendações de uso por tipo de informação e grupos de usuários incluindo processos disciplinares. - Os contratos com terceiros incluem acordos de confidencialidade da informação. - A coordenação da segurança da informação é realizada pela TI. Não existe a participação da direção da empresa em assuntos relacionados a segurança da informação. - Não existe um fórum específico para tratar a segurança da informação. - O acesso por terceiros aos sistemas e informações da empresa não é tratado nas políticas de segurança. - Não são realizados treinamentos sobre a segurança da informação. - A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por colaborador de acordo com suas atividades e responsabilidades. - A empresa dispõe de antivírus, porém não dispõe de sistema de detecção de intrusos. - A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000. - São realizadas auditorias eventuais nos sistemas da empresa em busca de uso indevido dos recursos de TI. - As informações são protegidas por senhas, porém não existe uma política de senha segura. - A empresa dispõe de um inventário de hardware com identificação dos equipamentos. - A infra-estrutura de rede da empresa é tratada de forma reativa e não segue padrão recomendado. Não é certificada. - A empresa não usa criptografia de dados. - Não esta prevista nas políticas de segurança práticas de desconexões por inatividades. - Os acessos remotos são realizados utilizando VPN.

Quadro 22: Coleta de dados: Objetivo de TI 20

Análise dos dados do Objetivo 20 - Garantir que as informações de negócio e transações automatizadas são confiáveis

Uma informação não confiável representa um alto risco para qualquer decisão. O processo do COBIT que envolve a segurança aponta para o nível Definido. Para isso a empresa estudada dispõe de políticas de controle de acesso para que a os dados não seja sejam manipulados por pessoas não incapacitadas e não autorizadas.

Apesar de não existir um processo padrão para desenvolvimento ou contratação de novas soluções, o setor de TI se preocupa em testar e validar as soluções antes da entrega para os usuários. Com isso, a possibilidade de entregar relatórios e informações não confiáveis diminui consideravelmente. Também são realizadas auditorias nos sistemas em busca de uso indevido dos sistemas. Esta prática permite identificar e tomar ações corretivas e preventivas em caso de acesso indevido a informação. Um ponto que se mostra falho nas políticas de segurança é o fato de não tratar o acesso de terceiros aos sistemas da empresa.

<table>
<tr><td colspan="4">Objetivo de TI 21 - Garantir que os serviços e infra-estrutura de TI resistam a falhas em função de erros, ataques deliberados ou desastres</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">F2, P3</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">PL, OI, RH, SA, GO, CA, AQ, GI, GC, CF</td><td rowspan="2">I, D</td></tr>
<tr><td>AI7, ES4, ES5, ES12, ES13, MO2</td><td>PO6</td></tr>
<tr><td colspan="5">Documentação analisada:
- Análise da Infra-Estrutura de TI
- Contrato Intranetworks
- Relatórios de atendimento Intranetworks
- Inventário de hardware
- Plano de ação de TI
- Política de uso dos sistemas de informação
- Perfil de uso dos sistemas de informação</td></tr>
</table>

Respostas da entrevista:

- Existe redundância de equipamentos para usuários e serviços essenciais.

- A empresa dispõe de antivírus

- A empresa esta iniciando um trabalho de auditoria para verificação da situação dos principais equipamentos e sistemas com o objetivo de prevenção de incidentes.

Práticas de segurança:

- A empresa mantém políticas de controle de acesso e recomendações de uso por tipo de informação e grupos de usuários incluindo processos disciplinares e mantém documentos com recomendações de uso dos sistemas de informação.

- A empresa realiza análise crítica da segurança da informação em nível operacional, porém não de forma independente.

- Não são realizados treinamentos sobre a segurança da informação.

- É mantido e documentado um sistema de backup.

- A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por colaborador de acordo com suas atividades e responsabilidades.

- São mantidos alguns manuais de sistemas, porém estão desatualizados.

- A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000.

- As informações são protegidas por senhas, porém não existe uma política de senha segura.

- A coordenação da segurança da informação é realizada pela TI. Não existe a participação da direção da empresa em assuntos relacionados a segurança da informação.

- Não existe um fórum específico para tratar a segurança da informação.

- O acesso por terceiros aos sistemas e informações da empresa não é tratado nas políticas de segurança.

- A empresa dispõe de antivírus, porém não dispõe de sistema de detecção de intrusos.

- São realizadas auditorias eventuais nos sistemas da empresa em busca de uso indevido dos recursos de TI.

- A empresa não usa criptografia de dados.

- Não estão previstos nas políticas de segurança práticas de desconexões por inatividades.

- Os acessos remotos são realizados utilizando VPN. Porém não identificados os riscos relacionados com partes externas.

- Não é implementado um processo de ações corretivas e preventivas para a segurança da informação.

- O processo de aquisição dos recursos operacionais é realizado em conjunto com

o setor de informática, a decisão é por parte dos setores e a especificação técnica é de informática. A liberação de recursos para aquisição de equipamentos rede e serviços comuns a empresa é do setor administrativo.
- Os contratos com terceiros incluem acordos de confidencialidade da informação.
- É realizada a separação dos recursos de desenvolvimento, testes e produção, porém não existem procedimentos documentos.
- O desenvolvimento de sistemas realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente.
- É mantida uma assessoria para tratar de assuntos com autoridades e grupos especiais.
- A empresa dispõe de um inventário de ativos de hardware e software com um plano de contingência dos serviços críticos, porém não são realizados testes e auditorias para verificar a disponibilidade em casos de desastres
- A empresa dispõe de um inventário de hardware com identificação dos equipamentos.
- A infra-estrutura de rede da empresa é tratada de forma reativa e não segue padrão recomendado. Não é certificada.
- Os servidores estão protegidos fisicamente em uma sala de servidores com controle de acesso.
- Não há proteção para os equipamentos de rede e estações de trabalho.
- A manutenção dos equipamentos operacionais é realizada de forma reativa. Para equipamentos que executam serviços críticos existe um plano de contingenciamento.
- Não estão previstos nas políticas de TI diretrizes sobre remoção de ativos.
- A manutenção dos equipamentos operacionais é realizada de forma reativa.

Quadro 23: Coleta de dados: Objetivo de TI 21

Análise dos dados do Objetivo 21 - Garantir que os serviços e infra-estrutura de TI resistam a falhas em função de erros, ataques deliberados ou desastres

Para este objetivo a maturidade da maioria dos processos se encontra em nível Definido. A empresa dispõe planos de contingenciamento para os serviços considerados essenciais e são implementados processos de backup bem como utilizados sistemas de antivírus. Apesar de não existir um sistema de detecção de intrusos, estão sendo desenvolvidas iniciativas com o objetivo de implementar ações

preventivas. Isso demonstra claramente que uma evolução no amadurecimento dos processos e práticas envolvendo este objetivo.

<table>
<tr><td colspan="4">Objetivo de TI 22 - Garantir impacto mínimo no negócio no caso de uma interrupção ou anormalidade em um serviço de TI</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">F2, C3, P3</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">SA, GO, CA, AQ, GC</td><td rowspan="2">I, D</td></tr>
<tr><td>AI6, ES4, ES12</td><td>PO6</td></tr>
<tr><td colspan="5">Documentação analisada:
- Análise da Infra-Estrutura de TI
- Inventário de hardware
- Contrato Intranetworks</td></tr>
<tr><td colspan="5">Respostas da entrevista:
- Existe redundância de equipamentos para usuários e serviços essenciais.
- A empresa dispõe de antivírus
- A empresa esta iniciando um trabalho de auditoria para verificação da situação dos principais equipamentos e sistemas com o objetivo de prevenção de incidentes.</td></tr>
<tr><td colspan="5">Práticas de segurança:
- A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários.
- As informações são protegidas por senhas, porém não é mantida uma política de senhas segura.
- Não há uma gestão de mudanças de sistemas e infra-estrutura. Este processo ocorre informalmente.
- É mantida uma assessoria para tratar de assuntos com autoridades e grupos especiais.
- É mantido e documentado um sistema de backup.
- A empresa dispõe de um inventário de ativos de hardware e software com um plano de contingência dos serviços críticos, porém não são realizados testes e auditorias para verificar a disponibilidade em casos de desastres.
- Os acessos remotos são realizados utilizando VPN. Porém não identificados os riscos relacionados com partes externas.
- Os servidores estão protegidos fisicamente em uma sala de servidores com controle de acesso.</td></tr>
</table>

- Não há proteção para os equipamentos de rede e estações de trabalho. - A manutenção dos equipamentos operacionais é realizada de forma reativa. Para equipamentos que executam serviços críticos existe um plano de contingenciamento. - Não estão previstos nas políticas de TI diretrizes sobre remoção de ativos.

Quadro 24: Coleta de dados: Objetivo de TI 22

Análise dos dados do Objetivo 22 - Garantir impacto mínimo no negócio no caso de uma interrupção ou anormalidade em um serviço de TI

Neste objetivo a maturidade os processos envolvendo o COBIT se encontra entre os níveis Repetitivo, Intuitivo e Definido. A empresa dispõe de planos de contingenciamento dos serviços críticos e contrata terceiros especializados nestes serviços. No contexto do negócio, isso garante uma resposta em tempo adequado em caso de falhas. Além disso, existem políticas que orientam o uso dos recursos de TI que entre outros objetivos auxiliam na preservação dos sistemas e equipamentos.

<table>
<tr><td colspan="5">Objetivo de TI 23 - Assegurar que os serviços de TI estão disponíveis quando solicitados</td></tr>
<tr><th>BSC</th><th colspan="2">Processos COBIT</th><th>ISO/IEC27002</th><th>Requisitos de segurança</th></tr>
<tr><td rowspan="2">C1, C3</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">OI, SA, GO, GC</td><td rowspan="2">D</td></tr>
<tr><td>ES3, ES4, ES13</td><td>ES8</td></tr>
<tr><td colspan="5">Documentação analisada:
- Análise da Infra-Estrutura de TI
- Inventário de hardware</td></tr>
<tr><td colspan="5">Respostas da entrevista:
- Os chamados e demandas de TI são tratados diretamente com os usuários, não existe um serviço de help-desk para registro das solicitações pelos próprios usuários.</td></tr>
<tr><td colspan="5">Práticas de segurança:
- A empresa possui boa capacidade e disponibilidade de sistemas, porém o</td></tr>
</table>

hardware é obsoleto e não é de procedência confiável. - É mantida uma assessoria para tratar de assuntos com autoridades e grupos especiais. - É mantido e documentado um sistema de backup. - A empresa dispõe de um inventário de ativos de hardware e software com um plano de contingência dos serviços críticos, porém não são realizados testes e auditorias para verificar a disponibilidade em casos de desastres. - A manutenção dos equipamentos operacionais é realizada de forma reativa. - A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000. - São mantidos alguns manuais de sistemas, porém estão desatualizados.

Quadro 25: Coleta de dados: Objetivo de TI 23

Análise dos dados do Objetivo 23 - Assegurar que os serviços de TI estão disponíveis quando solicitados

Os processos do COBIT envolvendo este objetivo estão definidos entre os níveis Repetitivo e Definido e as práticas de segurança são na maioria de proteção Mínima. A empresa mantém boas práticas de disponibilidade em relação aos serviços e *hardware* considerados críticos, porém poderia melhorar as práticas em relação a manutenção dos equipamentos dos usuários.

O inventário de *hardware* deixa claro a necessidade de atualização destes equipamentos o que poderia melhorar a disponibilidade da informação e produtividade dos colaboradores. O serviço de suporte é realizado conforme as demandas surgem e não mantém indicadores de incidência que poderia auxiliar a identifica e priorizar os incidentes mais críticos.

Objetivo de TI 25 - Entregar projetos no prazo e nos orçamento previstos, observando padrões de qualidade				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
C4, A1	Mapeados	Não	-	I

		mapeados		
	-	PO8, PO10		
Documentação analisada: - Plano de metas 2009 - Atas do TC estratégico e TC operacional - Plano de ação de TI				
Respostas da entrevista: - Dificilmente são cumpridos os prazos dos projetos e demandas de TI - A TI não implementa nenhuma metodologia de gestão de projetos				
Práticas de segurança:				

Quadro 26: Coleta de dados: Objetivo de TI 25

Análise dos dados do Objetivo 25 - Entregar projetos no prazo e nos orçamento previstos, observando padrões de qualidade

Apesar de não ser possível mapear as práticas de segurança da IEC/ISO27002 através do COBIT, este objetivo contribui para o requisito de integridade. Por este motivo foi avaliada a maturidade dos processos do COBIT, analisada a documentação em busca de evidencias e incluído no roteiro de entrevista. Na avaliação de maturidade, mesmo não existindo práticas de gestão de projetos os processos se encontram entre Repetitivo e Definido. Foi verificado que a TI mantém um plano de ação com revisões sistemáticas para acompanhar os seus projetos.

Objetivo de TI 26 - Manter a integridade da informação e da infra-estrutura				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
C6, P3	Mapeados	Não mapeados	PL, OI, RH, SA, GO, CA, AQ, GI, GC, CF	I, D
	AI6, ES5	-		
Documentação analisada: - Plano Estratégico				

- Política de uso dos sistemas de informação - Dicas de uso dos sistemas de informação - Perfil de uso dos sistemas de informação - Plano de ação de TI - Atas do TC estratégico e TC operacional - Plano de treinamento - Análise da Infra-Estrutura de TI - Inventário de hardware
Respostas da entrevista: - Não foram aplicadas questões para este objetivo
Práticas de segurança: - A coordenação da segurança da informação é realizada pela TI. Não existe a participação da direção da empresa em assuntos relacionados a segurança da informação. - A empresa mantém políticas de controle de acesso e recomendações de uso por tipo de informação e grupos de usuários incluindo processos disciplinares. - A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por colaborador de acordo com suas atividades e responsabilidades. - Não são realizados treinamentos sobre a segurança da informação. - As informações são protegidas por senhas, porém não é mantida uma política de senhas segura. - São realizadas auditorias eventuais nos sistemas da empresa em busca de uso indevido dos recursos de TI. - A empresa realiza análise crítica da segurança da informação em nível operacional. - A empresa não usa criptografia de dados. - Não existe um fórum específico para tratar a segurança da informação. - O acesso por terceiros aos sistemas e informações da empresa não é tratado nas políticas de segurança. - A empresa dispõe de antivírus, porém não dispõe de sistema de detecção de intrusos. - A empresa dispõe de um inventário de hardware com identificação dos equipamentos. - A infra-estrutura de rede da empresa é tratada de forma reativa e não segue padrão recomendado. Não é certificada. - Não esta prevista nas políticas de segurança práticas de desconexões por inatividades.

- Os acessos remotos são realizados utilizando VPN. - Não há uma gestão de mudanças de sistemas e infra-estrutura. Este processo ocorre informalmente. - Os contratos com terceiros incluem acordos de confidencialidade da informação. - A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000.

Quadro 27: Coleta de dados: Objetivo de TI 26

Análise dos dados do Objetivo 26 - Manter a integridade da informação e da infra-estrutura

A maturidade dos processos que envolvem este objetivo está localizado entre os níveis Repetitivo e Definido. A responsabilidade pela segurança da informação é o setor de TI. A direção não se envolve com diretrizes de segurança sendo estes assuntos tratados em nível operacional.

Objetivo de TI 27 - Garantir que a TI observe a legislação, regulamentações e contratos				
BSC	**COBIT**		**ISO/IEC27002**	
P3	Mapeados	Não mapeados	PL, OI, SA, GO, AQ, CF	C, I
	ES11, MO2, MO3, MO4	-		
Documentação analisada:				
Respostas da entrevista: - A empresa mantém uma assessoria para acompanhar as mudanças na legislação				
Práticas de segurança:				

Quadro 28: Coleta de dados: Objetivo de TI 27

Análise dos dados do Objetivo 27 - Garantir que a TI observe a legislação, regulamentações e contratos

Os processos em relação a este objetivo apontam para um nível de maturidade Inicial. O setor responsável por monitorar as mudanças na legislação é o setor administrativo, isto justifica a pouca preocupação da TI em seu monitoramento. Apesar do questionário de maturidade apontar um nível inicial, a entrevista deixa evidente que a empresa esta bem protegida, pois contrata uma acessória que monitora eventuais mudanças na legislação.

5 CONCLUSÕES FINAIS, LIMITAÇÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS.

5.1 Conclusões

Diversos estudos relacionados à função estratégica da informação e do alinhamento da TI com o negócio têm sido desenvolvidos (HENDERSON e VENKATRAMAN, 1993), (LUFTMAN, 2000), (HIRSCHHEIM e SABHERWAL, 2001). A referência histórica de Porter e Millar (1985) já antecipava a importância de tecnologia de informação e comunicação (TIC) em que os autores apresentam o tema destacando o “quanto” de informação está contida no processo e no produto através de uma “matriz de intensidade da informação”.

Em empresas em que os produtos e processos contêm grande quantidade de informação, os sistemas de informação terão grande importância estratégica e segundo Porter (1989), se algo pode gerar uma vantagem competitiva é por que está criando maior valor ao negócio. Esta linha de raciocínio é complementada por Macgee e Prusak (1994), afirmando que não é a tecnologia que cria valor, mas o seu uso. Eardley *et al.* (1996), complementam mostrando através de um estudo a influência dos sistemas de informação nas cinco forças competitivas de Porter.

Atualmente há segmentos empresariais em que a TI tem tamanha importância a ponto de reposicionar estrategicamente uma empresa potencializando novos negócios, como no caso de oferta de produtos e serviços via comércio eletrônico. Mesmo que aparentemente em alguns negócios não se identifique influência direta sobre as ações estratégicas é comprovado que indiretamente a informação pode exercer forças na sustentabilidade do negócio.

Para complementar, vivencia-se uma nova realidade da TI em função das ações nas instituições governamentais, o conhecido *e-Government* e a integração dos

sistemas públicos e privados que a cada dia controlam mais as atividades empresariais. Essa integração possibilita maior controle deste tipo de atividades empresariais bem como maior controle sobre a arrecadação do Estado. A Nota Fiscal Eletrônica (NF-e) e Sistema Público de Escrituração Digital Fiscal e Contábil são exemplos adequados desta nova realidade.

Estes aspectos remetem para importância de operar a informação em um ambiente seguro e seguidor de regras especificas em um contexto de governança corporativa. Em estudo recente realizado por Dlamini *et al*, (2009), as novas pesquisas no campo da segurança da Informação convergem na tentativa de aproximar os princípios de governança de TI e ações técnicas com os de governança corporativa.

Neste contexto este trabalho contribuiu com esta tendência com a proposta prática de desenvolver alinhamento estratégico em segurança da TI através da integração de modelos em um setor significativamente dependente de Tecnologia da Informação.

O primeiro objetivo do trabalho identificou a relação entre os modelos estratégico, tático e operacional de governança de TI, envolvendo aspectos de segurança da informação. A partir do estudo realizado foi possível então comprovar que modelos de governança têm focos específicos e atuam em níveis organizacionais diferentes.

Em relação ISO/IEC27002 foi possível verificar que o aspecto segurança da informação é tratado num nível estritamente técnico e operacional. Porém, em função das rápidas mudanças típicas desta área, se torna praticamente impossível se cercar de garantias técnicas que propiciem um ambiente suficientemente seguro.

O *framework* desenvolvido e apresentado na figura 8 integra o tema segurança nos níveis estratégico, tático e operacional (objetivos de negócios, objetivos de TI e práticas de segurança), possibilitando assim um entendimento e atuação na gestão da segurança nos diversos níveis da organização e resultando em um alinhamento estratégico. Esse *framework* é constituído por quatro instrumentos que juntos

possibilitaram uma análise dos aspectos de segurança atendendo os requisitos de confidencialidade, integridade e disponibilidade.

A integração de modelos desenvolvida pelo pesquisador e representada na composição do *framework* com seus respectivos instrumentos de verificação e análise do aspecto de segurança se mostrou uma prática viável e possibilitou contemplar esse em todos os níveis da organização, promovendo o alinhamento estratégico. Foram integrados os modelos BSC x COBT e ISO/IEC27002 considerando exclusivamente os princípios de segurança confidencialidade, integridade, disponibilidade inicialmente propostos.

O objetivo que identificou o grau de maturidade de governança de TI em relação aos processos operacionais envolvendo os requisitos de segurança da informação utilizou o modelo de maturidade do CMMI, este aplicado aos processos do COBIT. A maturidade final dos processos foi definida entre os níveis Inicial e nível Definido, conforme mostrado na Figura 14.

Considerando que o melhor modelo de governança de TI é aquele que atende ao negócio e seus parceiros e considerando o ambiente em que a empresa pesquisada opera, pode se afirmar que a maturidade da empresa se encontra em nível denominado como Repetitivo e Intuitivo evoluindo para o Definido, visto que a maioria dos processos em nível Inicial são os relacionados ao Monitoramento. A empresa pode evoluir em relação maturidade dando ênfase principalmente aos processos de monitoramento que se encontra em nível inicial.

Este resultado confirmou o observado pela entrevista e pela análise documental. A empresa dispõe quadros de indicadores para os processos de negócio, porém eles não existem na área de TI, justificando então o baixo nível de maturidade dos processos de monitoramento bem como a necessidade de um referencial de alinhamento estratégico de TI como aqui desenvolvido.

Com base no referencial teórico analisado se entende que este é um elevado nível de maturidade visto que a empresa não tem explicitado em seus objetivos a implantação de um modelo de governança de TI. Isto se explica pelo histórico da

empresa que mantêm um sistema da qualidade estruturado a mais de 15 anos e certificado há 10 anos, desenvolvendo uma cultura de gestão por metas e padronização dos processos empresariais.

Sobressai o fato do processo “ES5 - Garantir segurança dos sistemas” que se encontra como Definido. Esta percepção se fundamente pelo fato do setor de TI praticar auditorias regulares de uso dos sistemas de informação e ter iniciado um processo reuniões regulares para análise de infra-estrutura da rede.

O terceiro objetivo propôs a análise das práticas de segurança para alinhar as mesmas aos requisitos de negócio e de TI adotadas pelo caso estudado. Isso complementa o objetivo geral de promover o alinhamento estratégico entre os objetivos de negócio, objetivos de TI e as práticas da segurança da informação. Os dados revelaram que a segurança da informação na perspectiva técnica se encontra em um grau de proteção Mínima para Reativa e ela é tratada através ações isoladas baseadas no conhecimento técnico.

Confirmando o que referencial teórico aponta como uma limitação dos modelos de gestão de TI nas organizações, o presente trabalho contribuiu com o desenvolvimento e um referencial sintetizado e apresentado como um *framework* que possibilita alcançar as práticas de segurança a partir de uma visão de negócio (requisitos de negócio e de TI) e posicionar melhor a empresa perante suas práticas de segurança da informação. Isso contribui significativamente com a análise de Posthumos e Solms (2004), cujos autores afirmam que a segurança da informação deve ser incorporada as governança corporativa e tratada nos mais altos níveis gerenciais.

A segurança da informação se torna efetiva e incorporada na cultura da organização através de técnicas como estabelecimento de políticas, treinamento, conscientização e aplicação de práticas disciplinares (SOLMS e SOLMS, 2004). O estudo demonstrou que na sua aplicação junto à empresa foi possível constatar que mesma dispõe de um processo gerencial estruturado com base na norma ISO9000:2008 com o propósito de desdobrar a estratégia em ações, mesmo que não se caracterize um BSC. Mesmo assim, este caso empresarial estudado e

possivelmente outros ainda necessitariam de uma forma ainda mais estruturada de incorporar aspectos de segurança envolvendo essa cultura, proporcionado por este trabalho através de um direcionamento para aplicações constituído de diferentes instrumentos estruturados para esse fim.

Um aspecto que ficou evidente na entrevista é a questão da perda de Produtividade, a qual não foi possível identificar em nenhum dos modelos estudados (BSC, COBIT ou Segurança isoladamente). Essa situação ocorre em função do fácil acesso fácil às aplicações que desviam a atenção do colaborador.

Este fato é evidente devido ao uso intenso da internet mas também pelo variado aparato tecnológico que cercam os profissionais, ocasionando o desvio de foco em sua atividade principal. Esse desvio de foco de sua atividade principal ocasiona também fragilidades no tema relacionado à segurança da informação, bem como no requisito relacionado a excesso de disponibilidade de recursos tecnológicos, verificado pela aplicação prática deste trabalho.

Após o trabalho de mapeamento e aplicação dos instrumentos, ficou também evidente a necessidade de mais uma complementação conceitual em relação aos princípios básicos de segurança da informação incorporando outros aspectos de negócio. Esta complementação sugere uma abrangência maior, além dos aspectos técnicos, em torno do tema através de novos trabalhos de pesquisa.

5.2 Limitações do trabalho

O presente trabalho apresentou limitação relacionada à aplicação do instrumento de entrevista pode ter tido um viés do pesquisador, visto que o mesmo trabalha na organização onde a pesquisa foi realizada. Porém, como o *framework* desenvolvido e aplicado recebeu uma estruturação significativa, entende-se que este tipo de viés tenha sido bem reduzido e controlado principalmente no processo de coleta de dados. Isto também possibilitou um acesso facilitado aos dados, principalmente a documentação da empresa, fato este que enriqueceu a pesquisa pela quantidade de informações coletadas.

5.3 Recomendações para trabalhos futuros

Os temas correlatos e potenciais que esta pesquisa identificou para continuidade de trabalhos e/ou aprofundamento desta mesma pesquisa, são os seguintes:

a) Estudos quantitativos e estatísticos quanto aos temas explorados nos Quadros de resumo e na análise final;
b) Estudo sobre o impacto na produtividade frente facilidade de acesso a sistemas que não envolvem a atividade fim da empresa;
c) Realização de pesquisas similares com a aplicação deste tipo de alinhamento em outros setores empresariais;
d) Estudos com a proposta de um mapa estratégico envolvendo o tema segurança em sistemas de informação;
e) Estudos com análises mais aprofundadas em relação aos objetivos de TI para o Negócio ampliando os requisitos estudados.

6 REFERÊNCIAS

ALLEN J.; WESTBY J. R.. Characteristics of Effective Security Governance. **Carnegie Mellon University,** Software Engineering Institute, 2007

BNDES: Banco Nacional de Desenvolvimento Econômico e Social. **BNDES Setorial**, Complexo Eletrônico: Automação do Controle Industrial, Rio de Janeiro, n. 28, p. 189-232, set. 2008.

BSA: **Business Software Alliance**. Information Security Governance: Toward a Framework for Action, 2003.

CERT.br: Centro de Estudos. **Resposta e Tratamento de Incidentes de Segurança no Brasil**, http://www.cert.br/stats/incidentes, acessado em 29/10/2009.

CGTFR: Corporative Governance Task Force Report. Information Security Governance: A Call to Action, **National Cyber Security Summit Task Force**, 2004.

CMV: **Comissão de Valores Mobiliários.** Recomendações da CVM sobre Governança Corporativa. São Paulo: 2002.

DAHLBERG, T.; LAHDELMA, P. IT Governance Maturity and IT Degree: An Exploratory Study. ***Proceedings of the 40th Hawaii International Conference on Systems Sciences.*** Honolulu, Hawaii, 2007.

DIAS, C.. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axel Books, 2000.

DLAMINI M, ELOFF J, ELOFF M. Information security: The moving target. **Computers & Security**, 2009.

EARDLEY A.; LEWIS, T..; AVISON, D.; POWELL, P.. The Linkage between IT and Business Competitive Systems: a Reappraisal of Some ‘Classic’ Cases Using a

Competitive Analysis Framework. **International Journal of Technology Management**, v.11, n.3/4, p.395-411, 1996.

ELOFF, J.; ELOFF, M.. Information Security Management: A New Paradigm. Proceedings of **the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology,** p.130-136, 2003

ENTRUST: **Information Security Governance (ISG**): An Essential Element of Corporate Governance. Disponível on-line. em: http://www.entrust.com/governance/ Acessado em 16/03/2009.

FERNANDES, A. A.; ABREU, V. F. **Implantando a governança de TI: da estratégia à gestão dos processos e serviços.** Rio de Janeiro: Brasport, 2008.

FINK, K.; PLODER, F.; Decision support framework for the implementation of IT-Governance. **Proceedings of the 41 st Hawaii International Conference on Systems Science.** Honolulu, Hawaii, 2008, CDRom.

FITZGERALD, T, Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other, **Information Systems Security**, V 16, I 5, pp 257-63, 2007

GREMBERGEN, W. V.; HAES, S. D.. IT Governance and Its Mechanisms, **Information Systems Control Journal**, Vol1, 2004.

HENDERSON, J. C.; VENKATRAMAN, N. Strategic Alignment: leveraging information technology for transforming organization. **IBM Systems Journal**, V32, N01, 1993, pp 472 - 76.

HIRSCHHEIM, R.; SABHERWAL, R. Detours in the path toward strategic information systems alignment. **California Management Review**, v.44, n.1, p.87-108, 2001.

IBGC: Instituto **de Brasileiro de Governança Corporativa**. Código de Melhores Práticas de Governança Corporativa 4ª edição, 2009.

ISO/IEC27002. Tecnologia da Informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: **Associação Brasileira de Normas Técnicas,** 2001.

ITGI: **Information Security Governance:** Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006

ITGI: **Information Technology Governance Institute**. CobiT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models. Disponível em: http:// www.isaca.org/, acessado em: 24 de fevereiro de 2009.

ITSQC: **Information Technology Services Qualification Center**, eCSM-SP, eCSM-SL, Disponível em: http://itsqc.cmu.edu/, acessado em 05/01/2009.

KAPLAN, R. S.; NORTON, D. P. **A estratégia em ação: Balanced Scorecard**. Rio de Janeiro: Campus, 1997.

KWOK, l.; LONGLEY, D. Information security management and modeling, **Information Management & Computer Security**, V7, I1, pp 30 – 40, 1999.

LUFTMAN, J. N. Assessing business-IT alignment maturity. **Communications of the Association for Information Systems.** V. 4, Article 14, 2000.

MACGEE, J. e PRUSAK, L.. **Gerenciamento estratégico da informação:** aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica . RJ. Campus, 1994.

MANSUR, R.. **Governança de TI:** Metodologias, Frameworks e Melhores Práticas. Rio de Janeiro: Brasport, 2007.

MOREIRA, N. S.. **Segurança Mínima**: Uma Visão Corporativa da Segurança de Informações. Rio de Janeiro: Axcel Books, 2001.

NORFOLK, D. ***IT Governance: Managing Information Technology for Business***. London: Thorogood, 2005.

PORTER, M. E.; MILLAR, V.E. How information gives you competitive advantage. **Harvard Business Review**, 1985.

PORTER, M. E.. **A Vantagem Competitiva das Nações**. Rio de Janeiro: Editora Campus, 1989.

POSTHUMUS, S.; SOLMS, R.. A framework for the governance of information security - **Computers & Security**, V23. pp 638-46, 2004.

SARBANES-OXLEY ACT. **Congress of the United States of America**. Washington: 2002.

SEC: U.S. **Security and Exchange Comission**, Disponível em: http://www.sec.gov/, acessado em 05/01/2009.

SEI: **Software Enginneering Institute**, disponível em www.sei.cmu.edu/cmmi/, acessado em 15/11/2008.

SÊMOLA, M.. Gestão **da Segurança da informação**: Visão executiva da Segurança da Informação. Rio de Janeiro: Campus, 2003.

SOLMS, R.; SOLMS, B.. From policies to culture, **Computers & Security**, V 23, I 4, 2004, pp 275-79.

TRICKER, B. Information and power – the influence of IT on corporate governance.Corporate. **Governance reporting**, 1997. 5(2): p.49-51.

WEILL, P.; ROSS, J. W. **Governança de TI:** Como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores. São Paulo: M. Books, 2006.

ANEXOS

Anexo A – Questionários de avaliação de maturidade

Gestor: Carlos Hennig

O instrumento a seguir tem por objetivo avaliar o grau de maturidade da empresa Coester em relação governança de TI considerando o modelo COBIT 4.1 e os processos relacionados aos requisitos de segurança disponibilidade, integridade, confidencialidade.

A governança de TI e seus processos com o objetivo de adicionar valor ao negócio através do balanceamento do risco e retorno do investimento podem ser classificados, seguindo o modelo do CMMI *(Capability Maturity Model Integration),* da seguinte forma:

Grau de maturidade	**Descrição**
0 – Inexistente	Neste nível há uma absoluta falta do processo. A organização não tem conhecimento sobre as implicações que a falta do processo pode gerar.
1 – Inicial	Neste nível os processos são esporádicos e desorganizados, não existe documentação e controle alguma.
2 – Repetitivo, mas intuitivo	Neste nível os processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos.
3 – Definido	Neste nível os procedimentos estão estabelecidos e são cumpridos. Inicio do uso de indicadores para controle.
4 – Gerenciado	Neste nível os processos estão integrados e alinhados. As metas e planos são baseados em dados e indicadores consistentes.
5 – Otimizado	Boas práticas são seguidas e automatizadas, com base em

	resultados de melhoria contínua.

Quadro de análise:

Em nível de maturidade, marque com um “x” a coluna que você considera que o respectivo processo se encontra.

Processos COBIT		Nível de maturidade					
		0 - Inexistente	1 - Inicial	2 - Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado
PO - Organização e planejamento.							
PO1	**Define o planejamento estratégico de TI.** As empresas dispõem de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio			X			
PO2	**Define a arquitetura da informação.** A empresa documenta a estrutura de TI e sistemas de informação com modelos e dicionário de dados.			X			
PO4	**Define a organização de TI e seus relacionamentos.** A empresa estabelece a estrutura de RH de TI com cargos, suas responsabilidades e os relacionamentos com as demais áreas da organização.				X		
PO6	**Comunica as metas e diretrizes gerenciais.** A empresa estabelece e comunica as metas de TI para a equipe e as políticas de TI para a organização.			X			
PO7	**Gerencia os recursos humanos.** Gerencia o RH de TI com um plano de capacitação e desenvolvimento de pessoal e plano de carreira considerando as necessidades do negócio e as tecnologias utilizadas na empresa. Desenvolve mecanismos de motivação para a equipe de TI.				X		
PO8	**Gerencia a qualidade.** Mantém de um sistema de gestão da qualidade com documentação dos processos, seleção de fornecedores e melhoria contínua de TI, integrado ao sistema de qualidade da empresa.					X	
PO9	**Avalia e gerencia os riscos.** Mantém um quadro de gestão de riscos, analisa ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência.				X		
PO10	**Gerencia os projetos.** Coordena projetos através de um plano mestre com níveis de qualidade, recursos necessários e prazos observando modelos e melhores práticas de mercado.			X			
AI - Aquisição e Implementação.							
AI1	**Identifica soluções de automação.** Para compra ou desenvolvimento de novas aplicações é realizada uma				X		

	analise de requisitos, considerando fontes alternativas, análise de viabilidade econômica e tecnológica, análise de risco, custo benefício.						
AI3	**Adquire e mantém a arquitetura tecnológica.** Mantém um plano de manutenção, aquisição e implementação de melhoria da infra-estrutura tecnológica com o objetivo de dar sustentação as aplicações da empresa.				X		
AI4	**Desenvolve e mantém procedimentos de TI.** Disponibiliza documentação e treinamento os usuários e profissionais de TI para correta utilização dos sistemas e infra-estrutura de TI.					X	
AI5	**Obtém recursos de TI.** Dispões de um procedimento para aquisição de recursos de TI necessários incluindo hardware, software, serviços, pessoas, fornecedores e fornecedores.				X		
AI6	**Gerenciar mudanças** Avalia e aprova mudanças no ambiente, tanto em equipamentos e arquitetura quanto em sistemas e processos.				X		
AI7	**Instala e certifica soluções e mudanças.** Antes da entrega de novas soluções de TI (Software, Hardware e Sistemas) são realizados testes apropriados e um acompanhamento pós-implantação.			X			
DS - Entrega e suporte.							
ES1	**Define níveis e mantém os acordos de níveis de serviços.** Formaliza os níveis de atendimento e internos e externos das soluções TI.			X			
ES2	**Gerencia os serviços de terceiros.** Acompanha e avalia os serviços contratados.				X		
ES3	**Gerenciar desempenho e capacidade da TI.** A empresa define e revisa periodicamente os recursos computacionais e garante que não haja escassez de recursos, evitando problemas de desempenho nas aplicações ou desperdício de investimentos.			X			
ES4	**Garante a continuidade dos serviços.** Assegura a continuidade dos serviços, incluindo sistemas de Backup, manutenção de equipamentos, testes e plano de contingência de hardware e serviços críticos.				X		
ES5	**Garante a segurança dos sistemas.** A empresa dispõe de políticas de segurança, visa a preservação da confidencialidade, da integridade e da disponibilidade da informação.				X		
ES7	**Educa e treina os usuários.** A empresa mantém um plano de treinamento de usuários e profissionais de TI para uso eficaz e eficiente dos sistemas de informação.			X			
ES8	**Gerencia a central de serviços e incidentes.** Existe o registro e controle das solicitações e incidências de TI.			X			
ES9	**Gerencia a configuração.** A empresa dispõe de um repositório/registro das configurações de hardware e software com o objetivo de minimizar e resolver problemas com mais agilidade.			X			
ES10	**Gerencia os problemas.** Existe uma metodologia de ações corretivas e preventivas para os problemas de TI.		X				
ES11	**Gerencia os dados.** Define o ciclo de vida da informação, com definição de prazos para disponibilidade, arquivo morto e descarte de acordo com os requisitos do negócio e da legislação.				X		
ES12	**Gerencia a infra-estrutura.** Existe uma definição dos requisitos físicos e controle do ambiente físico para os equipamentos de TI, incluindo fatores ambientais, de acesso, instalações entre outros.					X	

ES13	**Gerenciar operações.** Administra o funcionamento das operações de TI				X		
ME - Medição e monitoramento.							
MO1	**Monitora e avalia a desempenho de TI.** Utiliza indicadores para monitorar e gerenciar o desempenho dos processos de TI.		X				
MO2	**Monitora e avalia o controle interno.** Estabelece mecanismos de controle interno dos requisitos da área e monitora a sua execução.			X			
MO3	**Assegura a conformidade aos requisitos externos.** Estabelece processo de revisão dos requisitos de legislação, contratuais e de negócio.		X				
MO4	**Fornecer governança de TI.** Estabelece um efetivo modelo de governança, que inclui definição da estrutura organizacional, processos, liderança, perfis e responsabilidades, a fim de garantir que os investimentos estejam alinhados às estratégias da organização.			X			

Gestor: Marcus Coester

O instrumento a seguir tem por objetivo avaliar o grau de maturidade da empresa Coester em relação governança de TI considerando o modelo COBIT 4.1 e os processos relacionados aos requisitos de segurança disponibilidade, integridade, confidencialidade.

A governança de TI e seus processos com o objetivo de adicionar valor ao negócio através do balanceamento do risco e retorno do investimento podem ser classificados, seguindo o modelo do CMMI *(Capability Maturity Model Integration),* da seguinte forma:

Grau de maturidade	**Descrição**
0 – Inexistente	Neste nível há uma absoluta falta do processo. A organização não tem conhecimento sobre as implicações que a falta do processo pode gerar.
1 – Inicial	Neste nível os processos são esporádicos e desorganizados, não existe documentação e controle alguma.
2 – Repetitivo, mas	Neste nível os processos seguem um padrão de

intuitivo	regularidade, com alta dependência do conhecimento dos indivíduos.
3 – Definido	Neste nível os procedimentos estão estabelecidos e são cumpridos. Inicio do uso de indicadores para controle.
4 – Gerenciado	Neste nível os processos estão integrados e alinhados. As metas e planos são baseados em dados e indicadores consistentes.
5 – Otimizado	Boas práticas são seguidas e automatizadas, com base em resultados de melhoria contínua.

Quadro de análise:

Em nível de maturidade, marque com um “x” a coluna que você considera que o respectivo processo se encontra.

Processos COBIT		Nível de maturidade					
		0 - Inexistente	1 - Inicial	2 - Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado
PO - Organização e planejamento.							
PO1	**Define o planejamento estratégico de TI.** As empresas dispõem de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio				X		
PO2	**Define a arquitetura da informação.** A empresa documenta a estrutura de TI e sistemas de informação com modelos e dicionário de dados.				X		
PO4	**Define a organização de TI e seus relacionamentos.** A empresa estabelece a estrutura de RH de TI com cargos, suas responsabilidades e os relacionamentos com as demais áreas da organização.				X		
PO6	**Comunica as metas e diretrizes gerenciais.** A empresa estabelece e comunica as metas de TI para a equipe e as políticas de TI para a organização.				X		
PO7	**Gerencia os recursos humanos.** Gerencia o RH de TI com um plano de capacitação e desenvolvimento de pessoal e plano de carreira considerando as necessidades do negócio e as tecnologias utilizadas na empresa. Desenvolve mecanismos de motivação para a equipe de TI.				X		
PO8	**Gerencia a qualidade.**					X	

	Mantém de um sistema de gestão da qualidade com documentação dos processos, seleção de fornecedores e melhoria contínua de TI, integrado ao sistema de qualidade da empresa.						
PO9	**Avalia e gerencia os riscos.** Mantém um quadro de gestão de riscos, analisa ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência.			X			
PO10	**Gerencia os projetos.** Coordena projetos através de um plano mestre com níveis de qualidade, recursos necessários e prazos observando modelos e melhores práticas de mercado.					X	
AI - Aquisição e Implementação.							
AI1	**Identifica soluções de automação.** Para compra ou desenvolvimento de novas aplicações é realizada uma analise de requisitos, considerando fontes alternativas, análise de viabilidade econômica e tecnológica, análise de risco, custo benefício.					X	
AI3	**Adquire e mantém a arquitetura tecnológica.** Mantém um plano de manutenção, aquisição e implementação de melhoria da infra-estrutura tecnológica com o objetivo de dar sustentação as aplicações da empresa.						X
AI4	**Desenvolve e mantém procedimentos de TI.** Disponibiliza documentação e treinamento os usuários e profissionais de TI para correta utilização dos sistemas e infra-estrutura de TI.					X	
AI5	**Obtém recursos de TI.** Dispões de um procedimento para aquisição de recursos de TI necessários incluindo hardware, software, serviços, pessoas, fornecedores e fornecedores.					X	
AI6	**Gerenciar mudanças** Avalia e aprova mudanças no ambiente, tanto em equipamentos e arquitetura quanto em sistemas e processos.				X		
AI7	**Instala e certifica soluções e mudanças.** Antes da entrega de novas soluções de TI (Software, Hardware e Sistemas) são realizados testes apropriados e um acompanhamento pós-implantação.					X	
DS - Entrega e suporte.							
ES1	**Define níveis e mantém os acordos de níveis de serviços.** Formaliza os níveis de atendimento e internos e externos das soluções TI.			X			
ES2	**Gerencia os serviços de terceiros.** Acompanha e avalia os serviços contratados.			X			
ES3	**Gerenciar desempenho e capacidade da TI.** A empresa define e revisa periodicamente os recursos computacionais e garante que não haja escassez de recursos, evitando problemas de desempenho nas aplicações ou desperdício de investimentos.			X			
ES4	**Garante a continuidade dos serviços.** Assegura a continuidade dos serviços, incluindo sistemas de Backup, manutenção de equipamentos, testes e plano de contingência de hardware e serviços críticos.					X	
ES5	**Garante a segurança dos sistemas.** A empresa dispõe de políticas de segurança, visa a preservação da confidencialidade, da integridade e da disponibilidade da informação.				X		
ES7	**Educa e treina os usuários.** A empresa mantém um plano de treinamento de usuários e profissionais de TI para uso eficaz e eficiente dos sistemas de informação.				X		
ES8	**Gerencia a central de serviços e incidentes.** Existe o registro e controle das solicitações e incidências de TI.		X				
ES9	**Gerencia a configuração.** A empresa dispõe de um repositório/registro das configurações de hardware e software com o objetivo de minimizar e resolver problemas com mais agilidade.			X			
ES10	**Gerencia os problemas.**		X				

	Existe uma metodologia de ações corretivas e preventivas para os problemas de TI.						
ES11	**Gerencia os dados.** Define o ciclo de vida da informação, com definição de prazos para disponibilidade, arquivo morto e descarte de acordo com os requisitos do negócio e da legislação.				X		
ES12	**Gerencia a infra-estrutura.** Existe uma definição dos requisitos físicos e controle do ambiente físico para os equipamentos de TI, incluindo fatores ambientais, de acesso, instalações entre outros.					X	
ES13	**Gerenciar operações.** Administra o funcionamento das operações de TI				X		
ME - Medição e monitoramento.							
MO1	**Monitora e avalia a desempenho de TI.** Utiliza indicadores para monitorar e gerenciar o desempenho dos processos de TI.		X				
MO2	**Monitora e avalia o controle interno.** Estabelece mecanismos de controle interno dos requisitos da área e monitora a sua execução.			X			
MO3	**Assegura a conformidade aos requisitos externos.** Estabelece processo de revisão dos requisitos de legislação, contratuais e de negócio.			X			
MO4	**Fornecer governança de TI.** Estabelece um efetivo modelo de governança, que inclui definição da estrutura organizacional, processos, liderança, perfis e responsabilidades, a fim de garantir que os investimentos estejam alinhados às estratégias da organização.			X			

Gestor: Tatiana Coester

O instrumento a seguir tem por objetivo avaliar o grau de maturidade da empresa Coester em relação governança de TI considerando o modelo COBIT 4.1 e os processos relacionados aos requisitos de segurança disponibilidade, integridade, confidencialidade.

A governança de TI e seus processos com o objetivo de adicionar valor ao negócio através do balanceamento do risco e retorno do investimento podem ser classificados, seguindo o modelo do CMMI *(Capability Maturity Model Integration),* da seguinte forma:

Grau de maturidade	**Descrição**
0 – Inexistente	Neste nível há uma absoluta falta do processo. A organização não tem conhecimento sobre as implicações que a falta do processo pode gerar.

1 – Inicial	Neste nível os processos são esporádicos e desorganizados, não existe documentação e controle alguma.
2 – Repetitivo, mas intuitivo	Neste nível os processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos.
3 – Definido	Neste nível os procedimentos estão estabelecidos e são cumpridos. Inicio do uso de indicadores para controle.
4 – Gerenciado	Neste nível os processos estão integrados e alinhados. As metas e planos são baseados em dados e indicadores consistentes.
5 – Otimizado	Boas práticas são seguidas e automatizadas, com base em resultados de melhoria contínua.

Quadro de análise:

Em nível de maturidade, marque com um “x” a coluna que você considera que o respectivo processo se encontra.

Processos COBIT		Nível de maturidade					
		0 - Inexistente	1 - Inicial	2 - Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado
PO - Organização e planejamento.							
PO1	**Define o planejamento estratégico de TI.** As empresas dispõem de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio				X		
PO2	**Define a arquitetura da informação.** A empresa documenta a estrutura de TI e sistemas de informação com modelos e dicionário de dados.			x			
PO4	**Define a organização de TI e seus relacionamentos.** A empresa estabelece a estrutura de RH de TI com cargos, suas responsabilidades e os relacionamentos com as demais áreas da organização.				X		
PO6	**Comunica as metas e diretrizes gerenciais.** A empresa estabelece e comunica as metas de TI para a equipe e as políticas			x			

	de TI para a organização.						
PO7	**Gerencia os recursos humanos.** Gerencia o RH de TI com um plano de capacitação e desenvolvimento de pessoal e plano de carreira considerando as necessidades do negócio e as tecnologias utilizadas na empresa. Desenvolve mecanismos de motivação para a equipe de TI.					X	
PO8	**Gerencia a qualidade.** Mantém de um sistema de gestão da qualidade com documentação dos processos, seleção de fornecedores e melhoria contínua de TI, integrado ao sistema de qualidade da empresa.					X	
PO9	**Avalia e gerencia os riscos.** Mantém um quadro de gestão de riscos, analisa ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência.			X			
PO10	**Gerencia os projetos.** Coordena projetos através de um plano mestre com níveis de qualidade, recursos necessários e prazos observando modelos e melhores práticas de mercado.				X		
AI - Aquisição e Implementação.							
AI1	**Identifica soluções de automação.** Para compra ou desenvolvimento de novas aplicações é realizada uma analise de requisitos, considerando fontes alternativas, análise de viabilidade econômica e tecnológica, análise de risco, custo benefício.				X		
AI3	**Adquire e mantém a arquitetura tecnológica.** Mantém um plano de manutenção, aquisição e implementação de melhoria da infra-estrutura tecnológica com o objetivo de dar sustentação as aplicações da empresa.				X		
AI4	**Desenvolve e mantém procedimentos de TI.** Disponibiliza documentação e treinamento os usuários e profissionais de TI para correta utilização dos sistemas e infra-estrutura de TI.				X		
AI5	**Obtém recursos de TI.** Dispões de um procedimento para aquisição de recursos de TI necessários incluindo hardware, software, serviços, pessoas, fornecedores e fornecedores.					X	
AI6	**Gerenciar mudanças** Avalia e aprova mudanças no ambiente, tanto em equipamentos e arquitetura quanto em sistemas e processos.			X			
AI7	**Instala e certifica soluções e mudanças.** Antes da entrega de novas soluções de TI (Software, Hardware e Sistemas) são realizados testes apropriados e um acompanhamento pós-implantação.					X	
DS - Entrega e suporte.							
ES1	**Define níveis e mantém os acordos de níveis de serviços.** Formaliza os níveis de atendimento e internos e externos das soluções TI.			X			
ES2	**Gerencia os serviços de terceiros.** Acompanha e avalia os serviços contratados.			X			
ES3	**Gerenciar desempenho e capacidade da TI.** A empresa define e revisa periodicamente os recursos computacionais e garante que não haja escassez de recursos, evitando problemas de desempenho nas aplicações ou desperdício de investimentos.			X			
ES4	**Garante a continuidade dos serviços.** Assegura a continuidade dos serviços, incluindo sistemas de Backup, manutenção de equipamentos, testes e plano de contingência de hardware e serviços críticos.					X	
ES5	**Garante a segurança dos sistemas.** A empresa dispõe de políticas de segurança, visa a preservação da					X	

	confidencialidade, da integridade e da disponibilidade da informação.						
ES7	**Educa e treina os usuários.** A empresa mantém um plano de treinamento de usuários e profissionais de TI para uso eficaz e eficiente dos sistemas de informação.				x		
ES8	**Gerencia a central de serviços e incidentes.** Existe o registro e controle das solicitações e incidências de TI.		X				
ES9	**Gerencia a configuração.** A empresa dispõe de um repositório/registro das configurações de hardware e software com o objetivo de minimizar e resolver problemas com mais agilidade.			x			
ES10	**Gerencia os problemas.** Existe uma metodologia de ações corretivas e preventivas para os problemas de TI.			x			
ES11	**Gerencia os dados.** Define o ciclo de vida da informação, com definição de prazos para disponibilidade, arquivo morto e descarte de acordo com os requisitos do negócio e da legislação.				x		
ES12	**Gerencia a infra-estrutura.** Existe uma definição dos requisitos físicos e controle do ambiente físico para os equipamentos de TI, incluindo fatores ambientais, de acesso, instalações entre outros.			X			
ES13	**Gerenciar operações.** Administra o funcionamento das operações de TI			x			
ME - Medição e monitoramento.							
MO1	**Monitora e avalia a desempenho de TI.** Utiliza indicadores para monitorar e gerenciar o desempenho dos processos de TI.			x			
MO2	**Monitora e avalia o controle interno.** Estabelece mecanismos de controle interno dos requisitos da área e monitora a sua execução.			x			
MO3	**Assegura a conformidade aos requisitos externos.** Estabelece processo de revisão dos requisitos de legislação, contratuais e de negócio.			x			
MO4	**Fornecer governança de TI.** Estabelece um efetivo modelo de governança, que inclui definição da estrutura organizacional, processos, liderança, perfis e responsabilidades, a fim de garantir que os investimentos estejam alinhados às estratégias da organização.			x			

Avaliador: Wilson Kapp

Data: 10/07/2009

O instrumento a seguir tem por objetivo avaliar o grau de maturidade da empresa Coester em relação governança de TI considerando o modelo COBIT 4.1 e os processos relacionados aos requisitos de segurança disponibilidade, integridade, confidencialidade.

A governança de TI e seus processos com o objetivo de adicionar valor ao negócio através do balanceamento do risco e retorno do investimento podem ser

classificados, seguindo o modelo do CMMI *(Capability Maturity Model Integration),* da seguinte forma:

Grau de maturidade	**Descrição**
0 – Inexistente	Neste nível há uma absoluta falta do processo. A organização não tem conhecimento sobre as implicações que a falta do processo pode gerar.
1 – Inicial	Neste nível os processos são esporádicos e desorganizados, não existe documentação e controle alguma.
2 – Repetitivo, mas intuitivo	Neste nível os processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos.
3 – Definido	Neste nível os procedimentos estão estabelecidos e são cumpridos. Inicio do uso de indicadores para controle.
4 – Gerenciado	Neste nível os processos estão integrados e alinhados. As metas e planos são baseados em dados e indicadores consistentes.
5 – Otimizado	Boas práticas são seguidas e automatizadas, com base em resultados de melhoria contínua.

Quadro de análise:

Em nível de maturidade, marque com um “x” na coluna que você considera que o respectivo processo se encontra.

Processos COBIT		**Nível de maturidade**					
		0 - Inexistente	**1 - Inicial**	**2 - Repetitivo**	**3 - Definido**	**4 - Gerenciado**	**5- Otimizado**
PO - Organização e planejamento.							
PO1	**Define o planejamento estratégico de TI.** As empresas dispõem de um Plano de TI com base em um plano estratégico			X			

	de negócio, vinculando as diretrizes de TI às necessidades do negócio						
PO2	**Define a arquitetura da informação.** A empresa documenta a estrutura de TI e sistemas de informação com modelos e dicionário de dados.			X			
PO4	**Define a organização de TI e seus relacionamentos.** A empresa estabelece a estrutura de RH de TI com cargos, suas responsabilidades e os relacionamentos com as demais áreas da organização.			X			
PO6	**Comunica as metas e diretrizes gerenciais.** A empresa estabelece e comunica as metas de TI para a equipe e as políticas de TI para a organização.				X		
PO7	**Gerencia os recursos humanos.** Gerencia o RH de TI com um plano de capacitação e desenvolvimento de pessoal e plano de carreira considerando as necessidades do negócio e as tecnologias utilizadas na empresa. Desenvolve mecanismos de motivação para a equipe de TI.		X				
PO8	**Gerencia a qualidade.** Mantém de um sistema de gestão da qualidade com documentação dos processos, seleção de fornecedores e melhoria contínua de TI, integrado ao sistema de qualidade da empresa.			X			
PO9	**Avalia e gerencia os riscos.** Mantém um quadro de gestão de riscos, analisa ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência.				X		
PO10	**Gerencia os projetos.** Coordena projetos através de um plano mestre com níveis de qualidade, recursos necessários e prazos observando modelos e melhores práticas de mercado.			X			
AI - Aquisição e Implementação.							
AI1	**Identifica soluções de automação.** Para compra ou desenvolvimento de novas aplicações é realizada uma analise de requisitos, considerando fontes alternativas, análise de viabilidade econômica e tecnológica, análise de risco, custo benefício.				X		
AI3	**Adquire e mantém a arquitetura tecnológica.** Mantém um plano de manutenção, aquisição e implementação de melhoria da infra-estrutura tecnológica com o objetivo de dar sustentação as aplicações da empresa.			X			
AI4	**Desenvolve e mantém procedimentos de TI.** Disponibiliza documentação e treinamento os usuários e profissionais de TI para correta utilização dos sistemas e infra-estrutura de TI.				X		
AI5	**Obtém recursos de TI.** Dispões de um procedimento para aquisição de recursos de TI necessários incluindo hardware, software, serviços, pessoas, fornecedores e fornecedores.			X			
AI6	**Gerenciar mudanças** Avalia e aprova mudanças no ambiente, tanto em equipamentos e arquitetura quanto em sistemas e processos.			X			
AI7	**Instala e certifica soluções e mudanças.** Antes da entrega de novas soluções de TI (Software, Hardware e Sistemas) são realizados testes apropriados e um acompanhamento pós-implantação.			X			
DS - Entrega e suporte.							
ES1	**Define níveis e mantém os acordos de níveis de serviços.** Formaliza os níveis de atendimento e internos e externos das soluções TI.				X		

ES2	**Gerencia os serviços de terceiros.** Acompanha e avalia os serviços contratados.				X		
ES3	**Gerenciar desempenho e capacidade da TI.** A empresa define e revisa periodicamente os recursos computacionais e garante que não haja escassez de recursos, evitando problemas de desempenho nas aplicações ou desperdício de investimentos.			X			
ES4	**Garante a continuidade dos serviços.** Assegura a continuidade dos serviços, incluindo sistemas de Backup, manutenção de equipamentos, testes e plano de contingência de hardware e serviços críticos.				X		
ES5	**Garante a segurança dos sistemas.** A empresa dispõe de políticas de segurança, visa a preservação da confidencialidade, da integridade e da disponibilidade da informação.			X			
ES7	**Educa e treina os usuários.** A empresa mantém um plano de treinamento de usuários e profissionais de TI para uso eficaz e eficiente dos sistemas de informação.			X			
ES8	**Gerencia a central de serviços e incidentes.** Existe o registro e controle das solicitações e incidências de TI.		X				
ES9	**Gerencia a configuração.** A empresa dispõe de um repositório/registro das configurações de hardware e software com o objetivo de minimizar e resolver problemas com mais agilidade.		X				
ES10	**Gerencia os problemas.** Existe uma metodologia de ações corretivas e preventivas para os problemas de TI.			X			
ES11	**Gerencia os dados.** Define o ciclo de vida da informação, com definição de prazos para disponibilidade, arquivo morto e descarte de acordo com os requisitos do negócio e da legislação.			X			
ES12	**Gerencia a infra-estrutura.** Existe uma definição dos requisitos físicos e controle do ambiente físico para os equipamentos de TI, incluindo fatores ambientais, de acesso, instalações entre outros.			X			
ES13	**Gerenciar operações.** Administra o funcionamento das operações de TI			X			
ME - Medição e monitoramento.							
MO1	**Monitora e avalia a desempenho de TI.** Utiliza indicadores para monitorar e gerenciar o desempenho dos processos de TI.		X				
MO2	**Monitora e avalia o controle interno.** Estabelece mecanismos de controle interno dos requisitos da área e monitora a sua execução.		X				
MO3	**Assegura a conformidade aos requisitos externos.** Estabelece processo de revisão dos requisitos de legislação, contratuais e de negócio.			X			
MO4	**Fornecer governança de TI.** Estabelece um efetivo modelo de governança, que inclui definição da estrutura organizacional, processos, liderança, perfis e responsabilidades, a fim de garantir que os investimentos estejam alinhados às estratégias da organização.		X				

Anexo B – Questionários de avaliação das práticas de segurança da informação

Avaliador: Bruno Jorge dos Santos Luz
Data: 11/07/2009

O instrumento a seguir tem por objetivo avaliar a adequação aos controles relacionados à segurança considerando a norma - ISO/IEC 27002. Tecnologia da Informação – Código de prática para a gestão da segurança da informação considerando os seguintes níveis:

1 – Proteção inadequada: Não existe nenhum esforço da organização em implementar qualquer um dos controles recomendados para as suas necessidades específicas. Produtos e equipamentos certificados não têm qualquer influência na classificação das seções neste nível.

2 – Proteção mínima: A organização demonstra o mínimo de esforço na adoção de alguns dos controles recomendados. Produtos e equipamentos certificados não têm qualquer influência na classificação das seções neste nível.

3 – Proteção reativa: A maioria dos controles são implementados e devem satisfazer os requisitos com base procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso.

4 – Proteção adequada: Implementa todos os controles recomendados pelo domínio. Sempre que possível é obrigatório o uso de produtos e equipamentos certificados.

N/A – Não aplicável: Considerando o segmento ou a estrutura da empresa, tal controle não se aplica.

Quadro de análise:

Na coluna avaliação, marque com um “x” na coluna que você considera que a respectiva prática de segurança se encontra:

Prática de segurança	***Proteção***				
	1 – inadequada	2 – Mínima	3 – Reativa	4 – Adequada	Não aplicável
5 - Política de segurança da informação (PL).	***0***	***0***	***2***	***0***	***0***
5.1.1 Documento da política de segurança da informação.			X		
5.1.2 Análise crítica da política de segurança da informação.			X		
6 - Organizando a segurança da informação (OI).	***2***	***3***	***5***	***0***	***0***
6.1.1 Comprometimento da direção com a segurança da informação.		X			
6.1.2 Coordenação da segurança da informação.	X				
6.1.4 Processo de autorização para os recursos de processamento da informação.			X		
6.1.5 Acordos de confidencialidade.			X		
6.1.6 Contato com autoridades.			X		
6.1.7 Contato com grupos especiais.	X				
6.1.8 Análise crítica independente de segurança da informação.		X			
6.2.1 Identificação dos riscos relacionados com partes externas.			X		
6.2.2 Identificando a segurança da informação, quando tratando com os clientes.			X		
6.2.3 Identificando segurança da informação nos acordos com terceiros.		X			
7 - Gestão de ativos (GA).	***0***	***1***	***2***	***1***	***0***
7.1.1 Inventário dos ativos.			X		
7.1.2 Proprietário dos ativos.				X	
7.2.1 Recomendações para classificação.			X		
7.2.2 Rótulos e tratamento da informação.		X			
8- Segurança em recursos humanos (RH).	***1***	***5***	***1***	***0***	***0***
8.1.1 Papéis e responsabilidades.		X			
8.1.2 Seleção.			X		
8.1.3 Termos e condições de contratação.		X			
8.2.2 Conscientização, educação e treinamento em segurança da informação.	X				
8.2.3 Processo disciplinar.		X			
8.3.1 Encerramento de atividades.		X			

8.3.3 Retirada de direitos de acesso.		X			
9 - Segurança física e do ambiente (SA).	***1***	***9***	***2***	***0***	***1***
9.1.1 Perímetro de segurança física.		X			
9.1.2 Controles de entrada física.			X		
9.1.3 Segurança em escritórios, salas e instalações.		X			
9.1.4 Proteção contra ameaças externas e do meio ambiente.		X			
9.1.5 Trabalhando em áreas seguras.					X
9.1.6 Acesso do público, áreas de entrega e de carregamento.		X			
9.2.1 Instalação e proteção do equipamento.		X			
9.2.2 Utilidades.		X			
9.2.3 Segurança do cabeamento.	X				
9.2.4 Manutenção dos equipamentos.		X			
9.2.5 Segurança de equipamentos fora das dependências da organização.		X			
9.2.6 Reutilização e alienação segura de equipamentos.			X		
9.2.7 Remoção de propriedade.		X			
10 - Gerenciamento das operações e comunicações (GO).	***6***	***9***	***12***	***1***	***2***
10.1.1 Documentação dos procedimentos de operação.			X		
10.1.2 Gestão de mudanças.	X				
10.1.3 Segregação de funções.	X				
10.1.4 Separação dos recursos de desenvolvimento, teste e de produção.		X			
10.2.1 Entrega de serviços.		X			
10.2.2 Monitoramento e análise crítica de serviços terceirizados.			X		
10.2.3 Gerenciamento de mudanças para serviços terceirizados.			X		
10.3.1 Gestão de capacidade.		X			
10.3.2 Aceitação de sistemas.		X			
10.4.1 Controles contra códigos maliciosos.			X		
10.4.2 Controles contra códigos móveis.		X			
10.5.1 Cópias de segurança das informações.			X		
10.6.1 Controles de redes.			X		
10.6.2 Segurança dos serviços de rede.				X	
10.7.1 Gerenciamento de mídias removíveis.	X				
10.7.2 Descarte de mídias.		X			
10.7.3 Procedimentos para tratamento de informação.	X				
10.7.4 Segurança da documentação dos sistemas.			X		
10.8.1 Políticas e procedimentos para troca de informações.			X		
10.8.2 Acordos para a troca de informações.	X				
10.8.3 Mídias em trânsito.	X				
10.8.4 Mensagens eletrônicas.			X		
10.9.1 Comércio eletrônico.					X
10.9.2 Transações on-line.					X

10.10.1 Registros de auditoria.			X		
10.10.2 Monitoramento do uso do sistema.			X		
10.10.3 Proteção das informações dos registros (*log*).		X			
10.10.4 Registros (l*og*) de administrador e operador.		X			
10.10.5 Registros (*log*) de falhas.		X			
10.10.6 Sincronização dos relógios.			X		
11 - Controle de acessos (CA).	***4***	***8***	***5***	***5***	***1***
11.1.1 Política de controle de acesso.			X		
11.2.1 Registro de usuário.			X		
11.2.2 Gerenciamento de privilégios.		X			
11.2.4 Análise crítica dos direitos de acesso de usuário.		X			
11.3.1 Uso de senhas.		X			
11.3.2 Equipamento de usuário sem monitoração.	X				
11.3.3 Política de mesa limpa e tela limpa.	X				
11.4.1 Política de uso dos serviços de rede.				X	
11.4.2 Autenticação para conexão externa do usuário.				X	
11.4.3 Identificação de equipamento em redes.			X		
11.4.4 Proteção e configuração de portas de diagnóstico remotas.				X	
11.4.5 Segregação de redes.				X	
11.4.6 Controle de conexão de rede.			X		
11.4.7 Controle de roteamento de redes.			X		
11.5.1 Procedimentos seguros de entrada no sistema (*log-on*).		X			
11.5.3 Sistema de gerenciamento de senha.		X			
11.5.4 Uso de utilitários de sistema.		X			
11.5.5 Desconexão de terminal por inatividade.	X				
11.5.6 Limitação de horário de conexão.	X				
11.6.1 Restrição de acesso à informação.				X	
11.6.2 Isolamento de sistemas sensíveis.					X
11.7.1 Computação e comunicação móvel.		X			
11.7.2 Trabalho remoto.		X			
12 - Aquisição, desenvolvimento e manutenção de sistemas de informação (AQ).	***2***	***11***	***3***	***0***	***0***
12.1.1 Análise e especificação dos requisitos de segurança.		X			
12.2.1 Validação dos dados de entrada.		X			
12.2.2 Controle do processamento interno.		X			
12.2.3 Integridade de mensagens.		X			
12.2.4 Validação de dados de saída.		X			
12.3.1 Política para o uso de controles criptográficos.			X		
12.3.2 Gerenciamento de chaves.			X		
12.4.1 Controle de software operacional.	X				
12.4.2 Proteção dos dados para teste de sistema.	X				
12.4.3 Controle de acesso ao código-fonte de programa.		X			
12.5.1 Procedimentos para controle de mudanças.		X			

12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.		X			
12.5.3 Restrições sobre mudanças em pacotes de software.			X		
12.5.4 Vazamento de informações.		X			
12.5.5 Desenvolvimento terceirizado de software.		X			
12.6.1 Controle de vulnerabilidades técnicas.		X			
13 - Gestão de incidentes de segurança da informação (GI).	***3***	***2***	***0***	***0***	***0***
13.1.1 Notificação de eventos de segurança da informação	X				
13.1.2 Notificando fragilidades de segurança da informação.	X				
13.2.1 Responsabilidades e procedimentos.		X			
13.2.2 Aprendendo com os incidentes de segurança da informação.	X				
13.2.3 Coleta de evidências.		X			
14 - Gestão da continuidade do negócio (GC).	***0***	***3***	***2***	***0***	***0***
14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio.		X			
14.1.2 Continuidade de negócios e análise/avaliação de riscos.		X			
14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação.			X		
14.1.4 Estrutura do plano de continuidade do negócio.			X		
14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.		X			
15 - Conformidade (CF).	***3***	***2***	***4***	***0***	***0***
15.1.1 Identificação da legislação vigente.		X			
15.1.2 Direitos de propriedade intelectual.			X		
15.1.3 Proteção de registros organizacionais.		X			
15.1.4 Proteção de dados e privacidade de informações pessoais.					
15.1.5 Prevenção de mau uso de recursos de processamento da informação.	X				
15.1.6 Regulamentação de controles de criptografia.			X		
15.2.1 Conformidade com as políticas e normas de segurança da informação.			X		
15.2.2 Verificação da conformidade técnica.			X		
15.3.1 Controles de auditoria de sistemas de informação.	X				
15.3.2 Proteção de ferramentas de auditoria de sistemas de informação.	X				

Avaliador: Intranetworks Soluções Corporativas Ltda

Data: 12/07/2009

O instrumento a seguir tem por objetivo avaliar a adequação aos controles relacionados à segurança considerando a norma - ISO/IEC 27002. Tecnologia da

Informação – Código de prática para a gestão da segurança da informação considerando os seguintes níveis:

1 – Proteção inadequada: Não existe nenhum esforço da organização em implementar qualquer um dos controles recomendados para as suas necessidades específicas. Produtos e equipamentos certificados não têm qualquer influência na classificação das seções neste nível.

2 – Proteção mínima: A organização demonstra o mínimo de esforço na adoção de alguns dos controles recomendados. Produtos e equipamentos certificados não têm qualquer influência na classificação das seções neste nível.

3 – Proteção reativa: A maioria dos controles são implementados e devem satisfazer os requisitos com base procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso.

4 – Proteção adequada: Implementa todos os controles recomendados pelo domínio. Sempre que possível é obrigatório o uso de produtos e equipamentos certificados.

N/A – Não aplicável: Considerando o segmento ou a estrutura da empresa, tal controle não se aplica.

Quadro de análise:

Na coluna avaliação, marque com um “x” na coluna que você considera que a respectiva prática de segurança se encontra:

Prática de segurança	***Proteção***				
	1 – inadequada	2 – Mínima	3 – Reativa	4 – Adequada	Não aplicável

5 - Política de segurança da informação (PL).	***0***	***2***	***0***	***0***	***0***
5.1.1 Documento da política de segurança da informação.		x			
5.1.2 Análise crítica da política de segurança da informação.		x			
6 - Organizando a segurança da informação (OI).	***1***	***6***	***2***	***0***	***0***
6.1.1 Comprometimento da direção com a segurança da informação.		x			
6.1.2 Coordenação da segurança da informação.			x		
6.1.4 Processo de autorização para os recursos de processamento da informação.		x			
6.1.5 Acordos de confidencialidade.			x		
6.1.6 Contato com autoridades.		x			
6.1.7 Contato com grupos especiais.	x				
6.1.8 Análise crítica independente de segurança da informação.		x			
6.2.1 Identificação dos riscos relacionados com partes externas.		x			
6.2.2 Identificando a segurança da informação, quando tratando com os clientes.			x		
6.2.3 Identificando segurança da informação nos acordos com terceiros.		x			
7 - Gestão de ativos (GA).	***0***	***4***	***0***	***0***	***0***
7.1.1 Inventário dos ativos. 2		x			
7.1.2 Proprietário dos ativos.		x			
7.2.1 Recomendações para classificação.		x			
7.2.2 Rótulos e tratamento da informação.		x			
8 - Segurança em recursos humanos (RH).	***1***	***3***	***1***	***2***	***0***
8.1.1 Papéis e responsabilidades.				x	
8.1.2 Seleção.		x			
8.1.3 Termos e condições de contratação.		x			
8.2.2 Conscientização, educação e treinamento em segurança da informação.		x			
8.2.3 Processo disciplinar.			x		
8.3.1 Encerramento de atividades.	x				
8.3.3 Retirada de direitos de acesso.				x	
9 - Segurança física e do ambiente (SA).	***0***	***8***	***2***	***2***	***1***
9.1.1 Perímetro de segurança física.		x			
9.1.2 Controles de entrada física.		x			
9.1.3 Segurança em escritórios, salas e instalações.		x			
9.1.4 Proteção contra ameaças externas e do meio ambiente.			x		
9.1.5 Trabalhando em áreas seguras.					x
9.1.6 Acesso do público, áreas de entrega e de carregamento.		x			
9.2.1 Instalação e proteção do equipamento.		x			
9.2.2 Utilidades.		x			
9.2.3 Segurança do cabeamento.			x		
9.2.4 Manutenção dos equipamentos.				x	

9.2.5 Segurança de equipamentos fora das dependências da organização.		x			
9.2.6 Reutilização e alienação segura de equipamentos.		x			
9.2.7 Remoção de propriedade.				x	
10 - Gerenciamento das operações e comunicações (GO).	***3***	***9***	***12***	***4***	***2***
10.1.1 Documentação dos procedimentos de operação.		x			
10.1.2 Gestão de mudanças.		x			
10.1.3 Segregação de funções.		x			
10.1.4 Separação dos recursos de desenvolvimento, teste e de produção.		x			
10.2.1 Entrega de serviços.		x			
10.2.2 Monitoramento e análise crítica de serviços terceirizados.				x	
10.2.3 Gerenciamento de mudanças para serviços terceirizados.				x	
10.3.1 Gestão de capacidade.			x		
10.3.2 Aceitação de sistemas.		x			
10.4.1 Controles contra códigos maliciosos.			x		
10.4.2 Controles contra códigos móveis.			x		
10.5.1 Cópias de segurança das informações.			x		
10.6.1 Controles de redes.			x		
10.6.2 Segurança dos serviços de rede.				x	
10.7.1 Gerenciamento de mídias removíveis.	x				
10.7.2 Descarte de mídias.		x			
10.7.3 Procedimentos para tratamento de informação.	x				
10.7.4 Segurança da documentação dos sistemas.			x		
10.8.1 Políticas e procedimentos para troca de informações.		x			
10.8.2 Acordos para a troca de informações.		x			
10.8.3 Mídias em trânsito.	x				
10.8.4 Mensagens eletrônicas.			x		
10.9.1 Comércio eletrônico.					x
10.9.2 Transações on-line.					x
10.10.1 Registros de auditoria.			x		
10.10.2 Monitoramento do uso do sistema.			x		
10.10.3 Proteção das informações dos registros (*log*).			x		
10.10.4 Registros (*log*) de administrador e operador.			x		
10.10.5 Registros (*log*) de falhas.			x		
10.10.6 Sincronização dos relógios.				x	
11 - Controle de acessos (CA).	***4***	***4***	***12***	***1***	***1***
11.1.1 Política de controle de acesso.			x		
11.2.1 Registro de usuário.				x	
11.2.2 Gerenciamento de privilégios.			x		
11.2.4 Análise crítica dos direitos de acesso de usuário.			x		
11.3.1 Uso de senhas.		x			
11.3.2 Equipamento de usuário sem monitoração.	x				

11.3.3 Política de mesa limpa e tela limpa.	x				
11.4.1 Política de uso dos serviços de rede.			x		
11.4.2 Autenticação para conexão externa do usuário.			x		
11.4.3 Identificação de equipamento em redes.			x		
11.4.4 Proteção e configuração de portas de diagnóstico remotas.				x	
11.4.5 Segregação de redes.			x		
11.4.6 Controle de conexão de rede.			x		
11.4.7 Controle de roteamento de redes.			x		
11.5.1 Procedimentos seguros de entrada no sistema (*log-on*).			x		
11.5.3 Sistema de gerenciamento de senha.		x			
11.5.4 Uso de utilitários de sistema.		x			
11.5.5 Desconexão de terminal por inatividade.	x				
11.5.6 Limitação de horário de conexão.	x				
11.6.1 Restrição de acesso à informação.			x		
11.6.2 Isolamento de sistemas sensíveis.					x
11.7.1 Computação e comunicação móvel.		x			
11.7.2 Trabalho remoto.			x		
12- Aquisição, desenvolvimento e manutenção de sistemas de informação (AQ).	***3***	***7***	***6***	***0***	***0***
12.1.1 Análise e especificação dos requisitos de segurança.		x			
12.2.1 Validação dos dados de entrada.			x		
12.2.2 Controle do processamento interno.			x		
12.2.3 Integridade de mensagens.		x			
12.2.4 Validação de dados de saída.			x		
12.3.1 Política para o uso de controles criptográficos.	x				
12.3.2 Gerenciamento de chaves.		x			
12.4.1 Controle de software operacional.		x			
12.4.2 Proteção dos dados para teste de sistema.	x				
12.4.3 Controle de acesso ao código-fonte de programa.			x		
12.5.1 Procedimentos para controle de mudanças.		x			
12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.			x		
12.5.3 Restrições sobre mudanças em pacotes de software.			x		
12.5.4 Vazamento de informações.	x				
12.5.5 Desenvolvimento terceirizado de software.		x			
12.6.1 Controle de vulnerabilidades técnicas.		x			
13 - Gestão de incidentes de segurança da informação (GI).	***4***	***0***	***2***	***0***	***0***
13.1.1 Notificação de eventos de segurança da informação	x				
13.1.2 Notificando fragilidades de segurança da informação.	x		x		
13.2.1 Responsabilidades e procedimentos.			x		
13.2.2 Aprendendo com os incidentes de segurança da informação.	x				
13.2.3 Coleta de evidências.	x				

14 - Gestão da continuidade do negócio (GC).	***0***	***2***	***3***	***0***	***0***
14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio.			x		
14.1.2 Continuidade de negócios e análise/avaliação de riscos.			x		
14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação.		x			
14.1.4 Estrutura do plano de continuidade do negócio.			x		
14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.		x			
15 - Conformidade (CF).	***3***	***3***	***4***	***0***	***0***
15.1.1 Identificação da legislação vigente.		x			
15.1.2 Direitos de propriedade intelectual.		x			
15.1.3 Proteção de registros organizacionais.		x			
15.1.4 Proteção de dados e privacidade de informações pessoais.	x				
15.1.5 Prevenção de mau uso de recursos de processamento da informação.			x		
15.1.6 Regulamentação de controles de criptografia.			x		
15.2.1 Conformidade com as políticas e normas de segurança da informação.			x		
15.2.2 Verificação da conformidade técnica.			x		
15.3.1 Controles de auditoria de sistemas de informação.	x				
15.3.2 Proteção de ferramentas de auditoria de sistemas de informação.	x				

Anexo C - Práticas de segurança consolidadas por processo do COBIT

Processos COBIT	Práticas de segurança ISO/IEC27002	Analise consolidada
PO2 - Definir a arquitetura de informação.	7.1.1 Inventário dos ativos. 7.2.1 Recomendações para classificação. 10.7.1 Gerenciamento de mídias removíveis. 10.9.1 Comércio eletrônico. 10.9.2 Transações on-line. 11.1.1 Política de controle de acesso.	- A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários. - A informação não é classificada por nível de confidencialidade. - A empresa mantém um inventário de ativos de software e hardware.
PO9 - Avaliar e gerenciar riscos.	5.1.2 Análise crítica da política de segurança da informação. 13.1.2 Notificando fragilidades de segurança da informação. 13.1.1 Notificação de eventos de segurança da informação. 14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio. 14.1.2 Continuidade de negócios e análise/avaliação de riscos.	- A empresa mantém um plano de contingenciamento para os serviços considerados críticos para o negócio. - A empresa realiza análise crítica da segurança da informação em nível operacional. O assunto não é tradado pela direção da empresa.
AI2 - Adquirir e manter software aplicativo.	6.1.4 Processo de autorização para os recursos de processamento da informação. 7.2.1 Recomendações para classificação. 10.3.2 Aceitação de sistemas. 10.10.1 Registros de auditoria. 10.10.5 Registros (*log*) de falhas. 11.6.2 Isolamento de sistemas sensíveis. 12.1.1 Análise e especificação dos requisitos de segurança. 12.2.1 Validação dos dados de entrada. 12.2.2 Controle do processamento interno. 12.2.3 Integridade de mensagens. 12.2.4 Validação de dados de saída.	- A informação não é classificada por nível de confidencialidade. - O desenvolvimento de sistemas realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente. - São realizadas auditorias eventuais do uso dos sistemas de informação.

	12.3.1 Política para o uso de controles criptográficos.	
	12.4.3 Controle de acesso ao código-fonte de programa.	
	12.5.1 Procedimentos para controle de mudanças.	
	12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.	
	12.5.3 Restrições sobre mudanças em pacotes de software.	
	12.5.4 Vazamento de informações.	
	12.5.5 Desenvolvimento terceirizado de software.	
	13.2.3 Coleta de evidências.	
	15.3.1 Controles de auditoria de sistemas de informação.	
	15.3.2 Proteção de ferramentas de auditoria de sistemas de informação.	
AI3 - Adquirir e manter arquitetura tecnológica.	9.1.5 Trabalhando em áreas seguras.	- Não existe um plano de manutenção dos equipamentos que executam serviços críticos, porém existe um plano de contingenciamento destes equipamentos. - É realizada a separação dos recursos de desenvolvimento, testes e produção, porém não há procedimentos documentados. - As informações dos setores de pesquisa e desenvolvimento são tratadas como as demais informações. - A empresa realiza análise crítica da segurança da informação em nível operacional.
	9.2.4 Manutenção dos equipamentos.	
	10.1.4 Separação dos recursos de desenvolvimento, teste e de produção.	
	10.4.2 Controles contra códigos móveis.	
	12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.	
	12.6.1 Controle de vulnerabilidades técnicas.	
AI4 - Desenvolver e manter procedimentos de TI.	10.1.1 Documentação dos procedimentos de operação.	- São mantidos alguns manuais de sistemas, porém estão desatualizados. - A empresa mantém políticas e recomendações de uso dos sistemas de informação para os usuários. - A empresa dispõe de um controle para
	10.3.2 Aceitação de sistemas.	
	10.7.4 Segurança da documentação dos sistemas.	
	13.2.2 Aprendendo com os incidentes de segurança da informação.	

		elaboração e revisão de documentos conforme requisitos da ISO9000.
AI5 - Obter recursos de TI.	6.1.5 Acordos de confidencialidade.	- São mantidos acordos de confidencialidade com terceiros através de contratos.
	6.2.3 Identificando segurança da informação nos acordos com terceiros.	
	10.8.2 Acordos para a troca de informações.	
	12.5.5 Desenvolvimento terceirizado de software.	
AI6 - Gerenciar mudanças.	10.1.2 Gestão de mudanças.	- A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários. - As informações são protegidas por senhas, porém não é mantida uma política de senhas segura. - Não há uma gestão de mudanças de sistemas e infra-estrutura. Este processo ocorre informalmente.
	11.5.1 Procedimentos seguros de entrada no sistema (*log-on*).	
	11.5.4 Uso de utilitários de sistema.	
	11.6.1 Restrição de acesso à informação.	
	12.5.3 Restrições sobre mudanças em pacotes de software.	
AI7 - Instalar e certificar soluções e mudanças.	6.1.4 Processo de autorização para os recursos de processamento da informação.	- O processo de aquisição dos recursos operacionais é realizado em conjunto com o setor de informática, a decisão é por parte dos setores e a especificação técnica é de informática. A liberação de recursos para aquisição de equipamentos rede e serviços comuns a empresa é do setor administrativo. - Não são realizados treinamentos sobre a segurança da informação. - É realizada a separação dos recursos de desenvolvimento, testes e produção, porém não existem procedimentos documentos. - O desenvolvimento de sistemas realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente.
	8.2.2 Conscientização, educação e treinamento em segurança da informação.	
	10.1.4 Separação dos recursos de desenvolvimento, teste e de produção.	
	10.3.2 Aceitação de sistemas.	
	12.4.3 Controle de acesso ao código-fonte de programa.	
	12.5.1 Procedimentos para controle de mudanças.	
	12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.	
	12.5.4 Vazamento de informações.	

ES1 - Definir níveis de serviços.	10.2.1 Entrega de serviços. 10.2.2 Monitoramento e análise crítica de serviços terceirizados. 10.2.3 Gerenciamento de mudanças para serviços terceirizados.	- Não existe um processo formal para seleção, avaliação e monitoramento de fornecedores de TI. - São mantidos contratos com os terceirizados. - O desenvolvimento de sistemas realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente.
ES2 - Gerenciar serviços de terceiros.	6.2.1 Identificação dos riscos relacionados com partes externas. 6.2.3 Identificando segurança da informação nos acordos com terceiros. 8.1.2 Seleção. 8.1.3 Termos e condições de contratação. 10.2.1 Entrega de serviços. 10.2.2 Monitoramento e análise crítica de serviços terceirizados. 10.8.2 Acordos para a troca de informações. 10.2.3 Gerenciamento de mudanças para serviços terceirizados. 12.4.1 Controle de software operacional. 12.5.5 Desenvolvimento terceirizado de software. 15.1.4 Proteção de dados e privacidade de informações pessoais.	- Não existe um processo formal para seleção, avaliação e monitoramento de fornecedores de TI. - São mantidos contratos com os terceirizados incluindo cláusulas de confidencialidade da informação. - São implementadas reuniões de analise crítica com os terceirizados dos serviços considerados críticos. - A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por colaborador de acordo com suas atividades e responsabilidades. - O desenvolvimento de sistemas realizado internamente e externamente. Não há evidencia de um processo documentado e controlado para o desenvolvimento de sistemas. A aceitação dos sistemas é realizada informalmente.
ES3 - Gerenciar desempenho e capacidade.	10.3.1 Gestão de capacidade.	- A empresa possui boa capacidade e disponibilidade de sistemas, porém o hardware é obsoleto e não é de procedência confiável.
ES4 - Garantir continuidade dos serviços.	6.1.6 Contato com autoridades.	- É mantida uma assessoria para tratar de

	6.1.7 Contato com grupos especiais.	assuntos com autoridades e grupos especiais. - É mantido e documentado um sistema de backup. - A empresa dispõe de um inventário de ativos de hardware e software com um plano de contingência dos serviços críticos, porém não são realizados testes e auditorias para verificar a disponibilidade em casos de desastres.
	10.5.1 Cópias de segurança das informações.	
	14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio.	
	14.1.2 Continuidade de negócios e análise/avaliação de riscos.	
	14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação.	
	14.1.4 Estrutura do plano de continuidade do negócio.	
	14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.	
ES5 - Garantir segurança dos sistemas.	5.1.1 Documento da política de segurança da informação.	- A empresa realiza análise crítica da segurança da informação em nível operacional. - A empresa mantém políticas de controle de acesso e recomendações de uso por tipo de informação e grupos de usuários incluindo processos disciplinares. - Os contratos com terceiros incluem acordos de confidencialidade da informação. - A coordenação da segurança da informação é realizada pela TI. Não existe a participação da direção da empresa em assuntos relacionados a segurança da informação. - Não existe um fórum específico para tratar a segurança da informação. - O acesso por terceiros aos sistemas e informações da empresa não é tratado nas políticas de segurança. - Não são realizados treinamentos sobre a segurança da informação. - A empresa dispõe de políticas de seleção e qualificação dos funcionários. É mantido um plano de treinamento e desenvolvimento por
	5.1.2 Análise crítica da política de segurança da informação.	
	6.1.1 Comprometimento da direção com a segurança da informação.	
	6.1.5 Acordos de confidencialidade.	
	6.1.2 Coordenação da segurança da informação.	
	6.1.8 Análise crítica independente de segurança da informação.	
	6.2.1 Identificação dos riscos relacionados com partes externas.	
	6.2.2 Identificando a segurança da informação, quando tratando com os clientes.	
	6.2.3 Identificando segurança da informação nos acordos com terceiros.	
	8.1.1 Papéis e responsabilidades.	
	8.2.2 Conscientização, educação e treinamento em segurança da informação.	
	8.2.3 Processo disciplinar.	
	8.3.1 Encerramento de atividades.	
	8.3.3 Retirada de direitos de acesso.	
	9.1.6 Acesso do público, áreas de entrega e de carregamento.	
	9.2.1 Instalação e proteção do equipamento.	
	9.2.3 Segurança do cabeamento.	

	10.1.3 Segregação de funções.	colaborador de acordo com suas atividades e responsabilidades. - A empresa dispõe de antivírus, porém não dispõe de sistema de detecção de intrusos. - A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000. - São realizadas auditorias eventuais nos sistemas da empresa em busca de uso indevido dos recursos de TI. - As informações são protegidas por senhas, porém não existe uma política de senha segura. - A empresa dispõe de um inventário de hardware com identificação dos equipamentos. - A infra-estrutura de rede da empresa é tratada de forma reativa e não segue padrão recomendado. Não é certificada. - A empresa não usa criptografia de dados. - Não esta prevista nas políticas de segurança práticas de desconexões por inatividades. - Os acessos remotos são realizados utilizando VPN.
	10.4.1 Controles contra códigos maliciosos.	
	10.4.2 Controles contra códigos móveis.	
	10.6.1 Controles de redes.	
	10.7.4 Segurança da documentação dos sistemas.	
	10.8.4 Mensagens eletrônicas.	
	10.10.1 Registros de auditoria.	
	10.10.2 Monitoramento do uso do sistema.	
	10.10.3 Proteção das informações dos registros (*log*).	
	10.10.4 Registros (*log*) de administrador e operador.	
	10.10.5 Registros (*log*) de falhas.	
	10.10.6 Sincronização dos relógios.	
	11.1.1 Política de controle de acesso.	
	11.2.1 Registro de usuário.	
	11.2.2 Gerenciamento de privilégios.	
	11.2.4 Análise crítica dos direitos de acesso de usuário.	
	11.3.1 Uso de senhas.	
	11.3.2 Equipamento de usuário sem monitoração.	
	11.3.3 Política de mesa limpa e tela limpa.	
	11.4.1 Política de uso dos serviços de rede.	
	11.4.2 Autenticação para conexão externa do usuário.	
	11.4.3 Identificação de equipamento em redes.	
	11.4.4 Proteção e configuração de portas de diagnóstico remotas.	
	11.4.5 Segregação de redes.	
	11.4.6 Controle de conexão de rede.	
	11.4.7 Controle de roteamento de redes.	
	11.5.1 Procedimentos seguros de entrada no sistema (*log-on*).	
	11.5.3 Sistema de gerenciamento de senha.	
	11.5.4 Uso de utilitários de sistema.	
	11.5.5 Desconexão de terminal por inatividade.	
	11.5.6 Limitação de horário de conexão.	
	11.6.2 Isolamento de sistemas sensíveis.	
	11.7.1 Computação e comunicação móvel.	

	11.7.2 Trabalho remoto.	
	12.2.3 Integridade de mensagens.	
	12.3.1 Política para o uso de controles criptográficos.	
	12.3.2 Gerenciamento de chaves.	
	12.4.1 Controle de software operacional.	
	12.6.1 Controle de vulnerabilidades técnicas.	
	13.1.1 Notificação de eventos de segurança da informação.	
	13.1.2 Notificando fragilidades de segurança da informação.	
	13.2.1 Responsabilidades e procedimentos.	
	13.2.3 Coleta de evidências.	
	14.1.4 Estrutura do plano de continuidade do negócio.	
	15.1.6 Regulamentação de controles de criptografia.	
	15.2.2 Verificação da conformidade técnica.	
	15.3.1 Controles de auditoria de sistemas de informação.	
	15.3.2 Proteção de ferramentas de auditoria de sistemas de informação.	
ES9 - Gerenciar a configuração.	7.1.2 Proprietário dos ativos.	- A empresa mantém políticas de controle de acesso e recomendações de uso por tipo de informação e grupos de usuários incluindo processos disciplinares. - As informações são protegidas por senhas, porém não existe uma política de senha segura. - A empresa dispõe de um inventário de ativos de hardware e software com um plano de contingência dos serviços críticos, porém não são realizados testes e auditorias para verificar a disponibilidade em casos de desastres. - Os servidores estão protegidos fisicamente em uma sala de servidores com controle de acesso. - A empresa realiza análise crítica da segurança da informação em nível operacional.
	7.2.2 Rótulos e tratamento da informação.	
	10.7.4 Segurança da documentação dos sistemas.	
	11.4.3 Identificação de equipamento em redes.	
	12.4.1 Controle de software operacional.	
	12.4.2 Proteção dos dados para teste de sistema.	
	12.6.1 Controle de vulnerabilidades técnicas.	
	12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional.	
	12.5.3 Restrições sobre mudanças em pacotes de software.	
	15.1.5 Prevenção de mau uso de recursos de processamento da informação.	

ES10 - Gerenciar problemas.	13.2.2 Aprendendo com os incidentes de segurança da informação.	- A empresa não mantém um banco de conhecimentos com os incidentes. Reativamente são tomadas ações para que os incidentes não se repitam.
ES11 - Gerenciar dados.	9.2.6 Reutilização e alienação segura de equipamentos. 10.5.1 Cópias de segurança das informações. 10.7.1 Gerenciamento de mídias removíveis. 10.7.2 Descarte de mídias. 10.7.3 Procedimentos para tratamento de informação. 10.8.1 Políticas e procedimentos para troca de informações. 10.8.3 Mídias em trânsito. 10.8.4 Mensagens eletrônicas. 12.4.2 Proteção dos dados para teste de sistema. 12.4.3 Controle de acesso ao código-fonte de programa. 15.1.3 Proteção de registros organizacionais.	- Não existem procedimentos para descarte de informações e equipamentos que contenham informações. - Não existem procedimentos para troca de informações. - As informações são protegidas por senhas, porém não existe uma política de senha segura.
ES12 - Gerenciar os ambientes físicos.	6.2.1 Identificação dos riscos relacionados com partes externas. 9.1.1 Perímetro de segurança física. 9.1.2 Controles de entrada física. 9.1.3 Segurança em escritórios, salas e instalações. 9.1.4 Proteção contra ameaças externas e do meio ambiente. 9.1.5 Trabalhando em áreas seguras. 9.1.6 Acesso do público, áreas de entrega e de carregamento. 9.2.2 Utilidades. 9.2.3 Segurança do cabeamento. 9.2.4 Manutenção dos equipamentos. 9.2.5 Segurança de equipamentos fora das dependências da organização. 9.2.7 Remoção de propriedade.	- Os acessos remotos são realizados utilizando VPN. Porém não identificados os riscos relacionados com partes externas. - Os servidores estão protegidos fisicamente em uma sala de servidores com controle de acesso. - Não há proteção para os equipamentos de rede e estações de trabalho. - A manutenção dos equipamentos operacionais é realizada de forma reativa. Para equipamentos que executam serviços críticos existe um plano de contingenciamento. - Não estão previstos nas políticas de TI diretrizes sobre remoção de ativos.
ES13 - Gerenciar operações.	9.2.4 Manutenção dos equipamentos. 10.1.1 Documentação dos procedimentos de	- A manutenção dos equipamentos operacionais

	operação.	é realizada de forma reativa.
	10.7.4 Segurança da documentação dos sistemas.	- A empresa dispõe de um controle para elaboração e revisão de documentos conforme requisitos da ISO9000. - São mantidos alguns manuais de sistemas, porém estão desatualizados.
MO1 - Monitorar e avaliar a desempenho de TI.	10.2.2 Monitoramento e análise crítica de serviços terceirizados.	- São mantidos contratos com os terceirizados. - São realizadas reuniões de analise crítica com os terceirizados dos serviços considerados críticos.
MO2 - Monitorar e avaliar o controle interno.	5.1.1 Documento da política de segurança da informação.	- A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários. - A Empresa disponibiliza documentação com políticas de uso e recomendações de uso dos sistemas de informação. - A empresa realiza análise crítica da segurança da informação em nível operacional, porém não de forma independente. - A empresa mantém políticas e recomendações de uso dos sistemas de informação para os usuários. - São realizadas auditorias eventuais para verificar o uso dos sistemas de informação. - Não é implementado um processo de ações corretivas e preventivas para a segurança da informação.
	5.1.2 Análise crítica da política de segurança da informação.	
	6.1.8 Análise crítica independente de segurança da informação.	
	6.2.3 Identificando segurança da informação nos acordos com terceiros.	
	10.2.2 Monitoramento e análise crítica de serviços terceirizados.	
	10.10.2 Monitoramento do uso do sistema.	
	10.10.4 Registros (*log*) de administrador e operador.	
	15.2.1 Conformidade com as políticas e normas de segurança da informação.	
	15.2.2 Verificação da conformidade técnica.	
	15.3.1 Controles de auditoria de sistemas de informação.	
MO3 - Assegurar a conformidade regulatória.	6.1.6 Contato com autoridades.	- É mantida uma assessoria para tratar de assuntos com autoridades e grupos especiais. - A empresa disponibiliza documentação com
	15.1.1 Identificação da legislação vigente.	
	15.1.2 Direitos de propriedade intelectual.	
	15.1.4 Proteção de dados e privacidade de	

	informações pessoais.	políticas de uso e recomendações de uso dos sistemas de informação. - A empresa mantém um inventário de software.
MO4 - Fornecer governança de TI.	5.1.2 Análise crítica da política de segurança da informação.	- A empresa mantém políticas de controle de acesso documentadas por tipo de informação e grupos de usuários. - A empresa disponibiliza documentação com políticas de uso e recomendações de uso dos sistemas de informação. - A empresa realiza análise crítica da segurança da informação em nível operacional, porém não de forma independente.
	6.1.8 Análise crítica independente de segurança da informação.	
	10.10.2 Monitoramento do uso do sistema.	