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 INDUSTRIAL.

This paper expands the focus of technical and operational about information security in business considering essential strategic elements to finding the most appropriate practices for the business context. The aim of this study was to develop and implement a framework to promote strategic alignment between Business goals, Information Technology (TI) goals and Information Security Practices. For this, we performed the integration of models of the Balanced Scorecard (BSC) x Control Objectives for Information and related Technology (COBIT) x ISO/IEC27002 with practical application in an industrial automation company significantly dependent of information systems. The integration of these models included the basic requirements of information security: confidentiality, integrity and availability, resulting in a framework that make possible to analyzing the information security in the strategic, tactical and operational levels. The application of this framework in the company occurred in four steps: Verification of IT governance maturity, Verification of safety practices, and documents recovery. The results show that the company may have a significant improvement in the practices of information security, focusing mainly HR as culture aspects through techniques such as establishing policies, training and awareness.

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

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 INDUSTRIAL.

Esse artigo amplia o enfoque técnico e operacional envolvendo o tema da segurança da informação nas empresas, considerando elementos estratégicos essenciais na busca das práticas mais adequadas para o contexto do negócio. O objetivo deste trabalho foi desenvolver e aplicar um *framework* para promover o alinhamento estratégico entre os Objetivos de Negócio, Objetivos de Tecnologia da Informação (TI) e as Práticas de Segurança da Informação, sendo que estas últimas foram avaliadas e analisadas no contexto da governança de TI. Para este fim, foi realizada a integração dos modelos do *Balanced Scorecard (BSC)* x *Control Objectives for Information and related Technology* (COBIT) x ISO/IEC27002 com a aplicação prática em uma empresa de automação industrial, esta significativamente dependente de sistemas de informação. A integração destes modelos contemplou os requisitos básicos de negócio e de segurança da informação: Confidencialidade, Integridade e Disponibilidade, resultando em um *framework* que possibilitou analisar a segurança da informação nos níveis estratégico, tático e operacional da organização. A aplicação do Framework na empresa ocorreu em 4 etapas: Verificação da maturidade em governança de TI, Verificação das práticas de segurança, Entrevista e Recuperação documental. Os resultados revelam que a empresa pode ter uma melhoria significativa em relação às práticas de segurança da informação,

atuando principalmente aspectos de RH como cultura da organização através de técnicas como estabelecimento de políticas, treinamento e conscientização.

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

INTRODUÇÃO

A utilização de sistemas de informação em maior escala tornou complexa a sua gestão, principalmente porque também gerou maior vulnerabilidade da informação estratégica. Esta complexidade aliada à necessidade de alinhar as ações de TI com a estratégia organizacional sugere a utilização de modelos que atendam também a uma governança corporativa.

Os riscos para o negócio ocasionados pela vulnerabilidade da informação estratégica inerentes a um ambiente de TI passam muitas vezes despercebidos e isso pode reduzir consideravelmente a competitividade da empresa. Tal situação remete à necessidade de uma abordagem da segurança da informação não somente no nível operacional como normalmente é realizada, mas também em nível estratégico em qualquer organização.

Dependendo do grau de importância que a TI representa para o negócio como a que ocorre em empresas de significativo investimento em P&D e destaque competitivo em investimento tecnológico, a segurança da informação deve ser administrada em seu mais alto nível (POSTHUMOS e SOLMS, 2004), ou seja, no nível estratégico da empresa (FERNANDEZ e ABREU, 2008) e (ENTRUST, 2009). 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 (GTI) como parte da Governança Corporativa (GC). (ENTRUST, 2009). Allen e Westby (2007) também consideraram a segurança da informação como um problema da empresa e não somente da área de TI. A gestão da segurança da informação sustentada pela TI deve ser integrada com todos os níveis da organização e alinhada com os objetivos estratégicos.

Com o intuito de proteger melhor a infra-estrutura de TI o relatório do *Corporate Governance Task Force* propõe às empresas a incorporação de 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 ISO/IEC27002 devem ser incorporados e ampliados para o desenvolvimento de um modelo capaz de romper o plano tecnológico, alcançando e integrando as melhores práticas corporativas também num plano estratégico (BSA, 2003). Em função destas questões, o presente trabalho define a seguinte questão problema: Como desenvolver alinhamento estratégico entre objetivos de negócio, objetivos de TI e as práticas de segurança da informação?

FUNDAMENTAÇÃO TEÓRICA

GOVERNANCA DE TI (GTI)

A GTI pode ser considerada a forma pela qual se decide e que responsabilidades são direcionadas para um comportamento desejável no uso da TI (WEILL e ROSS, 2006). Outra definição afirma que a GTI é a parte integrante da governança empresarial constituída pelos dirigentes, estruturas organizacionais e processos para assegurar a ampliação das estratégias e objetivos através das práticas de TI (ITGI, 2009). Também a GTI pode ser considerada como a capacidade organizacional exercida pela diretoria e gerência executiva para controlar a formulação e implantação da estratégia de TI, esta que busque assegurar a integração entre negócio e TI (GREMBERGEN e HAES, 2004).

Na seqüência são apresentados resumidamente alguns dos modelos de GTI entre os mais conhecidos (BSC, COBIT, ITIL, CMMI, ISO/IEC27002), os quais tendem a uma gestão mais eficaz dos recursos de TI.

O *Balanced Scorecard (BSC)* é um modelo de alinhamento estratégico e 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. Foi desenvolvido por Kaplan e Norton e constitui um modelo de gestão estratégica baseado em indicadores financeiros e não-financeiros vinculados à estratégia organizacional divididos em quatro perspectivas: Financeira (F), Clientes (C), Processos Internos (P) e Aprendizado e Crescimento (A), (KAPLAN e NORTON, 1997).

O modelo de Governaça de TI *Control Objectives for Information and related Technology (COBIT)* é focado em controle e auditoria de Tecnologia da Informação. Este modelo propõe que os recursos de TI sejam gerenciados por processo de TI para atingir as metas orientadas por requisitos de negócio. O COBIT é um modelo desenvolvido pelo *Information System Audit and Control Association* (ISACA) e tem por objetivo identificar um relacionamento entre os requisitos de negócio, os recursos e os processos de TI para atender as necessidades da empresa. O modelo divide a função de TI em 34 processos organizados através de quatro domínios: Planejamento e Organização (PO), Aquisição e Implementação (AI), Entrega e Suporte (ES) e Monitoramento (MO). Cada domínio é composto por um conjunto de processos sendo estes compostos por atividades (IGTI, 2009).

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).

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). 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).

A norma ISO/IEC27002:2005 relativa à segurança da informação é de origem britânica, sendo que sua origem remonta a *A British Standard (BS)* 7799 a qual resultou na ISO/IEC17799. Posteriormente seu nome foi utilizado e atualizado para a ISO/IEC27002 em 2007 e desenvolvida no *Commercial Computer Security Centre (CCSC)* do departamento de indústria e comércio. A norma abrange 10 domínios reunidos em 36 grupos que totalizam 127 controles, estabelecendo um conjunto de práticas para manter e melhorar a gestão da segurança da informação em uma organização (FERNANDES e ABREU, 2008).

São considerados requisitos básicos de segurança da informação a manutenção dos requisitos de negócios relacionados à Confidencialidade, a Integridade e Disponibilidade (ITGI, 2009), (KWOK e LONGLEY, 1999), (FITZGERALD, 2007), (SÊMOLA, 2003), (DIAS, 2000), (MOREIRA, 2001). A dependência atual das organizações em relação a sua infra-estrutura de TI associada 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. Resumidamente, pode-se descrever estes requisitos conforme apresentado na continuação. **Confidencialidade (C)**: A proteção da informação de acordo com o grau de seu sigilo, visando a limitação de acesso e uso apenas pessoas as quais a informação é destinada; **Integridade (I):** A manutenção da informação nas condições em que foi disponibilizada pelo proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais; **Disponibilidade (D):** O acesso a informação gerada ou adquirida pelos seus destinatários no momento em que ela solicitada.

A norma ISO/IEC27002 ressalta que a informação é um ativo importante da organização, sendo que estes três elementos anteriormente descritos são essenciais para preservar a competitividade da empresa. Na seqüência são apresentados resumidamente os objetivos dos domínios da Norma em forma de capítulos, sendo que dando início no de número 5. Os capítulos 1 a 4 são introdutórios da norma e por isto se dá início somente no capítulo 5 da mesma, com a Política de segurança da informação.

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): Organizar a segurança da informação 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, assegurando que a informação receba um nível adequado de proteção.

8 - Segurança em recursos humanos (RH): Assegurar que os colaboradores, fornecedores e terceiros entendam suas responsabilidades estejam de acordo com os seus papéis reduzindo o risco de roubo, fraude e mal uso de recursos.

9 - Segurança física e do ambiente (SA): Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

10 - Gerenciamento das operações e comunicações (GO): Garantir a operação segura e correta dos recursos de processamento da informação. Manter a segurança na troca de informações e softwares internamente e quaisquer entidades externas.

11 - Controle de acessos (CA): Assegurar o acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.

12 - Aquisição, desenvolvimento e manutenção de sistemas de informação (AQ): Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mal uso de informações no processo de desenvolvimento e manutenção de aplicações e sistemas de informação.

13 - Gestão de incidentes de segurança da informação (GI): Assegurar que fragilidades e eventos de segurança da informação associadas com sistemas de informação sejam identificados, comunicados, permitindo a tomada de ações corretivas e preventivas em tempo hábil.

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

15 - Conformidade (CF): Assegurar a conformidade legal e obrigações contratuais dos sistemas de informação. Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.

Com o objetivo de verificar a conformidade da organização em relação aos 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:

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

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.

Proteção reativa: A maioria dos controles é implementada satisfazendo os requisitos com base em procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso.

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

Os capítulos da norma conjuntamente com as práticas anteriormente descritas formam um instrumento de avaliação da segurança da informação, sendo que nesta pesquisa foi aplicado para identificar o atual estágio que se encontram estas práticas de segurança na empresa estudada.

MÉTODO

É possível estabelecer um relacionamento estratégico utilizando-se dos critérios de segurança e integrando-os através dos modelos BSC, COBIT e ISO/IEC27002, conforme representado na Figura 1. Esses modelos facilitam o mapeamento de objetivos genéricos de negócio para a TI nas perspectivas do BSC com os objetivos genéricos de TI para o negócio, estes sugeridos pelo IGTI (2009). Na sequência, pode-se mapear os objetivos genéricos de TI para o negócio com os processos do COBIT que envolvem os requisitos de Confidencialidade, Integridade e Disponibilidade. Por fim, para um alcance técnico e operacional, este alinhamento pode ser complementado mapeando os processos do COBIT com as práticas da ISO/IEC27002.

Assim o processo de mapeamento resulta em um *Framework* envolvendo as seguintes etapas:

1) Identificação dos objetivos de negócios nas perspectivas do BSC;
2) Identificação dos objetivos de TI;
3) Mapeamento dos objetivos de TI com os objetivos de negócio;
4) Mapeamento dos objetivos de TI com os processos do COBIT com relação aos requisitos de segurança Confidencialidade, Integridade e Disponibilidade;
5) Mapeamento dos processos do COBIT com as práticas de segurança propostos pela ISO/IEC27002.

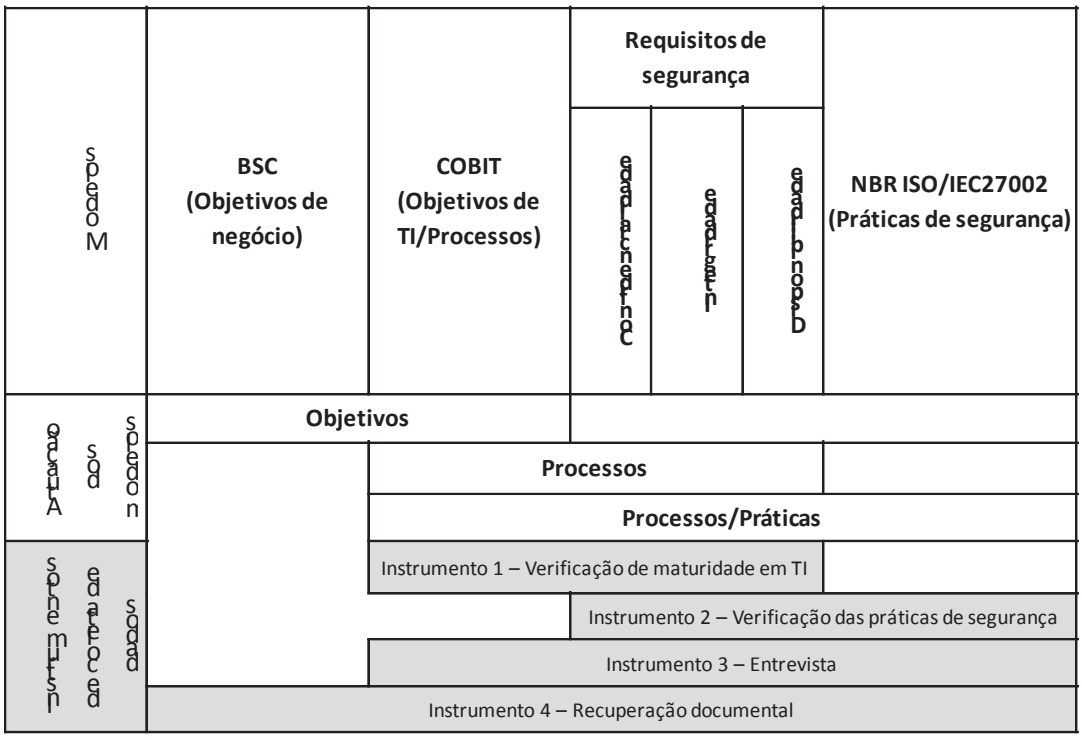


Figura 1: *Framework* de integração dos modelos BSC x COBIT x ISO/IEC27002
Fonte: KNORST (2010, pág. 68)

A figura1 apresenta a representa integração dos modelos com os requisitos de segurança da informação e o nível de atuação na estrutura organizacional. A figura também apresenta os instrumentos de coleta de dados que estão apresentados na sequencia metodológica.

Na seqüência, no quadro 1 é apresentado o mapeamento BSC x COBIT x ISO/IEC27002 em relação aos objetivos genéricos de TI que impactam nos requisitos de segurança, Confidencialidade, Integridade e Disponibilidade:

<table>
<tr><td colspan="5">1 - Responder aos requisitos do negócio de forma alinhados a estratégia do negócio</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></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">3 - Garantir a satisfação dos usuários finais com bons níveis de serviços</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></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">4 - Otimizar o uso da informação</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></tr>
<tr><td rowspan="2">C6</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">GA, SA, GO, CA, AQ, CF</td><td rowspan="2">I</td></tr>
<tr><td>PO2, ES11</td><td>-</td></tr>
<tr><td colspan="5">5 - Criar agilidade de TI.</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></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">10 - Garantir satisfação mútua em relacionamento com terceiros</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></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">11 - Garantir integração das aplicações com os processos de negócios</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></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">14 - Responder pelos ativos de TI e protegê-los</td></tr>
</table>

BSC	Processos COBIT		ISO/IEC27002	Requisitos de segurança
F2	Mapeados	Não mapeados	PL, OI, GA, RH, SA, GO, CA, AQ, GI, GC, CF	C, I, D
	PO9, ES5, ES9, ES12, MO2	-		
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		
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	-		
18 - Estabelecer clareza no impacto de riscos do negócio em relação a objetivos e recursos de TI.				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
F2, F3	Mapeados	Não mapeados	PL, GI, GC	C, I, D
	PO9	-		
19 - Assegurar que informações críticas e confidenciais são inacessíveis a aqueles que não devem ter acesso a elas.				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
F2, P3	Mapeados	Não mapeados	PL, OI, RH, SA, GO, CA, AQ, GI, GC, CF	C, I, D
	ES5, ES11, ES12	PO6		
20 - Garantir que as informações de negócio e transações automatizadas são confiáveis.				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
F2, C6, P3	Mapeados	Não mapeados	PL, OI, RH, SA, GO, CA, AQ, GI, GC, CF	I, D
	ES5	PO6, AI7		
21 - Garantir que os serviços e infra-estrutura de TI resistam a falhas em função de erros, ataques deliberados ou desastres.				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
F2, P3	Mapeados	Não mapeados	PL, OI, RH, SA, GO, CA, AQ, GI, GC, CF	I, D
	AI7, ES4, ES5, ES12, ES13, MO2	PO6		

<table>
<tr><td colspan="5">22 - Garantir impacto mínimo no negócio no caso de uma interrupção ou anormalidade em um serviço de TI.</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></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">23 - Assegurar que os serviços de TI estão disponíveis quando solicitados.</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></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">25 - Entregar projetos no prazo e nos orçamento previstos, observando padrões de qualidade</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></tr>
<tr><td rowspan="2">C4, A1</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">-</td><td rowspan="2">I</td></tr>
<tr><td>-</td><td>PO8, PO10</td></tr>
<tr><td colspan="5">26 - Manter a integridade da informação e da infra-estrutura.</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></tr>
<tr><td rowspan="2">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>AI6, ES5</td><td>-</td></tr>
<tr><td colspan="5">27 - Garantir que a TI observe a legislação, regulamentações e contratos.</td></tr>
<tr><td>BSC</td><td colspan="2">Processos COBIT</td><td>ISO/IEC27002</td><td>Requisitos de segurança</td></tr>
<tr><td rowspan="2">P3</td><td>Mapeados</td><td>Não mapeados</td><td rowspan="2">PL, OI, SA, GO, AQ, CF</td><td rowspan="2">C, I</td></tr>
<tr><td>ES11, MO2, MO3, MO4</td><td>-</td></tr>
</table>

Quadro 1: Integração dos modelos BSC x COBIT x ISO/IEC27002

Fonte: Adaptado de KNORST (2010)

CASO DE ESTUDO

A aplicação do *framework* foi realizada em uma empresa de automação localizada em São Leopoldo, RS com 50 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.

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 da empresa ser significativamente dependente de sistemas de informação, e problemas relacionados à segurança da informação podem representar resultados preocupantes ao seu modelo de negócio e a cadeia de valores a qual está inserida.

O estudo envolveu a coleta de dados com em 4 etapas que seguiram o *framework* desenvolvido integrando os três níveis organizacionais, estratégico, tático e operacional conforme figura 1.

Etapa 1 - A primeira etapa foi a aplicação do instrumento 1 (em anexo, quadro 1), questionário baseado nos processos do modelo COBIT envolvendo os requisitos de segurança com a equipe gerencial para avaliar o grau de maturidade da empresa. O instrumento foi desenvolvido seguindo a metodologia CMMI do *Software Engineering Institute* (SEI, 2008) de verificação de maturidade dos processos de TI. Os questionários foram aplicados ao Diretor Administrativo, ao Diretor Industrial, ao 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.

Etapa 2 - A segunda etapa foi a aplicação do instrumento 2 (em anexo quadro 2), questionário para verificar o nível de proteção das práticas de segurança recomendadas pela ISO/IEC27002. Este instrumento foi desenvolvido com base no modelo proposto pelo Eloff & Eloff, (2003) para verificação do grau de proteção das práticas de segurança. O questionário foi aplicado ao técnico interno responsável pelo suporte e a empresa terceirizada que fornece serviços de suporte a rede e servidores da empresa.

Etapa 3 - A terceira etapa da coleta de dados foi através do instrumento 3 (anexo, quadro 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.

Etapa 4 - A quarta e última etapa foi a recuperação documental para confirmar e obter informações que eventualmente levantaram dúvidas ou não foram respondidas através dos instrumentos anteriores.

Os resultados encontrados em cada etapa foram analisados com base nos 18 Objetivos Genéricos de TI sugeridos pelo COBIT com impacto nos requisitos de Confidencialidade, Integridade e Disponibilidade. 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

Objetivo genérico de tecnologia da informação (TI):				
BSC	**Processos COBIT**		**ISO/IEC27002**	**Requisitos de segurança**
Objetivo genérico de negócio:	Mapeados	Não mapeados	Domínios da Norma	C, I, D
Documentação analisada:				
Respostas da entrevista:				
Práticas de segurança:				

Quadro 2: Instrumento de análise de resultados da aplicação dos modelos de GTI

Fonte: KNORST (2010)

Na sequencia são apresentados os resultados das etapas 1 e 2. Os resultados das etapas 3 e 4 tiveram seus resultados avaliados somente por objetivo de TI e consequentemente nas análises conclusivas.

Etapa 1: Verificação de maturidade em TI

A figura 3 apresenta o resultado da maturidade da empresa em relação aos processos do COBIT que sintetiza a média da aplicação do instrumento nos quatro entrevistados.

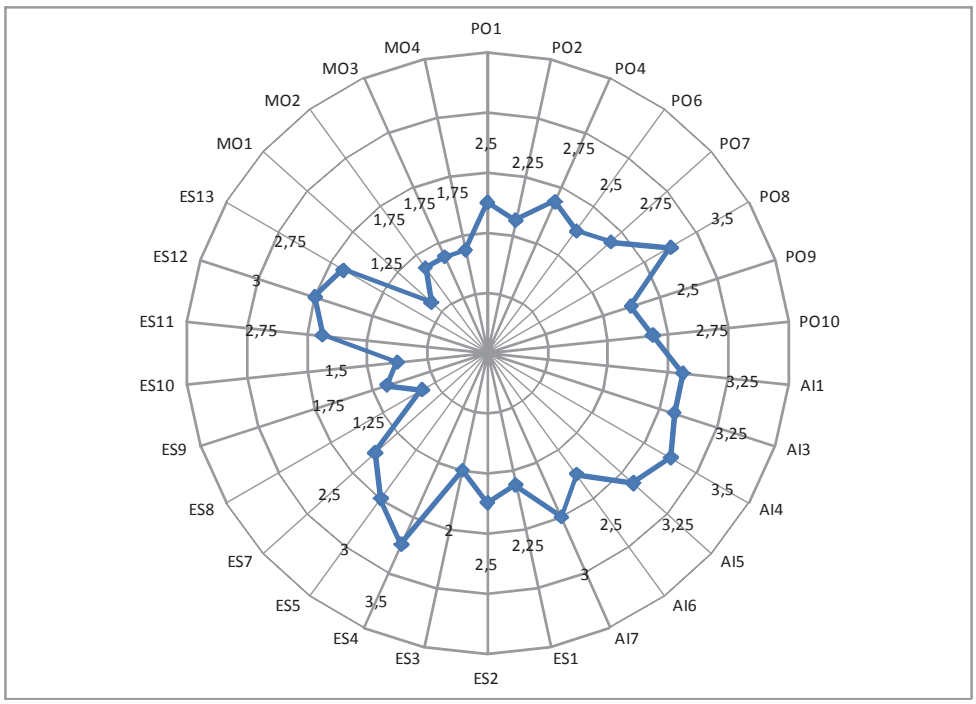
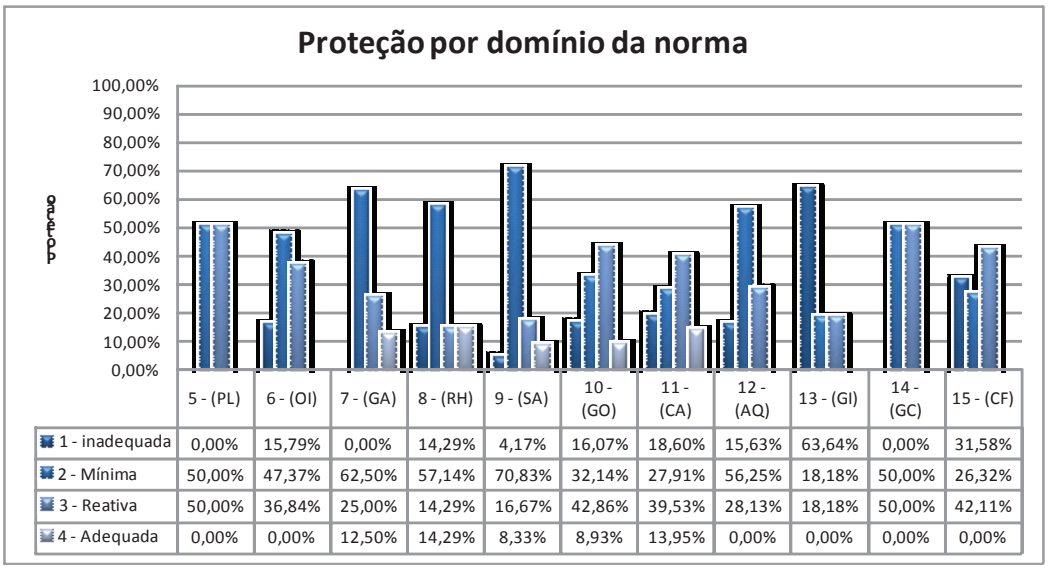


Figura 3: Maturidade da empresa em relação aos processos COBIT – Média

O resultado revela que a empresa se encontra em nível Repetitivo e Intuitivo em relação à maturidade de TI considerando o modelo COBIT. Uma vez que a empresa não dispõe de um programa formal para implantação de um modelo de maturidade, pode-se considerar este resultado um nível elevado. Isso se deve a quantidade significativa de processos estabelecidos e documentados inclusive na área de TI em função da certificação ISO9000:2000.

Etapa 2 – Verificação das práticas de segurança

A figura 4 apresenta o resultado do grau de proteção em relação aos domínios da norma ISO/IEC27002.



	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 4: Proteção dos domínios da ISO/IEC27002 na empresa pesquisada - Média

O gráfico evidencia que o grau de proteção se concentra entre mínimo e reativo. Considerando que as práticas avaliadas foram mapeadas a partir dos objetivos de negócio, este resultado demonstra uma fragilidade em relação à segurança da informação na empresa estudada.

ANÁLISES CONCLUSIVAS

As análises foram realizadas em duas etapas, primeiramente foi realizada uma análise individual de cada objetivo genérico de TI envolvendo os requisitos de segurança Confidencialidade, Disponibilidade e Integridade. Posteriormente estas análises foram consolidadas para possibilitar uma conclusão final e geral da empresa em relação à segurança em seu ambiente de TI considerando os níveis estratégico, tático e operacional.

A aplicação do *framework* através dos instrumentos apresentados anteriormente possibilita uma abordagem estratégica, tática e operacional através da integração dos modelos BSC (estratégico) x COBIT (tático) x ISO/IEC27002 (operacional). O resultado permitiu observar que a segurança da informação na perspectiva técnica se encontra de Mínima para Reativa, ela é tratada através ações isoladas baseadas no conhecimento técnico. Vale lembrar que a perspectiva técnica está alinhada estrategicamente com resultado da integração dos modelos.

Os dados indicam oportunidades de melhoria da segurança atuando principalmente no domínio de RH da empresa. O que leva a esta conclusão é o fato da empresa empregar uma mão de obra altamente qualificada em nível técnico característico do segmento de automação. Esta equipe detém grande conhecimento em sistemas digitais, de rede, comunicação entre outros, o que muitas vezes torna ineficaz a tentativa de promover a segurança no plano tecnológico. Isso confirma o que referencial teórico também aborda como um problema. Para que a segurança da informação seja efetiva ela necessita ser incorporada também na cultura da organização através de técnicas como estabelecimento de políticas, treinamento, conscientização e aplicação de práticas disciplinares (SOLMS e SOLMS, 2004).

Os instrumentos aqui apresentados foram desenvolvidos em dissertação de mestrado e em análise de bibliografia internacional, bem como de experiência prática de gestão de sistemas de informação. Por fim, apresentou-se a aplicação em caso real e para preservação da integridade das informações trabalhadas na empresa, alguns resultados foram analisados de maneira mais sintética.

REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

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

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.

ELOFF, J.; ELOFF, M**. Information Security Management** – A New Paradigm. Computers & Security, 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.

FITZGERALD, T, Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other, **Information Systems Security**, Volume 16, Issue 5, Pages 257-263, 2007.

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.

ISO/IEC 27002:2005: Information technology e code of practice for information security management. Switzerland: **International Organization for Standardization (ISO)**; 2005.

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

KNORST, A. M. **Alinhamento estratégico entre os objetivos de negócio e segurança da informação no contexto da governança de TI : um estudo no setor de automação**, Dissertação de Mestrado. Unisinos. São Leopoldo, 2010.

KWOK, l.; LONGLEY, D. Information security management and modeling, Information **Management & Computer Security,** Volume 7, Issue 1, Pág.30 – 40, 1999.

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.

POSTHUMUS, S.; SOLMS, R.. A framework for the governance of information security. **Computers & Security,** no. 23, pág. 638-646, 2004.

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.

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

	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 1: Instrumento de avaliação de maturidade da empresa

Fonte: Adaptado do COBIT e CMMI

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 2: Instrumento de Requisitos da norma ISO/IEC27002 aplicados para equipe técnica.
Fonte: Adaptado da norma ISO/IEC27002.

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 3: Instrumento de Questões para entrevista. **Fonte:** Adaptado do ITGI