UNIVERSIDADE FUMEC
FACULDADE DE CIÊNCIAS EMPRESARIAIS

MESTRADO EM ADMINISTRAÇÃO

O COMPORTAMENTO DO NÍVEL DE MATURIDADE EM GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

FRANCISCO PAULO TEMPONI

Belo Horizonte - MG

2010

FRANCISCO PAULO TEMPONI

O COMPORTAMENTO DO NÍVEL DE MATURIDADE EM GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Curso de Mestrado em Administração da Faculdade de Ciências Empresariais da Universidade FUMEC, como parte dos requisitos para a obtenção do título de Mestre em Administração.

Área de concentração: Gestão Estratégica de Organizações.

Orientador: Prof. Dr. Jersone Tasso Moreira Silva

Belo Horizonte - MG

2010

Dados Internacionais de Catalogação na Publicação (CIP)

T288c Temponi, Francisco Paulo, 1968-

O comportamento do nível de maturidade em governança de segurança da informação / Francisco Paulo Temponi. - Belo Horizonte, 2010.

163 f.: il.; 29,7 cm

Orientador: Jersone Tasso Moreira Silva

Dissertação (Mestrado em Administração), Universidade FUMEC, Faculdade de Ciências Empresariais, Belo Horizonte, 2010.

1. Tecnologia da informação. 2. Governança corporativa. 3. Sistemas de segurança. I. Título. II. Silva, Jersone Tasso Moreira. III. Universidade FUMEC, Faculdade de Ciências Empresariais.

CDU: 658

Ficha catalográfica elaborada pela Biblioteca Universitária-FUMEC

Universidade FUMEC
Faculdade de Ciências Empresariais
Cursos de Mestrado e Doutorado em Administração FACE/FUMEC

Dissertação intitulada **"O Comportamento do Nível de Maturidade em Governança de Segurança da Informação**, de autoria do mestrando ***Francisco Paulo Temponi***, aprovado pela banca examinadora constituída pelos seguintes professores:

Prof. Dr. Jersone Tasso Moreira Silva - Universidade FUMEC
(Orientador)

Prof. Dr. Luiz Antônio Antunes Teixeira - Universidade FUMEC

Prof. Dr. Hugo Ferreira Braga Tadeu– Centro Universitário UNA

Prof. Dr. Daniel Jardim Pardini
Coordenador do Programa de Doutorado e Mestrado em Administração
Universidade FACE/FUMEC

Belo Horizonte, 25 de novembro de 2010.

Dedico este trabalho à minha esposa Sandra, por tudo o que você é para mim, e aos meus filhos, Bernardo e Leonardo, pelo que vocês suportaram nas minhas ausências e por todo o amor que representam.

Adicionalmente à minha mãe Elza, por todo amor, carinho e perseverança que refletem em nós, ao meu pai Francisco, pelos conselhos, e às minhas irmãs, Paula e Rita, pela feliz convivência em família.

AGRADECIMENTOS

Primeiramente a Deus, pela oportunidade de viver mais e usufruir de tudo aquilo que compõe nossos momentos felizes e mesmo os infelizes que ajudam no crescimento espiritual.

A minha irmã Paula Elisabete Tempone de Aguiar por ter me presenteado com o primeiro livro da graduação em Ciência da Computação que nunca será esquecido por sua importância em toda esta jornada.

A Universidade FUMEC, ao professor Daniel Jardim Pardini, professores do Mestrado em Administração, e a equipe da pós-graduação, por me proporcionarem crescimento e momentos felizes na carreira docente bem como a realização deste trabalho.

A professora Silvia Calmon de Albuquerque e ao professor Rodrigo Baroni de Carvalho por terem me dado a oportunidade de lecionar na pós-graduação dessa instituição.

Ao professor George Leal Jamil por toda sua colaboração e amizade.

Agradeço em especial ao professor Jersone Tasso Moreira Silva pela orientação, pelo profissionalismo, e colaboração na vida docente da qual fazemos parte.

Aos meus alunos que aprendem e me ensinam a aprender.

A todos os profissionais que dispuseram de seu tempo para colaborar nos estudos de casos deste trabalho.

A todos que saibam, ao lerem este trabalho, mesmo que não estejam citados, e não por suas importâncias, sintam-se agradecidos por mim.

“Exércitos hostis podem se enfrentar por anos, lutando pela vitória, que pode ser decidida em um único dia. Sendo assim, permanecer na ignorância sobre a condição do inimigo, simplesmente para economizar, é o cúmulo da desumanidade.”

SUN TZU

RESUMO

O conflito de agência, decorrente da divergência de interesses entre a propriedade e a gestão empresarial, e os recentes casos de fraudes causaram nas organizações uma maior necessidade de adesão à Governança de Segurança da Informação (GSI) e seus pilares: a tecnologia da informação (TI), a segurança da informação e a conformidade com a legislação. Por ser de responsabilidade e governo dos altos escalões das organizações, a GSI proporciona melhor gestão dos riscos corporativos como base de sustentação para os valores da Governança Corporativa (GC), portanto, verifica-se a sua importância para a pesquisa do seu nível de maturidade. A pesquisa qualitativa, de caráter exploratório, apoiada no referencial teórico e nos modelos do ITGI, CGTF, COBIT, COSO, BASILÉIA, ISO/IEC 27001, 17799/27002, 27005 e 27014, foi realizada com apoio do estudo de múltiplos casos em organizações brasileiras sujeitas ou não à regulação. A amostragem contemplou 12 entrevistas semi-estruturadas, com gestores de segurança e executivos, em 6 empresas. O nível 2 (repetível) de maturidade em GSI foi predominante, ressaltando-se que a maioria dos executivos revelou comportamento de desconhecimento quanto à necessidade e priorização do alinhamento estratégico de segurança da informação. No geral, há um entendimento emergente sobre a necessidade de se tratar melhor a gestão dos riscos, entretanto, ainda é reativa e focada em segurança de TI. A conscientização de segurança nas organizações ainda é fragmentada e limitada. O posicionamento da área de segurança da informação na estrutura organizacional ainda é vinculado à área de TI refletindo negativamente nos níveis de maturidade. A adoção dos modelos que compõem a GSI, em muitos casos, ainda é dispersa e não faz parte de uma estratégia global. Diante de todo esse cenário, certas organizações que informam optar pelas práticas da GC estão comprometendo a eficácia no tratamento dos valores dessa na medida em que não priorizam estrategicamente a adesão à GSI.

Palavras-chave: Alinhamento Estratégico, Governança de Tecnologia da Informação (GTI), Gestão de Riscos Corporativos (GRC), Governança de Segurança da Informação (GSI), Governança Corporativa (GC).

ABSTRACT

The agency conflict, due to the divergence of interests between the property and business management, and recent fraud cases in organizations have caused a greater need for adherence to the Information Security Governance (ISG) and its pillars: information technology (IT), information security and compliance with legislation. Because it is the responsibility of the government and upper echelons of organizations, GSI provides better management of corporate risks as a basis for support for the values of Corporate Governance (CG), so there is its importance for research on their level of maturity. A qualitative research, exploratory, based on theoretical models as ITGI, CGTF, COBIT, COSO, BASEL, ISO / IEC 27001, 17799/27002, 27005 and 27014, was accomplished with support of multiple cases studies in Brazilian organizations subject to regulation or not. The sample included 12 semi-structured interviews with security managers and executives in 6 companies. The level 2 (repeatable) prevailed in ISG maturity, emphasizing that most executives revealed behavior of ignorance about the need and prioritization of the strategic alignment of information security. Overall, there is an emerging understanding about the need to better address risk management, however, is still reactive and focused on IT security. The security awareness in organizations is still limited and fragmentary. The positioning of the area of information security in the organizational structure is still tied to the IT field reflecting negatively on levels of maturity. The adoption of models that comprise the ISG, in many cases, is still scattered and not is part of an overall strategy. Faced with this whole scenario, certain organizations that inform the choice of CG practices are compromising the effectiveness of the treatment of values as it does not prioritize strategically to join the ISG.

Keywords: Strategic Alignment, Information Technology (IT) Governance, Enterprise Risk Management (ERM), Information Security Governance (ISG), Corporate Governance (CG).

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANATEL	Agência Nacional de Telecomunicações
ANEEL	Agência Nacional de Energia Elétrica
BACEN	Banco Central do Brasil
BASELII	Basiléia II
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
BPM	Business Process Model
BS	British Standard
BSC	Balanced Scorecard
CERT	Computer Emergency Response Team
CEO	Chief Executive Officer
CCITO	Cyber Crime & Insider Threat Obviation Solutions
CID	Confidencialidade, Integridade, Disponibilidade
CIDAL	Confidencialidade, Integridade, Disponibilidade, Autenticidade, Legalidade
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treatway Commission
CGTF	Corporate Governance Task Force
CSO	Chief Security Officer
ERM	Enterprise Risk Management
FISMA	Federal Information Security Management Act
GC	Governança Corporativa
GSI	Governança de Segurança da Informação
IDEAL	Initiating, Diagnosing, Establishing, Acting, Learning
ISACA	Information System Audit and Control Association
ISG	Information Security Governance
ISMS	Information Security Management system
ISO	International Organization for Standardization
ITGI	Information Technology Governance Institute

ITIL	Information Technology Infrastructure Library
PDCA	Plan, Do, Check, Action
PDI	Plano Diretor de Informática
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
ISO/IEC 15408	Evaluation Criteria for IT Security
ISO/IEC 17799	Information technology -- Security techniques -- Code of Practice for Information Security Management
ISO/IEC 27001	Information Security Management Systems – Requirements - (ISMS)
ISO/IEC 27002	Code of Practice for Information Security Management
ISO/IEC 27004	Information Security Management Measurements
ISO/IEC 27005	Information Security Risk Management
ISO/IEC 27006	Requirements for bodies providing audit and certification of Information Security Management Systems
ISO/IEC 27014	Information Security Governance Framework
ROB	Receita Operacional Bruta
SEI	Software Engineering Institute
SOX	Sarbanes Oxley
UML	Unified Modeling Language

SUMÁRIO

1 INTRODUÇÃO

Os mesmos fatores como estratégias, gestão de riscos, pessoas e processos, componentes que envolvem a propriedade da informação e sua devida utilização para a geração do conhecimento, conforme SUN TZU, estrategista militar século IV a.C, determinavam as condições existentes em um campo de batalha e hoje trazidos à reflexão no mundo contemporâneo podem ser percebidos no contexto organizacional como componentes de modelos fundamentais para a governança corporativa.

A evolução tecnológica existente nos atuais recursos de comunicação, como a *internet*, os *smartphones, notebooks*, teleprocessamento, e mídias em geral, disponibilizam rapidamente a informação tornando mais dinâmico o relacionamento corporativo com o meio interno e externo demandando rapidamente as mudanças estratégicas, conforme as três dimensões[1] de Pettigrew e Whipp (1991) para que as organizações possam atingir seus objetivos de negócio com segurança.

De posse da informação, o ser humano produz o conhecimento necessário para atingir seus objetivos lícitos, de acordo com as leis e regras que os regem, entretanto, os objetivos ilícitos, para benefício próprio ou de outrem, sem autorização ou a devida conformidade, conforme Dalkir (2005) são de difícil controle nas questões de segurança, acesso, e comportamento a respeito do código de ética profissional devido à passagem do conhecimento, pois esta se dá de forma individual e imprecisa tendo em seu resultado o interesse particular de quem o transmite. São exatamente os objetivos ilícitos que permeiam a as ações de segurança para mitigação dos riscos corporativos e que justificam tratá-las de forma estratégica e proativa.

Paralelamente às ações de competitividade, cresce a preocupação em tornar disponível a informação a quem é de direito, de forma íntegra, preocupando-se com a veracidade e confidencialidade de tais informações conforme apontado por Sêmola (2003),

---

[1] As três dimensões referenciadas por Andrew Pettigrew são o Conteúdo (objetivos e hipóteses), o Contexto (interno e externo) e o Processo (padrões de implementação).

Lara (2004), Campos (2007) e Beal (2008), e, adicionalmente, em conformidade com a legislação com apoio das equipes de controles internos dos sistemas de informação que, segundo Imoniana (2008), as mesmas tem por objetivo maior a salvaguarda de informações, a verificação da exatidão e veracidade das informações, bem como a efetividade do sistema contábil e operacional, atendendo à política organizacional.

Para Campos (2007), o comprometimento no tratamento da informação é considerado um incidente de segurança, que conforme ABNT (2005, p.2) é "[...] indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação" e que pode ter diferentes impactos porque cada organização possui uma estratégia de negócio heterogênea.

Estratégia na definição de Chandler (1962) *apud* Pugh e Hickson (2004, p. 3) seria "[...] a determinação das metas e objetivos em longo prazo, junto à adoção de linhas de ação e à alocação de recursos, para alcance desses objetivos.", então, seguindo-se o mesmo raciocínio, em virtude de intempéries durante o caminho para se atingir as metas e objetivos, é necessário estabelecer paralelamente outras linhas de ação que busquem garantir que os mesmos possam ser alcançados com segurança, sustentabilidade, e competitividade.

A estratégia de negócio, segundo Davis, Aquilano e Chase (2001) refere-se à estratégia individual adotada pelas unidades de negócios em termos de posicionamento diante do mercado. Essa mesma estratégia de negócios é fundamental para compor com a estratégia de segurança a estratégia global da empresa e, nessa linha, Alves (2006), relata que há necessidade de governar a segurança da informação (SI) principalmente em um nível estratégico o que leva este estudo a ser iniciado pelas definições dos conceitos de estratégia, alinhamento estratégico e governança corporativa (GC) para que seja obtido um melhor entendimento do papel do nível de maturidade da Governança de Segurança da Informação (GSI) nas organizações sujeitas ou não à regulação.

Na definição de Motta (2003) a regulação é uma forma de controle de determinada atividade exercido por uma agência pública ou por um órgão social no intuito de corrigir e prevenir distorções de conduta e transparência harmonizando os interesses públicos e privados. É uma atividade totalmente despolitizada, portanto, fundamental à GC.

Para Miles e Snow (1984), alinhamento estratégico pode ser tanto um processo que, conforme Prieto e Carvalho (2006) é uma sequência de atividades e tarefas para atingir o próprio alinhamento, quanto um resultado, pois a organização busca a sintonia com seu ambiente interno e externo.

Portanto, para entendimento do surgimento da GSI, a seguir é realizada uma breve explicação da evolução desse ambiente interno e externo do mundo corporativo, desde o nascimento do capitalismo até os processos históricos e culturais que levaram à criação da governança corporativa.

Governança corporativa, segundo o Instituto Brasileiro de Governança Corporativa - IBGC (2009, p.19), é "[...] o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle".

Weill e Ross (2006) relatam que após os escândalos envolvendo empresas como Enron, Worldcom, e Tyco houve maior preocupação com a habilidade e determinação das empresas em protegerem seus *Stakeholders*[2].

No âmbito global, conforme Bettarello (2008), a governança corporativa ganhou força com o escândalo de Watergate nos Estados Unidos da América, onde autoridades reguladoras e legislativas descobriram que grandes companhias contribuíram ilegalmente para campanhas políticas e subornaram membros da administração pública. Após este escândalo, os modelos de monitoramento e *compliance* foram questionados e houve a necessidade de maior regulação.

Nascimento (2007, p. 70) define *compliance* como o grau mensurável da conformidade para com as obrigações legais e, para atender a essa, muitas organizações criaram áreas internas de *compliance* que, para Mattarozzi e Trunkl (2008, p. 145), é "[...] a área de controles internos e de definição de responsabilidades dentro da instituição."

Lahti e Peterson (2006) informam que, em consequência das crescentes fraudes envolvendo as 100 maiores empresas da revista *Fortune*, o Congresso Americano decretou em

[2] Para Andrade e Rossetti (2009, p.109), *Stakeholders* são" Pessoas, grupos ou instituições, com interesses legítimos em jogo nas empresas e que afetam ou são afetados pelas diretrizes definidas, ações praticadas e resultados alcançados.".

2002 o *Ato Sarbannes Oxley* que orienta como as empresas de capital aberto irão prestar contas de suas finanças. Isto afeta toda a infraestrutura organizacional e por consequência a tecnologia da informação (TI) para aderência às suas conformidades sendo estas, juntamente com a necessidade de alinhar TI ao negócio, os pilares para a criação da governança de TI (GTI).

Para o *IT Governance Institute* - ITGI (2010):

> A Governança de TI é parte integrante da Governança Corporativa e consiste da liderança e as estruturas organizacionais e processos que assegurem que a organização de TI sustente e estenda as estratégias e objetivos da organização. (ITGI, 2010)

A estrutura organizacional, que conforme Laurindo *et al.* (2001) , é componente de sucesso para o alinhamento estratégico de TI e negócio. Argumento que também é defendido por Sêmola (2003) e Campos (2006) quando informam que a segurança da informação deve ser assunto na pauta da alta direção das corporações.

Fernandes e Abreu (2008) consideram que a maior transparência da administração é o maior motivador da governança de TI e esta é motivada pelos seguintes fatores: TI como prestadora de serviços, integração tecnológica, ambiente de negócios, dependência do negócio em relação a TI, e finalmente os marcos de regulação (*compliance*) e segurança da informação sendo estes dois últimos a base para este estudo da GSI.

Segundo o ITGI (2006), Governança de Segurança da Informação é:

> [...] da responsabilidade do conselho de diretores e altos executivos. Deve ser uma parte integral e transparente da Governança Corporativa e estar alinhada com a estrutura de Governança de TI. Embora os executivos seniores tenham a responsabilidade de atender e responder as preocupações e sensibilidades levantadas pela segurança da informação, conselhos de diretores serão cada vez mais esperados para fazer a segurança da informação como uma parte intrínseca do governo, integrada com os processos que eles já têm para reger a outros recursos organizacionais críticos. (ITGI, 2006, p.11, *tradução do autor*)

Vê-se na definição do ITGI (2006) a real necessidade de haver a integração dos fatores que compõem a GSI como a TI, a segurança da informação, a transparência e conformidade, ressaltando-se a necessidade de ser tratada e governada como parte da responsabilidade da alta gestão da empresa na preservação e sustentabilidade da GC.

Tratando-se de GSI, especificamente, adentra-se mais nos componentes: marcos de regulação (*compliance*) e a própria segurança da informação. Segundo Fernandes e Abreu (2008), esses são pertencentes ao domínio de alinhamento estratégico e *compliance*, ambos também contemplados na governança de TI.

Servirão para corroborar as questões da pesquisa e do estudo das repercussões dos *frameworks*[3] (modelos) de governança de TI, também utilizados como base para a Governança da Segurança da Informação, como o *Control Objectives for Information and Related Technologies* (COBIT), o *Information Technology Infrastructure Library* (ITIL), o *Information Security Management Systems* (ISO/IEC 27001) e o *Code of Pratice for Information Security Management* (ISO/IEC 27002) e finalmente a ISO/IEC 27014 *Information technology - Security techniques -- Information security governance framework (draft).*

O conceito de segurança da informação abrange além da tecnologia, processos e pessoas, sendo este último, conforme Beal (2008) o elo mais frágil no comprometimento do ativo informacional. Campos (2007, p. 80) acrescenta informando que as próprias pessoas são os ativos mais importantes da organização pois executam processos, geram e consomem informações, portanto, podem oferecer os maiores riscos.

Fleury *et al.* (2002, p. 262) quando cita as formas de poder fazem referência ao poder da informação como "[...] posse de dados estratégicos para uma situação crítica ou de informações que orientem processos decisórios e escolhas de diversas ordens.", ou seja, destacam a relevância da posse deste ativo para decisões de alta importância.

Westerman e Hunter (2008, p.7) demonstraram que a "maioria dos riscos de TI decorre não de problemas técnicos ou de problemas com funcionários de baixo escalão, mas sim de falhas de supervisão e da governança dos processos de TI" o que reforça a importância da proteção dos acervos na governança de TI a partir de uma visão holística desde o executivo das organizações.

---

[3] *Frameworks:* "[...] palavra que significa esqueleto, mas que na área de informática pode ser entendida com um modelo formatado" (SILVA, 2009, p. 52).

O *compliance* e a segurança da informação são o arcabouço necessário à proteção dos acervos informacionais, mas necessariamente a GSI e a governança de TI, conforme Alves (2006, p.15), "[...] funcionarão como habilitadores criando processos estruturados, constantemente controlados e alinhados com a estratégia da empresa.", devem ser componentes da governança corporativa, argumento também defendido por Bernardes e Moreira (2005).

Assim, diante do pressuposto de que as organizações sujeitas à regulação devem ter priorização em ações que as posicionem em níveis elevados de maturidade de GSI em relação às que não estão sob estas conformidades justamente por serem as primeiras suscetíveis a maiores riscos e que o aumento destes são fatores negativos para a transparência necessária a governança corporativa, surge a questão cuja resposta é o objetivo (item 1.2.1) do estudo proposto: **Qual o comportamento do nível de maturidade em Governança de Segurança da Informação nas organizações sujeitas ou não à regulação?**

1.1 Justificativa

Em virtude da relevância do assunto e pelo resultado do levantamento bibliográfico que apontou o predomínio internacional em estudos acerca do tema sobre nível de maturidade em GSI adicionalmente abrindo oportunidades para contribuição com produção nacional, este trabalho inicia-se no estudo do maior ativo das corporações: a informação.

Para Sêmola (2003) informação é:

> [...] conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas operações que envolvam, por exemplo, a transferência de valores monetários). (SÊMOLA, 2003, p. 45).

Já para Beal (2008), os ativos de informação são associados a valores de negócio, portanto, podendo ser um dado ou uma informação com relevância no contexto no qual estão inseridos.

Entretanto, pode-se dizer que o conceito de informação adotado por Jamil (2005, p. 16), o qual define esta como "[...] um elemento composto a partir de um conjunto de dados relevantes para uma análise, contextualizados.", é fundamental à relevância do tratamento do contexto para se efetuar a gestão de risco, um dos domínios da GSI, ou seja, a segurança tem de ser um processo contínuo e cíclico em virtude das diferenças de contexto no qual se está inserido, o que corrobora o raciocínio de Westerman e Hunter (2008) que expõem a dificuldade na relação contexto dos negócios e a tecnologia (que mudam demais) para depender de abordagens reativas no tratamento do risco. Ainda segundo estes mesmos autores, os riscos mais perigosos são os que nunca são considerados ou reconhecidos tarde demais. Uma informação pode não ter valia para determinada pessoa, mas em outro contexto pode ser extremamente útil para outrem.

Para Paiva (2008, p. 13), "A informação, como qualquer ativo, precisa ser classificada, estruturada, validada, valorada, protegida, monitorada, medida e gerenciada eficiente e eficazmente" o que é respaldado pelos modelos de governança de TI, pelos marcos regulatórios e pela segurança da informação.

Allee (1997), Nonaka e Takeuchi (1997) e Sveiby (1998), Jamil (2005) destacam a preocupação com os ativos intangíveis, dentre estes, o conhecimento e a informação que são os ativos mais importantes dentro das organizações e protegê-los é o maior desafio em um mundo interconectado.

Portanto, como a informação é base para a geração do conhecimento, é necessário mitigar os riscos que envolvem os quatro momentos do ciclo de vida da informação conforme Sêmola (2003, p.10) ilustrados na FIG. 1: Manuseio (momento em que a informação é criada e manipulada), o armazenamento (momento em que a informação é armazenada em meio qualquer), o transporte da mesma e o descarte (momento em que a informação é excluída definitivamente), bem como mitigar os riscos relativos ao conhecimento que conforme Beal (2008, p.71) envolve o ser humano que é o elo mais frágil da segurança da informação.

O ciclo de vida da informação ainda requer requisitos de segurança para o CIDAL (Confidencialidade – garantir a informação somente a quem é de direito; Integridade – garantir que a informação enviada seja a mesma recebida; Disponibilidade – garantir a disponibilização da informação quando necessária; Autenticidade – garantir a origem da informação; Legalidade – garantir a informação em conformidade com as leis e normas).

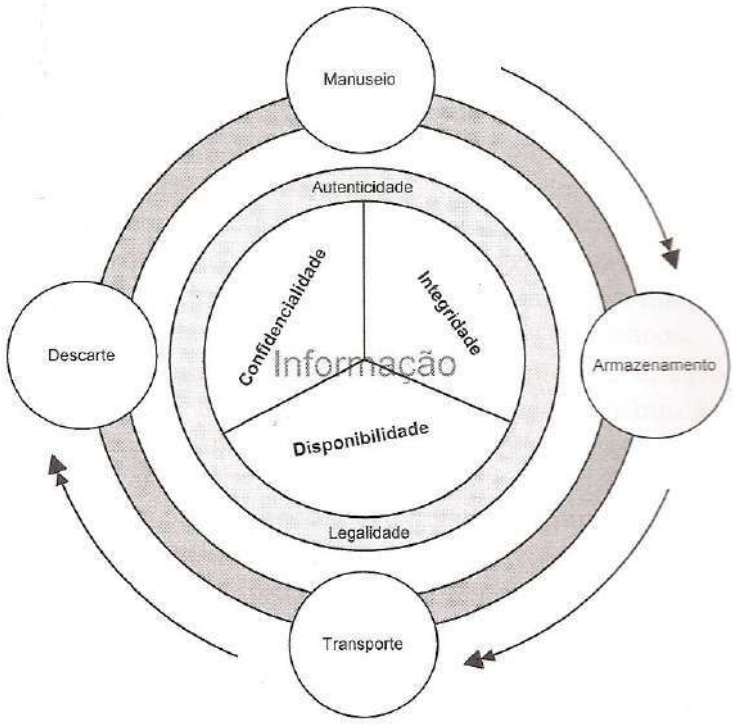

FIGURA 1 - Ciclo de vida da informação
Fonte: SÊMOLA, 2003, p.11.

Quando se refere à segurança do maior ativo das organizações, as atitudes do ser humano inspiram o estudo dos fatores que levam o mesmo a ser o principal agente de corrupção, comprometendo a segurança das informações.

Westerman e Hunter (2008, p. 127) acreditam que não há como tratar devidamente os riscos, portanto, em se implantar segurança, se não há uma cultura de riscos nas empresas e se esta não é proveniente dos altos escalões das mesmas.

A necessidade de tratar a segurança da informação e a conformidade com as leis como prioridades para as ações da GSI é fundamental para a transparência demandada pela governança corporativa.

Adicionalmente, justifica-se este estudo pela gravidade dos casos mais recentes de comprometimento da segurança da informação, infração da legislação, corrupção e violação de direitos, ocorridos no Brasil e no mundo afora que envolvem justamente o conhecimento privilegiado de informações críticas:

a) para Sander (2009, p. 13) o caso americano Madoff é "A Maior Fraude Financeira de Sempre". Madoff foi o mentor de um negócio bilionário que tinha por base o mesmo esquema adotado por Charles Ponzi[4] porém com a sofisticação e a engenharia dos dias atuais o que lhe permitiu atingir grandes corporações e entidades físicas e jurídicas;

b) outro caso internacional, relatado por Ciampa (2009), foi a operação fraudulenta no *Societé* arquitetada pelo operador de contratos futuros Jérôme Kerviel que havia trabalhado no setor de TI (o que facilitou sua ação). Desperta a atenção a negligência humana, pois durante toda operação houveram vários alertas ignorados pela gestão;

c) no Brasil também há casos que envolvem cargos de posição estratégica das organizações e que geraram grandes prejuízos como informa Cortês (2010)

[4] Charles Ponzi foi, na década de 20, o mentor de um esquema espiral semelhante ao que conhecemos como pirâmide, que segundo a SEC (Security and Exchange Commission), a Comissão de Valores Imobiliários dos Estados Unidos da América, os participantes obtinham lucro com a entrada de novos participantes. Porém a certa altura, com o volume muito grande de novos participantes o negócio não suporta mais pagar lucros aos mesmos.

sobre o escândalo que envolveu um esquema onde houve ocultamento de doações irregulares para obtenção de vantagens nas aprovações de projetos federais do governo brasileiro. Conforme Ashforth (2008), este caso teria uma abordagem *top-down* de corrupção, portanto, sendo mais danosa e perigosa para a sociedade por ter a sua origem na parte estratégica das organizações comprometendo as ações dos altos escalões.Pessoas passam a valer-se da própria influência para conseguir ativos ou informações privilegiadas ilicitamente ao seu favor. A GSI juntamente com as estruturas de governança de TI em seus dois pilares citados anteriormente fornecem controles que permitem mitigar o risco do comprometimento da informação;

d) outros casos que justificam a preocupação com a segurança das informações foram as fraudes na previdência, conforme Silva (2006), com a participação de funcionários do Ministério, com destaque para a maior delas comandada e arquitetada por uma advogada ex-procuradora do INSS onde a quadrilha fraudava superestimando o valor das aposentadorias além de criar aposentadorias fictícias.

Concluindo relatam-se os problemas com vazamento de informações, com destaque em uma empresa petrolífera do governo federal, conforme Lima (2010), em que vazaram informações referentes ao Pré-sal[5] invocando a sociedade a acompanhar mais de perto a custódia das informações mantidas por estatais.

Conforme Alves (2006), a transparência exigida pela governança corporativa demanda de controles em seus mecanismos, onde se destaca a governança de TI fundamentada no alinhamento e transparência da tecnologia ao negócio.

Segundo o ITGI (2006), domínios da GSI também existentes nas estruturas dos modelos de governança de TI, dentre seus conceitos e processos, são responsáveis pelo gerenciamento dos riscos ao negócio bem como pela conformidade com as leis e, em segurança da informação, pela disponibilidade, confidencialidade e integridade das informações protegendo todo o ciclo de vida destas.

---

[5] Segundo Pannunzio (2008, p.29), o Pré-sal é "[...] camada de petróleo sob urna capa de dois mil metros de sal." Esta mesma camada é rica em Petróleo mais fino.

A *Transparency International*[6] informa que o incremento do número de escândalos envolvendo os atores dos casos citados requer a priorização das ações de segurança nos governos, empresas e sociedade, com mecanismos de governança que possam manter a transparência dos envolvidos.

Em um mundo globalizado onde, segundo Sêmola (2003, p. 1), a informação é um dos ativos cada vez mais valorizados, a mesma passa a ser fator crítico de sucesso, portanto, as formas de disponibilizá-la, classificá-la e mantê-la são primordiais à competitividade sendo definitivamente reconhecida em sua importância e tratamento.

Sendo a GSI um assunto relativamente novo, bem como a inexistência de grandes estudos acerca desse, principalmente no Brasil, aliado à necessidade da adesão às práticas de mercado como melhor roteiro para a implantação dos requisitos de governança, vê-se a motivação e oportunidade para contribuir tanto com o meio acadêmico quanto com a necessidade de se estabelecer caminhos mais seguros para organizações que desejam aprimorar a competitividade mantendo a transparência perante seus *stakeholders*.

Este trabalho ressalta a importância de se aprofundar os estudos de GSI como princípio estratégico e de competitividade dentro das corporações. Importância essa que é respaldada por Alves (2006, p. 39) que coloca a GSI como assunto estratégico para as empresas e Sêmola (2003, p. 33) que vai adiante e informa que é necessário o alinhamento a estratégia da empresa buscando obter, além da segurança, o retorno aos investimentos e a busca de valor ao negócio, também defendido por Beal (2008, p.41).

Entidades como o ITGI (2006), CGTF (2006), Campos (2007, p.146), Beal (2008, p.51), também defendem a necessidade da GSI ser inserida dentro da estrutura estratégica da empresa sob o argumento de que além de facilitar a tomada e a implantação de decisões relativas a assuntos de segurança, ela assegura melhor eficácia no alinhamento entre negócio e os requisitos de segurança.

O ITGI (2006) e CGTF (2006), inclusive, propõem respectivos modelos de maturidade em GSI justamente para que haja a mensuração da inserção da mesma nas organizações.

---

[6] **Transparency International.** Disponível em: < http://www.transparency.org/>. Acesso em: 16/07/2010.

O modelo utilizado para a realização da pesquisa e a verificação do comportamento do nível de maturidade a ser detalhada na metodologia é justamente o do ITGI (2006) por ter fortes embasamentos no alinhamento estratégico, na governança de TI, nas práticas como o COBIT *Security Baseline*, ISO 27001 e 27002, nos conselhos como COSO, bem como no fato do mesmo incluir referências diretas ou indiretas a outros modelos inclusive o relacionado no *Information Security Governance. A Call To Action* do CGTF (2006) e o de Pironti (2007) sobre *baselines metrics* adaptadas neste estudo para uma abordagem mais focada em GSI, portanto, em um nível mais gerencial dos requisitos de segurança.

1.2 Objetivos

1.2.1 Objetivos gerais

O objetivo deste trabalho é verificar o comportamento do nível de maturidade em Governança de Segurança da Informação nas organizações sujeitas ou não à regulação.

1.2.2 Objetivos específicos

Os objetivos específicos deste trabalho são:

a) identificar os conceitos e as estruturas da GSI existente nos diferentes modelos de governança de TI;

b) identificar como a GSI está sendo adotada nas organizações sujeitas ou não à regulação;

c) identificar os artifícios da GSI para a mitigação dos riscos organizacionais;

d) analisar as atitudes dos gestores e executivos das organizações frente às práticas de mercado que sustentam os princípios de GSI para mitigar os riscos;

e) identificar a relação dos valores da governança corporativa com a necessidade de proteger os acervos informacionais.

2 REVISÃO DE LITERATURA

Este capítulo tem por objetivos: a) a construção dos conceitos elementares deste estudo; b) apresentar seus principais construtos, como governança corporativa, alinhamento estratégico, governança de TI e GSI explicitando a ligação entre os construtos baseando-se em teorias e em práticas aplicadas no mercado; c) dar embasamento à metodologia apresentada no próximo capítulo.

Esta revisão de literatura apresenta a base conceitual do trabalho de acordo com as teorias existentes e as práticas de mercado adotadas pelas empresas estrangeiras e, principalmente, as nacionais.

Antes de iniciarem-se as exposições dos demais construtos deste estudo, prioriza-se a discussão sobre o alinhamento estratégico como elo entre os outros construtos, pois, segundo Andrade e Rossetti (2009), Weill e Ross (2006), Sêmola (2003), Campos (2007), Mintzberg (2003) e Beal (2008), os conceitos relativos à governança tem a estratégia em seus embasamentos.

Os conceitos são ilustrados a partir de uma concepção histórica mostrando porque existem diferentes modelos de governança corporativa, portanto, para contextos econômicos e sócio-culturais distintos.

Relaciona-se o comportamento dos executivos frente à governança corporativa e à GSI principalmente em relação à conformidade e a segurança da informação. Conforme citado anteriormente, esses são fatores da governança de TI, o que os destaca como componentes da GSI e conseqüentemente como artifícios para a obtenção da transparência requerida na governança corporativa. Pode-se dizer que os mesmos são o elo comum existente entre a GTI e GSI e a todo o momento são referenciados neste trabalho.

Adentra-se mais nos conceitos da própria Tecnologia da Informação e Comunicação (TIC), relacionando seus principais modelos, características, importância, e sua ligação com a GSI.

Seguindo-se no referencial, disserta-se sobre a GSI, sua importância, seus princípios, objetivos, características, principais teóricos e institutos que contribuem para sua divulgação, e os modelos existentes para essa finalidade. Devido ao relacionamento entre os *frameworks* de GTI e os *frameworks* de GSI, o nível de maturidade neste último reflete também certo alinhamento estratégico de TI com o negócio. As teorias existentes juntamente com os domínios comuns a esses modelos servirão de embasamento para o desenvolvimento da metodologia e das questões de pesquisa no mercado.

Finalmente, na última parte deste capítulo, fundamenta-se a elaboração dos questionários com base em todo conteúdo visto anteriormente, passo final para o desenvolvimento da metodologia deste trabalho.

A seguir a apresentação da base teórica dos construtos adotados para elaboração deste estudo, descrevendo seus conceitos, suas características, importância, relacionamento com outros construtos, modelos e práticas imprescindíveis para o entendimento da metodologia, análise de resultados e discussões e, finalmente, da conclusão.

2.1 Alinhamento estratégico

Venkatraman e Camillus (1984) informam que a palavra "alinhamento" tem origem na Teoria da Contingência[7] e que o alinhamento é entre o ambiente, recursos organizacionais e as ameaças. Especificamente na linha de frente para este estudo, as ameaças são a base para a preocupação com os riscos organizacionais e as formas de mitigá-los.

No mesmo raciocínio acima Porter (1979) defende que uma empresa estrategista sabe aproveitar e alinhar as oportunidades e ameaças, gerados pelo ambiente interno e externo. Exemplificando o papel das ameaças neste trabalho, estas poderiam ser facilmente

[7] Para Bowditch e Buono (2004, p. 17), "A tese central da teoria da Contingência é que não há princípios universais de administração que possam ser aplicados indiscriminadamente a todas as situações.", concluindo, para o mesmo deve ser levado em consideração o contexto e a estrutura organizacional.

originadas pela entrada de um produto concorrente no mercado com características semelhantes ao produto da companhia estas fornecidas através de vazamento de informações muito frequente nos incidentes de segurança.

Para Campos (2007, p. 36) a vantagem competitiva é oriunda da estrutura organizacional onde que deve ser aproveitada e explorada em cada possibilidade, entretanto, para realizar tais ações devem ser levados em consideração os riscos impostos ao negócio pelo ambiente aliando-se a Porter (1979), quando cita sobre oportunidades e ameaças, Luftman (2000), quando escreve sobre o Compartilhamento dos Riscos e Kieling (2005, p.4) quando relata positivamente sobre o papel da análise de riscos nos negócios.

D'Avila e Oliveira (2002) informam que a definição dos objetivos também mapeia os riscos a serem aceitos ou mitigados, bem como são representados na missão e nos valores da empresa. Completam o raciocínio da seguinte forma: "[...] Juntamente com uma avaliação de potencialidades e fraquezas, bem como de oportunidades e ameaças, chega-se à estratégia para a empresa como um todo." (D'AVILA; OLIVEIRA, 2002, p.53).

A palavra "estratégia", segundo Campos (2007) e Alves (2006), é oriunda dos tempos de guerra, portanto, utilizada para planejamento militar e, assim como Porter (1986), também usada como diferencial competitivo.

Conforme Davenport e Prusak (1997, p.46) a estratégia é um processo contínuo e incremental para manter a direção organizacional de acordo com seus objetivos, ou seja, em sintonia aos conceitos de Campos (2007, p.49) que informa ser fato que o contexto estratégico é fundamental para definir ou contribuir para a gestão da segurança da informação. Vê-se que tanto a estratégia quanto a gestão da segurança da informação são baseadas em iteratividade, portanto, não podem ser tratadas como um projeto com início e fim.

Embora haja muitos conceitos diferenciados de estratégia, conforme Mintzberg *et al.* (2003, p. 23), muitos adotam o conceito de Porter (1986) que assim a define como "[...] conceito firmemente integrado, claramente coerente e altamente deliberado, que coloca a empresa em posição de obter vantagem competitiva.".

Rezende (2008, p. 2) acrescenta que para se criar estratégia com efetividade deve-se ter o Pensamento Estratégico[8] para dominar o presente e conquistar o futuro. Cita ainda que o alinhamento estratégico contemple a inteligência organizacional e que este é formado por quatro grandes construtos a seguir relacionados: "[...] tecnologia da informação; sistemas de informação e sistemas de conhecimentos; pessoas ou recursos humanos; e contexto ou infra-estrutura organizacional." (REZENDE, 2008, p. 7)

Para Laurindo *et al.* (2001) , Rathnam *et al*. (2005), TI é um elemento estratégico que sustenta as operações de negócios, portanto, o alinhamento entre negócio e TI é fundamental para a sustentabilidade das organizações.

Henderson e Venkatraman (1993), na mesma linha de Laurindo *et al.* (2001) e Brodbeck *et al.* (2005) , acrescenta informando que os problemas advindos do retorno dos investimentos em TI são justamente por causa da falta de alinhamento de TI com o negócio, considerando-se assim um risco aos projetos, em conformidade com Campos (2007, p. 50) quando informa que a análise de riscos é fator tanto para a proteção dos ativos quanto para a aplicação inteligente dos recursos da organização.

Laurindo *et al.* (2001), alinhado com Sêmola (2003) e Alves (2006), defendem a necessidade de adoção de uma estrutura organizacional adequada para dar base ao alinhamento entre negócios, tecnologia da informação, e, respectivamente, à GSI.

Chan e Reich (2007), Luftman (2000), Reich e Benbasat (1996), relatam, juntamente com pesquisas recentes, que a alta cúpula estratégica das organizações reconhece, com preocupação, a necessidade de alinhamento entre estratégias de TI e estratégias de negócio. Em sentido oposto, quando o assunto é o alinhamento entre segurança da informação e estratégias de negócio, Sêmola (2003, p. 13) alerta para o fato dos executivos não terem visão holística sobre os riscos que envolvem o ambiente corporativo, ou seja, eles vêem somente a ponta do *iceberg*, analogia esta que se refere ao fato de que este tem volume muito maior e fora da área de visibilidade do observador.

Luftman (2000) relata que, quando há existência harmônica entre a tecnologia da informação e a estratégia de negócios, essas são coesas, ocorrem simultaneamente e fazem

---

[8] Para Rezende (2008), o Pensamento Estratégico é a arte de criar estratégias com efetividade.

parte de um mesmo planejamento. Então, por dedução lógica devido aos relacionamentos existentes entre disciplinas comuns a ambas, pode-se concluir que esta afirmação também é valida para a estratégia de segurança da informação uma vez que a mesma é parte das práticas de mercado para GTI e, juntamente com essas, a necessidade de regulação que, conforme ITGI (2006), Andrade e Rossetti (2009), Lahti e Peterson (2006), Fernandes e Abreu (2008), estabelecem o alicerce para a boa governança corporativa.

Para Sêmola (2003, p. 33) a estratégia de segurança é uma etapa de um modelo de gestão corporativa de segurança e da Governança de Segurança da Informação, cujo objetivo é o de definir um plano de ação com particularidades estratégicas, táticas e operacionais mapeadas através de um inventariado de ativos, da relação entre processo de negócio e seu ambiente, do ciclo de vida da informação, e das demandas do negócio além de contemplar também diversos tipos de riscos tecnológicos, humanos e físicos.

Por ter o assunto segurança da informação surgido originalmente a partir de raízes sob o contexto de tecnologia da informação, alguns modelos utilizados possuem características semelhantes, o que pode ser atestado no modelo de maturidade em GSI do ITGI (2006). Esse modelo que é baseado no COBIT e este, originalmente baseado no CMMI[9], também defendido por Beal (2008, p.40), e está em conformidade com o apresentado nos ANEXOS B e C, que servirão também para enriquecer o relacionamento dos construtos apresentados.

O modelo de maturidade em GSI do ITGI (2006) pode ser utilizado pela alta gestão da empresa para verificar seu posicionamento no nível de maturidade, entretanto, diferentemente dos modelos de Henderson e Venkatraman (1993) e Luftman (2000) esse modelo está inserido no contexto de segurança da informação, portanto sendo mais relevante aos objetivos a serem atingidos pelo presente estudo.

O modelo de maturidade, adaptado pelo ITGI (2006), estabelece níveis assim como o CMM (*Capability Maturity model for Software*), conforme (PAULK *et al*., 1993) e Luftman (2000).

---

[9] Para Fernandes e Abreu (2008) o CMMI (*Capability Maturity Model Integration*) originalmente foi criado como um modelo de maturidade para Engenharia de Software. Posteriormente, após a unificação de vários padrões CMMs viu-se que o CMMI poderia ser utilizado para medições de várias disciplinas do mundo corporativo.

Logo abaixo uma visão do modelo de Luftman (2000):

a) nível 0 – Gerenciamento dos processos não implantado;

b) nivel 1 – Processos de apoio são desorganizados;

c) nível 2 – Processos seguem um padrão;

d) nível 3 – Processos documentados e comunicados;

e) nível 4 – Processos são monitorados e mensurados;

f) nível 5 – Boas práticas são seguidas e automatizadas.

Realizando-se uma analogia ao modelo de Luftman (2000), o modelo do ITGI (2006) fornece subsídios para que a empresa verifique onde ela está e onde deve chegar para ter a maturidade em GSI. Além disto, assim como Luftman (2000) o modelo do ITGI também pressupõe a existência de alinhamento estratégico nas organizações mesmo que em níveis mínimos.

A descrição completa dos níveis e seus significados no contexto de GSI são mais bem detalhados no QUADRO 3.

A ausência de informações acerca da participação dos indivíduos nos processos de alinhamento estratégico dos modelos tradicionais de Henderson e Venkatraman (1993), Luftman (2000), Miles e Snow (1984), dentre outros, atestada por Prieto e Carvalho (2006), não é refletida no modelo de maturidade do ITGI (2006), pois este contempla uma das principais causas de falhas em segurança que, conforme Beal (2008) é justamente o ser humano.

Luftman (2004), Sêmola (2008), Alves (2006), Campos (2007), Beal (2008), acordam que a TI por si só não garante sozinha a entrega de valor ao negócio, sendo necessários outros componentes, dentre estes, o *compliance* e a segurança da informação, intrinsecamente para o primeiro, se a organização está sob fiscalização de órgãos reguladores.

Nos próximos tópicos o assunto sobre alinhamento estratégico está dissolvido entre outras teorias sempre relembrando a relevância do mesmo para as ações de GTI, GSI e GC.

2.2 Governança corporativa

Para iniciar a apresentação deste construto, aprecia-se a definição do IBGC (2009), referência em assuntos de GC no Brasil:

> Conceitualmente, a Governança Corporativa surgiu para superar o 'conflito de agência', decorrente da separação entre a propriedade e a gestão empresarial. Nesta situação, o proprietário (acionista) delega a um agente especializado (executivo) o poder de decisão sobre sua propriedade. (IBGC, 2009).

Realizando um retrospecto histórico para chegarem-se as origens da governança corporativa é importante citar as concepções propostas por Werner Sombart com sua concepção idealista, Max Weber e seu racionalismo, e, finalmente Karl Marx com sua concepção crítica, que segundo Andrade e Rossetti (2009), não conflitam entre suas definições, e apontam o capitalismo como fruto de um espírito empreendedor da busca incessante pelo lucro e até mesmo de aspectos morais e religiosos.

O desenvolvimento do sistema capitalista, segundo Maurice Dobb (1963) *apud* Andrade e Rossetti (2009, p.31), foi concebido de uma miscelânea de componentes afirmados na sua frase: "Período algum da história é feito de um só tecido – todos os períodos são misturas complexas de diferentes elementos.", portanto, evolui devido aos seguintes aspectos: a ética Calvinista, a doutrina liberal, a revolução industrial, o desenvolvimento tecnológico incessante, a ascensão do capital, o sistema de sociedade anônima, o crash de 1929-1933, o desenvolvimento da ciência da administração e, finalmente, o agigantamento das corporações e o divórcio propriedade-gestão.

As organizações se vêem diante do desafio de seguir a estratégia de negócio em um sistema capitalista voraz e heterogêneo, provendo auto-suficiência, e se resguardando de riscos pertinentes à evolução tecnológica e as mudanças estratégicas que, segundo Mintzberg

(2003, p.21), exigem comprometimento das cinco partes básicas da organização[10], sendo a cúpula estratégica, a parte mais importante da organização, pois:

> [...] é encarregada de assegurar que a organização cumpra sua missão de modo eficaz e também que atenda às necessidades dos que a controlam ou que detêm poder sobre ela (como seus proprietários, órgãos governamentais, sindicatos de empregados, grupos de pressão). (MINTZBERG, 2003, p.24).

E levando em consideração os problemas na governança da cúpula estratégica, Andrade e Rossetti (2009) citam três marcos que foram pilares da moderna governança corporativa: o Ativismo pioneiro de Robert Monks[11], o Relatório Cadbury e os princípios da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE). Robert Monks foi o pioneiro nos Estados Unidos e teve seu trabalho centrado em dois vetores: *Fairness* (senso de justiça) e *Compliance* (conformidade legal, especialmente relacionada a direito dos minoritários passivos). Outros países também aprimoraram seus modelos e, conforme Bettarello (2008), em maio de 1991 foi criado em Londres o *Committee on the Financial Aspects of Corporate Governance* que ficou conhecido por *Cadbury Committee* culminando em 1992 com o *Cadbury Report,* sendo o pioneiro na divulgação das práticas de governança corporativa.

No âmbito mundial a publicação da Organização para Cooperação e Desenvolvimento Econômico (OCDE), segundo Andrade e Rossetti (2009), tornou seus princípios uma referência internacional.

Também na cúpula estratégica, Jensen e Meckling (1976), declarando a inexistência do agente perfeito (Axioma de Jensen e Meckling), e Klein (1985), informando sobre a inexistência de um contrato completo (Axioma de Klein) contribuem com este estudo na medida em que colocam fatores de riscos imprevisíveis que afetam a gestão das organizações.

A consequência desses axiomas, segundo Andrade e Rossetti (2009, p. 140) é justamente o conflito de agência que foi o despertar da governança corporativa e seus valores que lhe dão sustentação como:

---

[10] Para Mintzberg, as organizações são compostas por cinco partes: o núcleo operacional, a tecnoestrutura, a linha intermediaria, a assessoria de apoio e, finalmente, a cúpula estratégica.

[11] Para Andrade e Rossetti (2009), Robert Monks, nascido em 1933 em Boston, EUA, advogado, classe média, foi um empreendedor bem sucedido e ativista singular da Governança Corporativa. Escritor de vários livros proclamou a necessidade primordial de monitoramento das empresas por seus acionistas.

a) o *Fairness* (senso de justiça, equidade no tratamento dos acionistas);

b) o *Disclosure* (transparência das informações);

c) o *Accountability* (prestação de contas);

d) o *Compliance* (conformidade).

A governança corporativa varia entre nacionalidades, pois leva em consideração aspectos políticos, culturais, econômicos, morais e religiosos, estes dois últimos, em consonância com a obra de Weber (2007) em "A ética do protestantismo e o espírito do capitalismo".

Andrade e Rossetti (2004) e Bettarello (2008) apontam que justamente os elementos apresentados justificam os diferentes modelos de governança corporativa. Citam ainda que existam cinco modelos: o modelo Anglo-Saxão, o modelo Germânico, o modelo Japonês, o modelo Latino-Europeu e o modelo Latino-Americano.

Pela contextualização e domínio do assunto nos quais este trabalho está inserido, as referências sobre governança corporativa são baseadas no modelo latino-americano, este que, conforme Andrade e Rossetti (2009) têm as seguintes características: o mercado de capitais é pouco expressível, a propriedade é concentrada, a gestão é exercida por acionistas majoritários, o conflito de agência é predominante, acionistas minoritários tem pouca proteção legal, as forças mais atuantes são as internas, pois as forças externas ainda dependem de um ambiente regulatório em transição, bem como a governança corporativa ainda é embrionária, mas é ajudada pelo capital estrangeiro que entrou com força nas privatizações, e finalmente, prevalecem os interesses dos acionistas.

O conflito de agência, ainda conforme Andrade e Rossetti (2009), é o conflito de interesses entre acionistas e gestores ou acionistas majoritários e minoritários com origem na dispersão do capital das corporações e na consequente separação entre propriedade e gestão. Justifica-se pelas diferentes raízes históricas de governança corporativa, e também nos dois axiomas fundamentais sintetizados por Klein e Jensen-Meckling: respectivamente, a ausência do contrato completo e a inexistência do agente perfeito.

Da mesma forma que os modelos são diferenciados, os conceitos sobre governança corporativa também variam e, para este trabalho, adota-se os conceitos dos

"Princípios de Governança Corporativa" da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), citado por Weill e Ross (2006, p. 5), a qual define governança corporativa como "[...] a criação de uma estrutura que determinasse os objetivos organizacionais e monitorasse o desempenho para assegurar a concretização desses objetivos".

O IBGC (2009, p.54) dá ênfase à transparência (*disclosure*) necessária para a boa governança informando que "O diretor-presidente deve garantir que sejam prestadas aos *stakeholders* as informações de seu interesse, além das que são obrigatórias por lei ou regulamento, tão logo estejam disponíveis."

Ashforth (2008), Misangyi *et al.* (2008), Pfarrer (2008) e Pinto *et al.* (2008) contribuem com a contextualização relativa a formas de corrupção *top-down* e *down-top* que ilustram a forma como ocorrem alguns dos problemas existentes na SI.

Monks e Minow (2008, p. 331) relatam que estudos recentes de advogados, economistas e administradores, direcionam que dar mais autoridade aos empregados sobre seus trabalhos é fator imprescindível para o crescimento da corporação sendo muito mais produtivo para a vitalidade organizacional do que o próprio interesse dos acionistas. Ao mesmo tempo elaboram um estudo sobre os casos de incidentes de segurança contemporâneos que abalaram o mercado internacional.

Ribeiro e Andrade (2004) em seu trabalho conseguem relacionar a forma com que o estado reconhece, manipula e manuseia a informação trazendo à reflexão a governança informacional e a relação existente entre o exercício pleno da cidadania e o acesso à informação pública e governamental e sua consequência no combate à corrupção.

Para Sêmola (2008) as ações de GRC – gestão de riscos e *Compliance* são forte apoio à governança corporativa na medida em que essa é implementada através de *frameworks* de governança como COSO (*Committee of Sponsoring Organizations of the Treatway Commission)*, ITIL (*Information Technology Infrastructure Library*) e COBIT (*Control Objectives for Information and related Technology*); *frameworks* de gestão de riscos como ISO 31010 e ERM, e *frameworks* de conformidade como SOX (Sarbanes Oxley), BASELII (Basiléia II) e ainda regulamentações setoriais específicas. Os mais relevantes para a metodologia serão descritos no item 2.5 desta seção.

Bergamini Junior (2005), D'Avila e Oliveira (2002), e Imoniana (2008) aprofundam os estudos sobre os controles internos das organizações como um mecanismo de governança corporativa a partir do momento em que os mesmos são o pilar para a efetividade do atendimento aos marcos regulatórios porque são responsáveis pelo acompanhamento do "cumpra-se" na efetividade.

Conforme visto no conceito de governança de TI do ITGI (2010) a mesma é parte integrante da governança corporativa e, conforme ITGI (2006) deve estar alinhada em suas estruturas à GSI, portanto, o próximo tópico adentra na GTI caracterizando-a e apresentando-a no relacionamento entre construtos.

2.3 Governança de TI

Para o ITGI (2007), em concordância com conceitos de Fernandes e Abreu (2008, p. 34) e Henderson e Venkatraman (1993), a necessidade de avaliação do valor de TI, o gerenciamento de riscos e a necessidade de controle sobre as informações são a essência da governança de TI.

Para Weill e Ross (2006), governança de TI é: "[...] a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização de TI." (WEILL; ROSS, 2006, p. 8)

Weill e Ross (2006) dão embasamento internacional, ou seja, o que efetivamente acontece no mundo corporativo externo, ilustrando para este estudo um *benchmark* das práticas aplicadas de governança de TI no cenário de diversos países do mundo.

Para Fernandes e Abreu (2008, p.15) "o principal objetivo de Governança de TI é alinhar TI aos requisitos de negócio" e que este mesmo alinhamento deverá proporcionar a continuidade do negócio, atendimento às estratégias de negócio e aos marcos regulatório.

Cabe aqui ressaltar a importância do alinhamento estratégico e sua definição de acordo com Fernandes e Abreu (2008):

> O processo de alinhamento estratégico da tecnologia da informação procura determinar qual deve ser o alinhamento da TI em termos de arquitetura, infra-estrutura, aplicações, processos e organização com as necessidades presentes e futuras do negócio. (FERNANDES; ABREU, 2008, p.17).

O parágrafo acima encontra fundamento nas alegações de Laurindo *et al.* (2001) Porter e Millar (1985) e Luftman (2004) quando reconhecem a TI como parte estratégica das organizações.

Alinhar TI ao negócio também é estar em conformidade, e para Fernandes e Abreu (2008) existem vários órgãos reguladores que vão desde a área de saúde, telefonia, financeira, dentre outros, especificamente sobre o crivo da *Sarbanes Oxley Act* (SOX) e o Acordo da Basiléia II. O primeiro, com foco na regulação de empresas de capital aberto destinadas a movimentação na bolsa de valores de Nova Iorque e, o segundo, patrocinado pelo *Bank for International Settlements* ou BIS ou Banco Central dos Bancos Centrais, com sede na Basiléia na Suiça.

Os marcos regulatórios provém requisitos que afetam a TI e consequentemente fazem parte da governança de TI principalmente nas disciplinas ligadas à gestão de riscos que é domínio da Governança em Segurança da Informação.

Com Mansur (2007) aprofunda-se nas disciplinas que compõem os modelos *(frameworks)* existentes de governança justamente para realizar a referência cruzada entre governança corporativa e governança de TI, pois o estudo propõe apresentar o relacionamento dos itens comuns, seja um padrão de ferramentas, software, peopleoware, hardware, normas, marcos regulatórios ou ISOs.

O assunto governança de TI, iniciado no item 2.1 sobre o assunto de alinhamento estratégico, é referenciado nos tópicos restantes, principalmente por conter em sua estrutura, o *compliance* e a segurança da informação bases para a GSI e que juntos são ponto comum nas práticas contempladas no item 2.5.

2.4 Governança de Segurança da Informação (GSI)

Inicia-se este tópico com a definição de Beal (2008, p. 1) sobre o que é segurança da informação "[...] Segurança da Informação pode ser entendida como o processo de proteger informações das ameaças para sua integridade, disponibilidade e confidencialidade."

Os conceitos sobre informação e conhecimento, adotados por Jamil (2005) servem de ligação no tratamento dos riscos inerentes a informação em determinado contexto se aproximando dos conceitos de tratamento da informação na disciplina de gestão dos riscos. O estudo sobre o conhecimento colabora para desenvolver este trabalho tocando no ponto mais frágil da segurança que, segundo Beal (2008), é o ser humano.

Sêmola (2008) define a Governança como "[...] um atributo de administração dos negócios que procura criar um nível adequado de transparência através da definição clara de mecanismos de tomada de decisão e gestão que irão garantir a aderência aos processos e políticas estabelecidas." somando-se a definição acima de Beal (2008) a Governança em Segurança da Informação é um conceito que envolve a administração estratégica na proteção de um dos maiores ativos da empresa, a informação.

Segundo Farhat (1996, p.465) "A finalidade de governar é prover segurança, bem-estar e prosperidade dos que investem os governantes de poder." conceito este que respalda a transparência que é necessária para que a administração mantenha conformidade com seus investidores, reguladores e toda a sociedade.

Alves (2006, p. 5) introduz neste estudo o conceito de que governar é "[...] criar e manter uma estrutura organizacional eficiente e eficaz." alinhando-se aos conceitos de Mintzberg (2003, p. 24), sobre a cúpula estratégica de uma empresa, nos quais o mesmo informa que a essa é "[...] é encarregada de assegurar que a organização cumpra sua missão de modo eficaz e também que atenda às necessidades dos que a controlam ou que detêm poder sobre ela [...]"

A estrutura organizacional fortemente projetizada, modelo defendido por Nonaka e Takeuchi (1997) como a melhor para a inovação e consequentemente para a competitividade, não é aderente ao modelo a ser adotado na Governança em Segurança da

Informação, pois esta como um processo contínuo e cíclico, não pode ter fim como os projetos. As soluções de segurança são contínuas, exigem acompanhamento e, justamente por isto, muitas vezes são comercializadas com serviços adicionais. O dilema entre a competitividade versus a aceitação, rejeição e mitigação dos riscos é justamente o ponto de equilíbrio exigido na gestão de riscos defendido por Westerman e Hunter (2008, p.111), Sêmola (2003, p.56), Campos (2007, p.85), Alves (2006, p.59) e Beal (2008, p.13).

Kerzner (2009, p.743) define risco como a probabilidade e impacto de não se alcançar os objetivos do projeto praticamente alinhado com risco de ti que segundo Westerman e Hunter (2008, p.1) é "[...] a possibilidade de que algum evento imprevisto, que envolva falha ou mal uso de TI ou à central de dados da empresa."

Portanto, dentro dos conceitos vistos anteriormente pode-se dizer que o ITGI (2006) ao definir a Governança em Segurança da Informação consegue realizar a junção das idéias principais sobre o assunto:

> A Governança em Segurança da Informação é um subconjunto da Governança Corporativa que fornece direção estratégica, garante que os objetivos sejam alcançados, gerencia os riscos de forma adequada, usa os recursos organizacionais responsavelmente, e monitora o sucesso ou falha do programa de segurança corporativa. (ITGI, 2006, p. 18, *tradução do autor*).

Allen (2005) complementa a definição de GSI da seguinte forma:

> Dirigir e controlar uma organização para estabelecer e sustentar uma cultura de segurança na condução da organização (crenças, comportamentos, capacidades e ações). Tratar de segurança adequadamente como requisito inegociável de estar no negócio.

Esta definição também tem apoio em Westerman e Hunter (2008, p.126) quando incluem a consciência do risco como fator mitigante de ameaças como vazamentos em todos os alicerces comprometendo a eficácia do processo de governança.

A necessidade das pessoas desenvolverem a estratégia de segurança alinhada com objetivos de negócio, desde a alta direção da empresa até o operacional, é fundamental para que os requisitos obtidos a partir da estratégia de negócios, definida pelo corpo diretor, sejam ponto de partida para o gerenciamento dos riscos, para a estratégia de segurança, e que

fomentam juntos os requisitos necessários à segurança da informação subsidiando as ações do CISO[12], do Comitê Diretor e Diretoria.

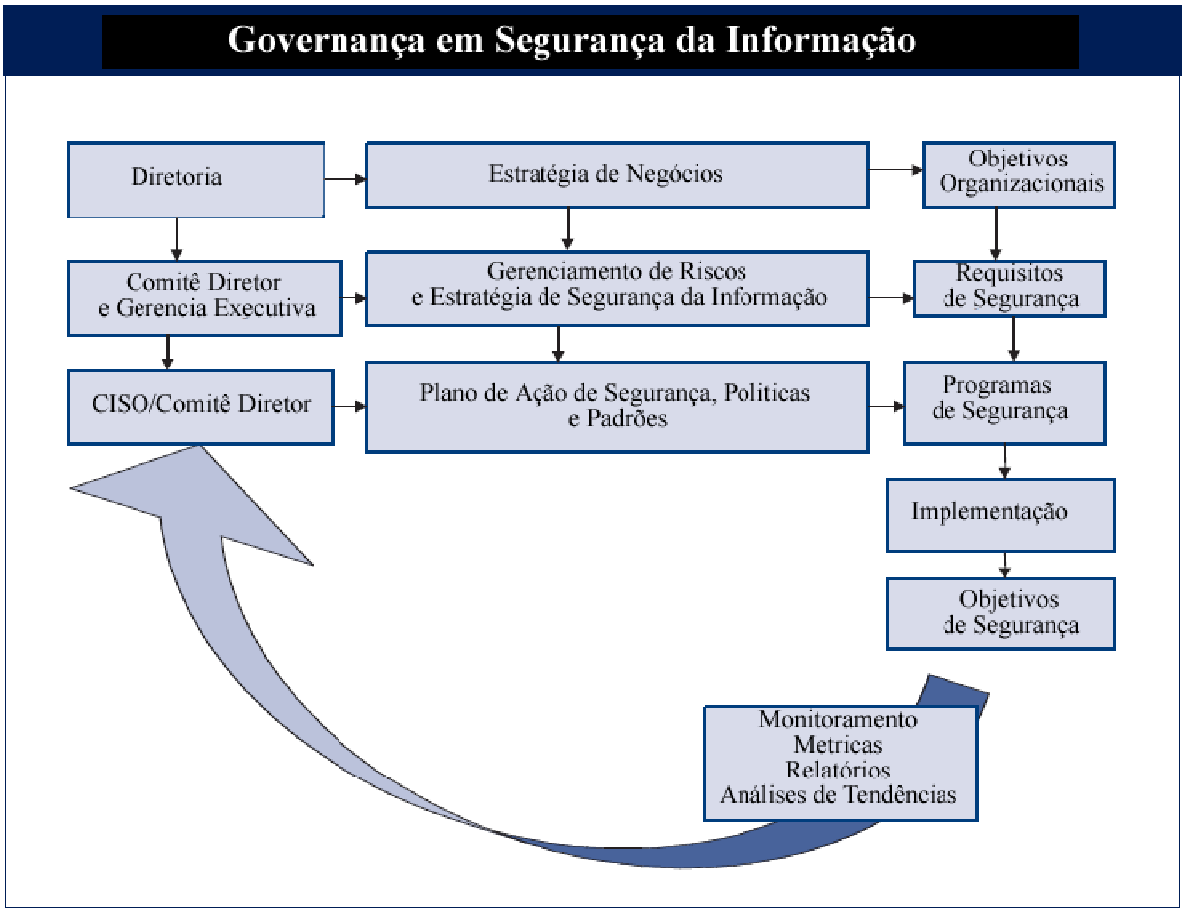

FIGURA 2 - A Governança de Segurança da Informação
Fonte: ITGI, 2006.

Na FIG. 2, percebe-se o relacionamento entre os construtos deste estudo, alinhamento estratégico, governança de TI, GSI, evidenciando a necessidade de validação da aderência destes nas organizações em busca do último construto, a governança corporativa. O Comitê Diretor juntamente com o CISO, fundamentados no gerenciamento de riscos e na estratégia de segurança da informação, são os responsáveis diretos pelo plano de ação de segurança e pelas políticas e padrões a serem seguidos através de requisitos de segurança e de programas de segurança. Para saber se os objetivos de segurança foram atingidos utiliza-se de

[12] CISO: *Chief Information Security Officer* é o Gestor de Segurança da Informação. Segundo o ITGI (2006) pode até mesmo ser o Executivo maior da empresa, ou seja, a importância desse profissional de segurança é de alta direção e estratégico para a empresa.

monitoramento, métricas, relatórios e análises de tendências para novo reporte ao CISO e Comitê estabelecendo assim o processo cíclico da GSI em conformidade com o modelo IDEAL descrito a seguir.

Conclui-se que a FIG. 2 ilustra os conceitos apresentados e tem em sua definição a forma como o processo de Governança em Segurança da Informação subsidia a estratégia de negócio e consequentemente os objetivos organizacionais.

Allen e Carnegie (2007) ressaltam que nos dias de hoje para se chegar a um resultado esperado de sustentabilidade, os conselhos de administradores, incluindo diretores, executivos, gerentes e demais *stakeholders* obrigatoriamente devem incluir a Governança em Segurança da Informação como responsabilidade dos participantes, desde a alta direção até as camadas mais operacionais da empresa.

Entretanto, conforme Campos (2007, p.29) e Sêmola (2003, p.14), dentre as dificuldades existentes para se governar a segurança da informação, pode se afirmar que justamente a distância entre a percepção da alta administração sobre a importância e relevância do assunto acaba exigindo do profissional de segurança o conhecimento da estratégia e do negócio da empresa para que todos possam atingir seus objetivos. Conhecimento que é respaldado por Magalhães e Pinheiro (2007, p. 35) quando afirmam o novo cenário da área de TI que deverá garantir que tudo que é feito é em função da estratégia de negócio.

Para o CERT[13] (2010) a segurança da informação é um termo relativamente novo para a governança das organizações, entretanto, algumas ações para conscientização do corpo diretor das empresas estão sendo tomadas, principalmente nos Estados Unidos em virtude de crescentes ameaças financeiras e terroristas que o país enfrenta.

Na mesma linha de Allen (2005) em entender a GSI como sustentação da cultura de segurança a ser preservada para se atingir os objetivos de negócio, o CGTF[14] (2004) já

---

[13] O CERT ® *Program* é parte do *Software Engineering Institute* (SEI), uma pesquisa financiada pelo governo federal e centro de desenvolvimento na Universidade Carnegie Mellon em Pittsburgh, Pensilvânia. Trata-se de um centro para coordenar a comunicação entre especialistas de segurança em situações de emergência e para ajudar a prevenir futuros incidentes.

[14] O CGTF (*Corporate Governance Task Force)* foi criado em dezembro de 2003 para desenvolver e promover um coerente modelo de governança para guiar a efetiva implementação dos programas de segurança da informação. (CGTF, 2004, *tradução do autor*).

propunha adotar o modelo IDEAL (*Initiating, Diagnosing, Establishing, Acting, Learning*), criado pela Universidade Carnigie Mellon da Califórnia, para implantar a Governança em Segurança a Informação dentro da própria estrutura organizacional. O modelo é composto por cinco fases iterativas conforme descrito abaixo:

a) inicialização (*initiating*) – estabelecer as bases para um esforço bem sucedido;

b) diagnóstico (*diagnosing*) – determinar onde você está em relação aonde quer chegar;

c) elaboração (*establishing*) – planejar os detalhes de como você vai chegar lá;

d) ação (*acting*) – trabalhar de acordo com o planejado;

e) aprendizado (*learn*) – aprender com a experiência e melhorar sua capacidade de adotar novas melhorias no futuro.

O Modelo é descrito em quatro funções que serão adotadas como roteiro para este estudo, bem como são desdobradas em cinco domínios de uma GSI eficaz e que são utilizados na avaliação do nível de maturidade do modelo do ITGI (2006) e nas questões de pesquisa, são eles:

a) **dependência do negócio**: mensurando a dependência de uma organização em relação à tecnologia da informação para a continuidade dos negócios, bem como o grau de interdependência do setor e regulação;

b) **gerenciamento de riscos:** avaliando o processo de gestão de risco no que se refere à criação de uma estratégia de informação e um programa de segurança;

c) **pessoas:** avaliando os aspectos organizacionais do programa de segurança da informação;

d) **processos:** identificando os processos que devem ser parte de um programa de segurança da informação.

O ITGI (2006), com ênfase na responsabilidade atribuída ao quadro de diretores sobre as informações estratégicas das organizações, informa que os mesmos deverão participar das seguintes ações:

a) compreender a importância crítica da informação e segurança da informação da organização;

b) rever o investimento em segurança da informação para o alinhamento com o perfil de organização e estratégia de risco;

c) endossar o desenvolvimento e implantação de um abrangente programa de segurança da informação;

d) requerer relatórios sobre a efetividade e adequação do programa de segurança da informação.

A visão do ITGI acima também é defendida por Alves (2006) que acrescenta aos desafios de governar a segurança das informações, adotar e seguir as Melhores Práticas[15] de mercado e cuidados exigidos pelo mercado bem como atender as exigências legais e regulamentares alinhadas com a estratégia da organização.

Lonsane[16] (2010) ressalta que "Quando uma organização é conhecida por melhores práticas de governança de segurança da informação, recursos e ações da empresa podem facilmente alcançar aumento significativo no valor." *(Tradução do autor).*

Seguindo o modelo IDEAL, é necessária a adoção de uma ferramenta para verificar o grau com que uma organização tenha implantado a Governança em Segurança da Informação no nível estratégico da empresa e, dentre outras, vale citar a *ISG Assessment Tool* (ferramenta de avaliação de Governança em Segurança da Informação) utilizada para apoio referencial complementar às perguntas de pesquisa, pois considera os mesmos domínios ou assuntos estabelecidos para a pesquisa do comportamento do nível de maturidade em GSI.

---

[15] Para Alves (2006) o termo 'Melhores Práticas' é referente à unicidade de conhecimento e experiência de diversos executivos e gestores que atuaram durante anos para levar as organizações ao sucesso e para maximizar os resultados dos negócios.

[16] Lonsane, Raj. D é fundador da CCITO (*Cyber Crime & Insider Threat Obviation Solutions*) empresa indiana que provê soluções, treinamentos e consultoria na área de Crimes Cibernéticos.

Conforme orientação do próprio CGTF (2006), em conformidade com estudos realizados por Alves (2006) e Sêmola (2003), é necessário avaliar cada *framework* de acordo com a estrutura organizacional.

Embora dentre as finalidades deste estudo não esteja contemplada a metrificação da GSI e sim uma análise comportamental baseada em dados qualitativos, buscam-se modelos mais flexíveis que permitam embasamento em padrões já conhecidos do mercado brasileiro.

De certa forma, os modelos existentes incluem métricas que são apoiadas pelo modelo de métricas proposto por Pironti (2007) e adotados pelo ISACA·: *Developing Metrics for EffectiveInformation Security Governance:Baseline Metrics Frameworks.*

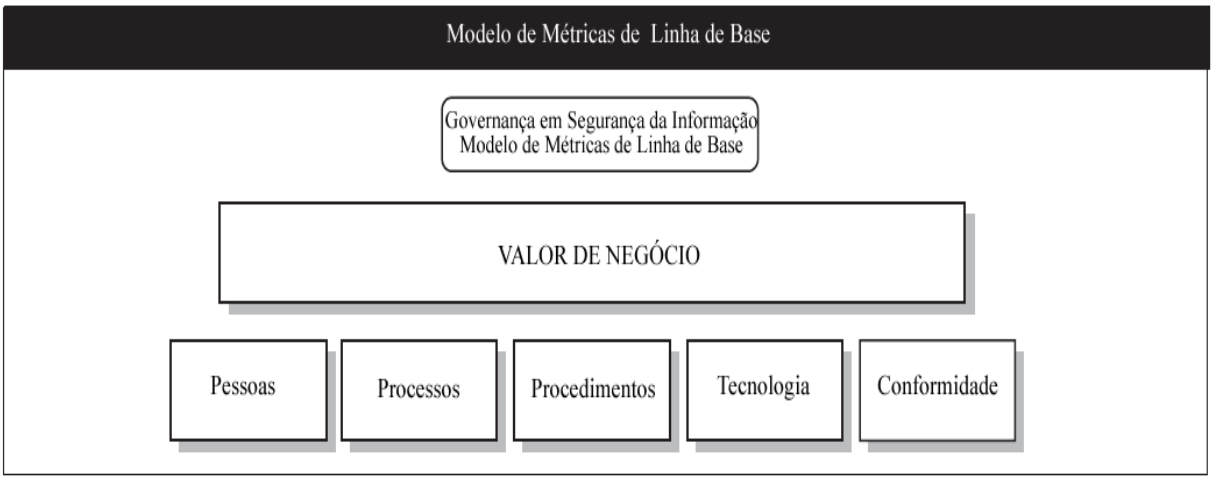

FIGURA 3 – Modelo de métricas de linha de base
Fonte: PIRONTI, 2007.

Linhas de Base ou *Baselines* de segurança da informação são o mínimo aceitável de segurança que deve ser fornecida para proteger recursos de informação. *Baselines* variam dependendo da sensibilidade e criticidade do ativo.

De acordo com Pironti (2007), este modelo deve ser flexível o bastante para permitir alterações nas métricas de acordo com o contexto ao qual a organização está inserida frente às ameaças. Essas métricas devem conter necessariamente *baselines* para pessoas, processos, procedimentos, tecnologia, conformidade e, principalmente, uma métrica que é o peso, ou controle versus custo de sua implantação para os negócios. Este custo pode ser implantado na forma de valores monetários, ou de impacto nos processos, impacto sobre a experiência do usuário ou mesmo a complexidade do trabalho devido ao novo controle.

Efetua-se a junção das teorias e orientações de Governança em Segurança da Informação indicadas pelo CGTF (2006), principalmente relativos ao modelo IDEAL e sua iteratividade, com o *framework* de Governança de Segurança da Informação do ITGI (2006), entretanto, como este trabalho tem cunho qualitativo por ser mais aderente aos objetivos propostos, o modelo de métricas de Pironti (2007) aqui descrito servirá não só para inserir as *baselines* no modelo de maturidade do ITGI (2006), mas também para ilustrar a possibilidade de se adotar metodologia quantitativa para trabalhos futuros.

O elo principal entre os dois frameworks de Governança em Segurança da Informação é justamente a ISO 17799 e o COBIT que, existentes em pontos comuns nos frameworks de governança de TI, consegue-se obter maior consistência nas bases teóricas inclusive refletindo nos níveis de maturidade e consequentemente no alinhamento estratégico.

Para contextualização do assunto proposto, em nível de mercado, colocam-se em evidência os estudos:

a) da Pricewaterhousecoopers (2*010*): "*The 2011 Global State of Information Security Survey*" pesquisa global com a participação de 135 países onde foram entrevistados 12.800 executivos e profissionais de segurança. Nessa pesquisa 77 % dos entrevistados apontaram o *Compliance* (conformidade) como maior motivador de investimentos em segurança da informação em suas organizações. Portanto, devido a importância desses componentes para a GSI, o fato do segmento estar sob regulação delimita a amostra primária deste trabalho;

b) do Gartner Group (2010): com a pesquisa "*The Gartner CyberThreat Landscape 2010*" que servirá para ilustrar o comportamento dos investimentos de TI na segurança da informação. A abordagem de selecionar as organizações que mais investem em TI é justamente por ter-se a dedução de que, em virtude da segurança da informação ser originariamente à partir da TI, maior investimento nesta pode contribuir com o nível de maturidade uma vez que haveria mais recursos para a segurança da informação;

c) da Pricewaterhousecoopers (2009a): com a pesquisa "Redefinindo o Sucesso" onde foram coletados dados o comportamento dos executivos perante vários

assuntos, principalmente, relativos à regulação e relacionamento com *stakeholders*;

d) da Pricewaterhousecoopers (2009b): com a "*The Global Economic Crime Survey*" onde foram coletados dados sobre os perfis dos incidentes de segurança mais cometidos no Brasil e exterior. Essa pesquisa também servirá como contextualização para a seleção da amostra, voltada para maiores organizações alvo de ataques, a ser detalhada na metodologia.

Alves (2006, p. 21) informa que, embora não haja uma fórmula para a implantação, há pontos-chave para se obter o sucesso na Governança de Segurança da Informação:

a) aderência aos requisitos legais através de políticas em acordo com Campos (2007, p. 141), Chambers e Rand (2010, p.118), Beal (2008, p. 149);

b) a linguagem em comum com executivos. Também defendido por Westerman e Hunter (2008, p.20);

c) o alinhamento a estratégia de organização em conformidade com Weill e Ross (2006, p.152), Fernandes e Abreu (2008, p. 36), Porter (1979);

d) a implantação de processos com níveis de maturidade conforme Luftman (2000) e Fernandes e Abreu (2008, p. 203);

e) a adoção de frameworks de segurança conforme Westerman e Hunter (2008, p.20), Beal (2008, p. 31), Fernandes e Abreu (2008, p. 420-421), em conformidade com Alves (2006, p. 102-106);

f) a utilização de métricas, conforme Pironti (2007).

Finalmente, ISACA (2008, p. 78), em acordo com o CGTF (2006) e ITGI (2006), define cinco resultados básicos do desenvolvimento de uma abordagem de governança eficaz em segurança da informação a serem descritos e utilizados como variáveis estudadas nos níveis de maturidade descritos na metodologia.

2.5 Práticas da GSI

As práticas de governança, segundo o ITGI (2005), servem para garantir aos gerentes, executivos, reguladores e *Stakeholders* em geral, de que o investimento em TI está protegido, é feito da melhor maneira, entrega valor ao negócio apoiado em padrões reconhecidos de mercado, e é crítica para a estratégia de negócio.

Segundo o CGTF (2006), o COBIT, o *Federal Information Security Management Act* (FISMA), e a ISO 17799 servem de referência na orientação de segurança da informação nas corporações e juntamente com o COSO fazem a base de apoio à governança corporativa.

Beal (2008), quando escreve sobre normas e padrões de segurança, ressalta os modelos mais utilizados para este fim dando ênfase no ITIL como sendo um conjunto de documentos desenvolvidos pelo governo Britânico. Ressalta que, embora não seja um padrão voltado para segurança da informação, colabora para estabelecimento de processos para TI e, por conseguinte, para o alcance dos objetivos de segurança.

Para Magalhães e Pinheiro (2007, p. 65) o ITIL "[...] não define processos a serem implantados na área de TI, mas, sim, demonstra as práticas que podem ser utilizadas para esta definição.", portanto, alinhado à Beal (2008), o ITIL é focado em TI.

O ITIL é composto por vários livros e assuntos que abordam as áreas de gestão de Incidentes, gestão de problemas, configuração, mudanças, níveis de serviços, dentre outros. Entretanto, o ITIL servirá apenas como referência para assuntos de tecnologia da informação em virtude deste estudo ser de governança, portanto, embasado para camadas mais gerenciais e superiores das organizações. Statdlober (2006, p. 40) vai além e afirma que o ITIL é superficial em segurança e Albertin e Sanchez (2008, p. 16) completam informando que a ISO 17799 (BS 7799-1) é voltada para assuntos mais práticos de segurança da informação. Essas afirmações têm apoio e relevância nos autores citados de Governança em Segurança da Informação.

Como visto o ITIL não tem uma abordagem mais voltada para alinhamento estratégico, gestão de riscos e conformidade, ficando mais restrito à entrega de serviços pela TI, sendo esses requisitos, segundo ITGI (2007) e Fernandes e Abreu (2008, p. 174), somente

para cobrir o sucesso da entrega de serviços (finalidade do ITIL), portanto, é necessário um modelo que controle a execução alinhada às expectativas e requisitos do negócio e para isto foi criado o COBIT em 1994 pelo ISACA.

Para Mansur (2007, p. 113) o ITIL, em contrapartida aos pontos fortes, tem como ponto fraco a segurança da informação sendo muito superficial nesse assunto, porém processos do COBIT alinhados a ISO 17799 provêem maior aderência aos requisitos de segurança.

Entretanto, o Gartner (2005) informa que tanto o ITIL quanto o COBIT não são mutuamente exclusivos e que para a efetiva governança de TI os dois são complementares.

Segundo o ITGI (2007, p. 7) o COBIT:

> O *Control Objectives for Information and related Technology* (CobiT®) fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. As boas práticas do CobiT representam o consenso de especialistas.

Para o ITGI (2006), no contexto da Governança em Segurança da Informação, o COBIT, juntamente com a ISO 17799, provê normas de segurança que garantem que todos os elementos de segurança fazem parte da estratégia de segurança da informação. Esta afirmação também é dividida com outros autores como Fernandes e Abreu (2008, p. 181), Mansur (2007, p. 113), Bernardes e Moreira (2005).

Conforme Mansur (2007, p. 113) e Bernardes e Moreira (2005) o COBIT é considerado por muitos como o a base da governança tecnológica e fornece métodos e padronizações para guiar a área de tecnologia da empresa principalmente com respeito a qualidade, segurança da informação e níveis de maturidade.

A FIG. 4 abaixo ilustra o conteúdo do COBIT, segundo o ISACA (2007), onde se percebe facilmente que o mesmo tem em sua base requisitos de alinhamento estratégico, *compliance* e segurança da informação, também exposto por Beal (2008), bem como se posiciona em um alto nível na organização. Estruturado em três altos níveis para dar suporte aos profissionais que atuam nos requisitos acima citados. Especificamente sobre Governança em Segurança da Informação, em conformidade com Fernandes e Abreu (2008, p. 186), o COBIT embasa os conceitos de Pironti (2007) sobre o *Security Baseline* colaborando para a

adoção de métricas que provêem o acompanhamento dos requisitos da boa governança e auxiliando a visão estratégica de segurança no nível mais alto da organização.

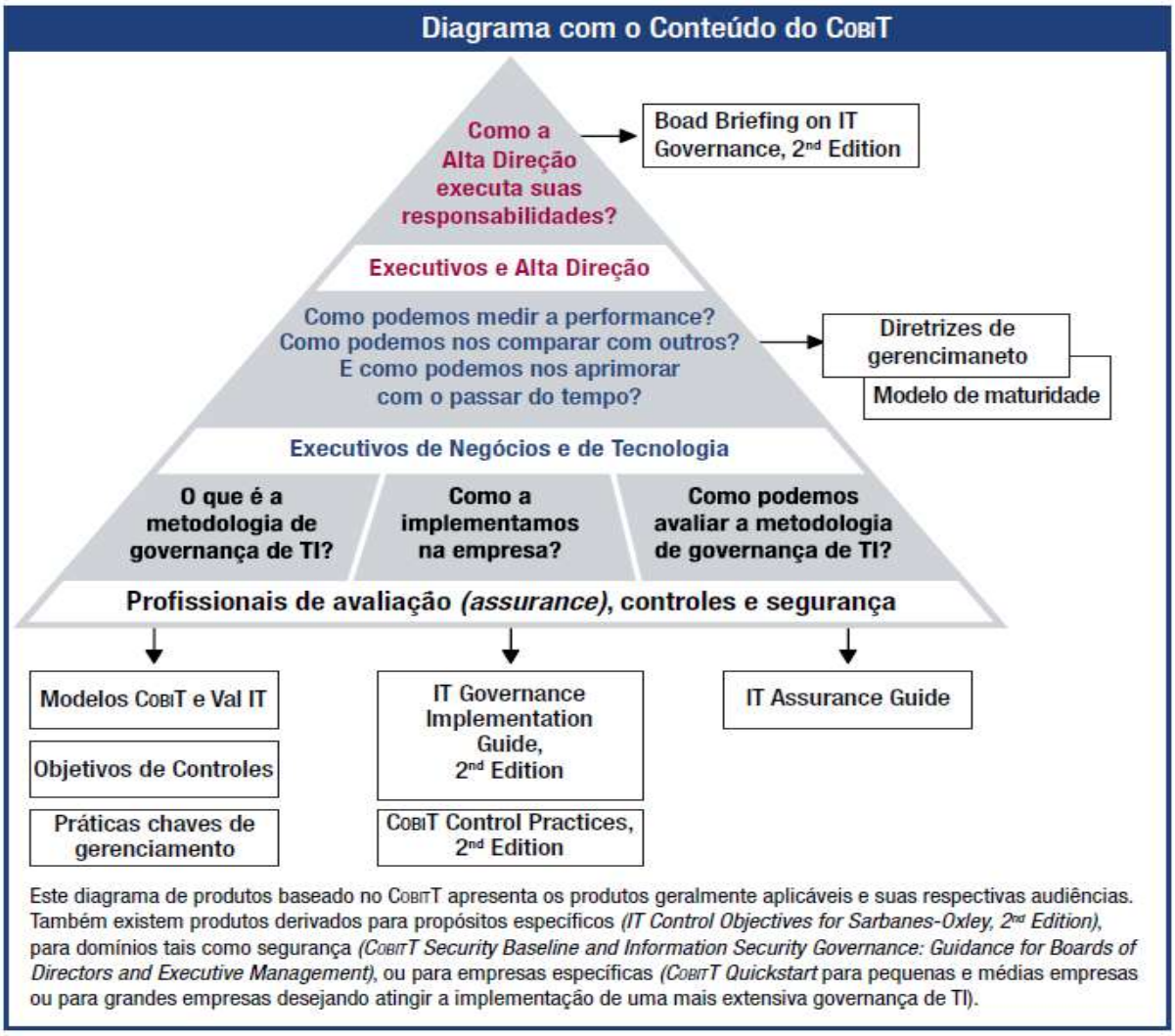

FIGURA 4 – Conteúdo do COBIT
Fonte: ISACA, 2007.

Fernandes e Abreu (2008), bem como Fagundes (2008), sobre a composição do COBIT informam que o mesmo é composto por quatro domínios e 34 processos de TI. Adicionalmente Fernandes e Abreu (2008) acrescentam questões gerenciais que o modelo responde em cada processo conforme ANEXO A.

Para o ITGI (2006), muitos processos do COBIT contemplam assuntos de segurança, entretanto, quatro processos são mais diretamente relacionados à segurança da informação, são eles:

a) PO 6 Gerencia a Comunicação das Direções de TI;

b) PO 9 Avaliar os Riscos;

c) DS 4 Assegura a continuidade dos serviços;

d) DS 5 Assegurar Segurança dos Serviços.

Fernandes e Abreu (2008, p. 181) dissertam que o controle exercido pelo COBIT sobre seus processos é através de objetivos, que segundo o ITGI (2007, p. 15) é "[...] o conjunto de políticas, procedimentos, práticas e estruturas organizacionais desenvolvidas para dar uma garantia razoável de que os objetivos de negócio serão atingidos e de que os eventos indesejáveis serão prevenidos ou mesmo detectados e corrigidos."

Portanto, conforme Alves (2006, p. 85) as empresas devem ter instrumentos que permitam a mensuração dos processos com seus objetivos de negócios, portanto, alinhado ao ITGI (2006) que criou o modelo de maturidade em Governança de Segurança da Informação baseado no COBIT, seguindo o CMMI, apresentado no QUADRO 3 sobre o nível de maturidade em GSI.

Como modelo de alinhamento da TI ao negócio o COBIT como qualquer *framework*, segundo Weill e Ross (2006, p. 158), necessita de instrumentos de mensuração e de responsabilidades para a implantação de uma boa Governança.

Para Pironti (2007) e ITGI (2006) as *Baselines* de segurança da informação, descritas anteriormente, são requisitos mínimos de segurança e são obtidas a partir da combinação de *frameworks* conhecidos como COBIT, ISO 17799 e publicações de risco e *compliance*. Um exemplo dessa combinação é o COBIT *Security Baselines* que é composto de controles e mapeamentos para a ISO 17799.

Gallegos e Senft (2009, p. 473) e ITGI (2006) definem a ISO 17799 como um conjunto de controles que consistem nas práticas de segurança em tecnologia da informação. Defendem ainda que uma empresa com maior aderência a ISO 17799 detenha vantagem competitiva alinhando-se aos pensamentos de Porter (1986), Westerman e Hunter (2008) e Campos (2007, p. 36).

Segundo Santos Junior, Fonseca e Coelho (2006) *apud* ABNT (2005) a norma 17799:2000 é oriunda da primeira parte da BS7799:1999 (*British Standard* 7799), norma britânica criada pelo BSI (*British Standard Institution*).

Beal (2008, p. 33), informa que a família de padrões BS-7799 trata da gestão de segurança da informação. A parte 1 desse conjunto de padrões corresponde ao Código de Práticas Para a Gestão da Segurança da Informação e a parte 2 corresponde ao ISMS (*Information Security Management System*), ou sistema de gestão de segurança da informação. Fernandes e Abreu (2008, p. 352) complementam e informam que a BS-7799 deu origem a série 27000 da seguinte forma:

a) BS 7799-1:1999 -> ISO/IEC 17799:2000 - *Information technology -- Security techniques -- Code of Practice for Information Security Management* ou Código de Prática para a Gestão de Segurança da Informação ;

b) BS 7799-2:2002 -> ISO/IEC 27001:2005 – *Information Security Management Systems – Requirements - (ISMS),* ou seja, Requerimento de Sistemas de Gerenciamento de Segurança da Informação, segundo Sêmola (2007), alinha-se à ISO/IEC 27005 na GRC – gestão de riscos e Conformidades;

c) ISO/IEC 27002 – *Code of Practice for Information Security Management* – que substitui a ISO 17799;

d) ISO/IEC 27004 - *Information Security Management Measurements* ou Medições para o Gerenciamento de Segurança da Informação;

e) ISO/IEC 27005 – *Information Security Risk Management* ou Gerenciamento de Riscos de Segurança da Informação;

f) ISO/IEC 27006 – *Requirements for bodies providing audit and certification of Information Security Management Systems* ou Requisitos para organismos de auditoria e certificação de Sistemas de Gestão de Segurança da Informação.

Segundo Chambers e Rand (2010, p. 484) a ISO/IEC 27014 – *Information Security Governance Framework,* ou Modelo de Governança em Segurança da Informação, ainda está em fase de concepção, portanto, para este trabalho não será um guia referencial, exceto, pontualmente em aspectos de segurança já consolidados na mesma.

Existem outras normas ISO voltadas para segurança da informação, porém não são foco para este trabalho, ficando o escopo deste estudo ISO voltado para as ISOs acima citadas principalmente referente a 27001, 27002 (17799:2005) e parte da 27014.

Foco deste tópico a ISO/IEC 17799:2005, ou ISO/IEC 27002, contempla as disciplinas de segurança mais importantes da organização conforme apresentado a seguir:

a) **política de segurança** – Fornece uma direção clara sobre os requisitos e objetivos de segurança. É formalizada através do documento "Política de Segurança" onde constam todas as políticas**;**

b) **segurança organizacional** – Com foco na informação dentro da organização, demanda de uma estrutura gerencial para iniciar e controlar a implementação da segurança de informações;

c) **gestão de ativos** – Com foco na informação, determina que a mesma tenha propriedade e segurança;

d) **segurança em recursos humanos** – Visa minimizar os riscos no elo mais frágil da segurança da informação responsável por casos de vazamento de informações, outros incidentes de segurança, além da má conduta perante a política de segurança;

e) **segurança física e do ambiente** – Controle de acesso físico às dependências da organização;

f) **gerenciamento das operações e comunicações** – Visa a gestão dos recursos operacionais e processamento de informações contemplando inclusive procedimentos para resposta à incidentes;

g) **controle de acessos** - Controlar o acesso às informações com base nos requisitos de segurança e do negócio;

h) **aquisição, desenvolvimento e manutenção de sistemas de informação** – Contempla os requisitos de segurança de aplicações para os sistemas de informação. Este requisito é muito utilizado em norma específica ISO/IEC 15408 (*Evaluation Criteria* f*or IT Security)*. Segundo Albuquerque e Ribeiro

(2002, p. 7) também conhecida como *Common Criteria* (ou Critérios Comuns para o desenvolvimento de software), o objetivo da norma ISO/IEC 15408 é estabelecer um conjunto de critérios fixos para o desenvolvimento de aplicações e de garantia de segurança para os clientes dessas.

i) **gestão de continuidade de negócios** – Visa implementação de controles que possibilitem que o negócio continue em funcionamento mesmo em situações críticas;

j) **conformidade** – Também chamada de *compliance*, tem como fundamento preservar a organização de infringir qualquer lei civil e criminal, estatutária, regulamentadora ou de obrigações contratuais, de quaisquer requisitos de segurança, em alinhamento com a governança corporativa.

Calder e Watkins (2005, p. 37) alertam que, independente de a ISO 17799 ser reconhecidamente um padrão para a segurança da informação, a mesma está sujeita a mudanças de acordo com estrutura organizacional de cada organização.

Para o ITGI (2005), as práticas necessitam estar alinhadas umas com as outras e com os procedimentos internos, portanto, o COBIT pode ser adotado em mais alto nível e o ITIL e a ISO 17799 como práticas devem ser mapeadas no primeiro. Para isto, Fernandes e Abreu (2008, p. 420-421), em conformidade com Alves (2006, p. 102-106) e ITGI (2005) propõem um alinhamento entre o COBIT 4.0 e a ISO 17799:2005[17] exclusivamente nos processos relacionados à GSI conforme o ANEXO A.

Calder (2009, p. 9), em acordo com Alves (2006, p. 31), estabelece a relação entre a ISO/IEC 27001 e 27002 (17799:2005) na especificação que esta faz a primeira para a concepção do ISMS. Em contrapartida, o caminho inverso é gerado quando se considera os controles detalhados para o desenvolvimento e implantação do ISMS contido na segunda parte da BS 7799.

Para Campos (2007, p.87) a ISO 27001 "[...] determina que controles mínimos devam ser considerados, ao passo que a norma 27002 orienta na implementação desses

[17] A ISO 17799:2005, conforme Fernandes e Abreu (2008, p. 352) já está sendo substituída pela ISO 27002, entretanto, a nomenclatura da primeira ainda mais referenciada no mercado.

controles.", portanto, enquanto a primeira é mais voltada para a gestão dos controles que respaldam os requisitos de segurança a segunda é mais voltada para a aplicabilidade dos referidos controles.

Solms e Solms (2008, p. 57) informam que a certificação ISO/IEC 27001, com a implantação do ISMS, pode consolidar os requisitos da ISO/IEC 27002. Solms e Solms (2008, p. 59) também ratificam que para a implantação do ISMS é necessária a adoção do PDCA (*Plan, Do, Check, Action*), também defendido por Watkins (2007 , p. 15), da seguinte forma:

QUADRO 1
ISO/IEC 27001 – Modelo PDCA para o ISMS

Planejamento (Estabelece o ISMS)	Estabelece o ISMS na política, objetivos, processos e procedimentos relevantes para o gerenciamento de risco e proporcionando a segurança da informação a entregar resultados em acordo com as políticas e objetivos da organização.
Realização (Implantação e Operação do ISMS)	Implanta e opera as políticas, controles, processos e procedimentos do ISMS
Monitoramento (Monitoramento e Revisão do ISMS)	Avalia e, quando aplicável, mensura o desempenho dos processos comparando com a política, objetivos e experiência prática e reporta os resultados para a revisão do gerenciamento do ISMS.
Ação (Manutenção e melhoramento do ISMS)	Realiza as ações preventivas e corretivas baseadas nos resultados de uma auditoria ou revisão ou outra relevante informação em relação ao ISMS. Para proporcionar a contínua melhora do ISMS.

Fonte: SOLMS; SOLMS, 2008, p. 59, *tradução do autor*.

Para a Wolcott (2007) a ISO/IEC 27001 é mapeada no marco regulatório Sarbanes Oxley na seção SOX 404 (a) (1), que abrange a responsabilidade pela gestão de manter uma estrutura de controles internos apropriados, e na seção 5 - Responsabilidade da Administração. Da mesma forma, a seção 404 (a) (2) abrange

uma avaliação da eficácia dos controles internos, que é mapeada com a norma ISO 27001, seção 7 - Análise dos ISMS.

Rebouças, Braga e Tundisi (2002) alinhado a Wolffenbüttel (2007) definem marco regulatório como conjunto de procedimentos, normas, leis e diretrizes para controle e fiscalização dos setores, nos quais os agentes privados prestam seus serviços, visando assegurar a conformidade e transparência.

Adentrando-se ao assunto de regulação, Campos (2007, p.141) informa que para se certificar na ISO 27001 é preciso garantir as evidências através de auditoria devidamente assinada pelo alto escalão das organizações. Campos (2007, p.213) acrescenta ainda que, mesmo com a utilização de uma política de segurança e um ISMS, os direitos dos *stakeholders* podem inadvertidamente serem infringidos principalmente na conformidade legal.

Na mesma linha de Campos (2007, p. 141), Chambers e Rand (2010, p.118) informam que as fraudes financeiras demandaram ações que culminaram na criação do COSO (*Committee of Sponsoring Organizations*) que é um marco como modelo nas ações, processos e relatórios dos controles internos. Esta definição também é adotada por Brand e Boonen (2007, p. 5) e tem sua relevância para este trabalho principalmente com a publicação em 2004 do *Enterprise Risk Management* (ERM) que é um modelo para a gestão de riscos Corporativos.

Para Moeller (2008, p. 280) o ERM difere dos outros modelos de gestão de risco, pois seus antecessores consideravam o risco em pequenas unidades, mas sem uma visão corporativa, ao contrário, o ERM dá uma visão corporativa dos riscos e não deixa de atender a gestão dos riscos em unidades menores. Complementa relatando que apesar do COSO ERM ser concebido após a SOX, esse é muito mais amplo do que a seção 404 da SOX, em acordância concordância com Lahti e Peterson (2006, p. 26) que informam que a mesma seção para muitos é incompleta.

O ERM é contemplado em uma das seções do *framework* de Governança de Segurança da Informação criado CGTF (2006) que se utiliza de conceitos e processos do COBIT e COSO para seu modelo de gestão de riscos.

Ainda referente à governança dos riscos, algumas metodologias auxiliam na consolidação do modelo de gestão de risco como a metodologia *Octave* para análise de riscos que foi desenvolvida, segundo Alves (2006, p. 65), pela Carnegie Mellon University e pelo *Software Engineering Institute* (SEI) ambos ligados ao CERT *Coordinator Center* e responsáveis pela criação do padrão CMM para desenvolvimento de software.

Alves (2006, p. 65) complementa informando que a metodologia *Octave* possui uma visão organizacional e estratégica da empresa, o que força o profissional do risco a entender do negócio, e pode ser utilizada por organizações de pequeno a grande porte.

Partindo-se para conformidades e controles internos, para Fernandes e Abreu (2008, p. 23) a SOX e o Acordo Basiléia II são fortes propulsores das ações de controles internos nas corporações, muito embora haja outros reguladores no âmbito nacional e internacional.

Para Moeller (2008, p. 1) a Sarbanes-Oxley (SOX) é oriunda desde a grande depressão da bolsa em 1930 e finalmente concebida em 2002, em acordo a Fernandes e Abreu (2008, p. 24) quando diz que o cume do escândalo da Enron Corporation, foi o motivador para a publicação da Lei.

Lahti e Peterson (2006, p. 26) e Moeller (2008, p. 3) destacam que dentre as mais importantes seções da SOX , respectivamente as seções 404 – Gerenciamento da Avaliação dos Controles Internos e a Seção 302 – Responsabilidade pelo Relatório Financeiro Corporativo são as mais importantes para a transparência, entretanto, Lahti e Peterson alegam que há discordância sobre a complementaridade entre as mesmas e que seriam redundantes, portanto, para efeito de maior abrangência aos controles internos será mais considerada a seção 404. Acrescentam ainda que nessa mesma seção a gerência executiva de capital aberto é responsável por: "[...] estabelecimento e manutenção de uma estrutura e de procedimentos de controle interno adequados à geração de relatórios financeiros" e "[...] relatar a eficácia da estrutura e dos procedimentos de controle interno." (LAHTI; PETERSON, 2006, p.27)

Devido à seção 404 não contemplar qualquer tratamento sobre TI, para Lahti e Peterson (2006, p.28), a maioria dos Auditores adotou o COBIT. Essa mesma adoção, segundo Fernandes e Abreu (2008, p. 30) ocorreu com a Basiléia II consolidando o COBIT como padrão de conformidade de TI, justamente por esta ser um dos elementos de risco

operacional de uma instituição financeira, e complementam informando a existência da Resolução 3380 do Banco Central do Brasil oriunda da Basiléia II.

Portanto, segundo o ITGI (2006), Alves (2006, p. 101-106), Fernandes e Abreu (2008, p. 163), para se atingir os critérios de Governança em Segurança da Informação é necessário obter o alinhamento entre os principais padrões de mercado ou práticas buscando os pontos comuns para atingir os objetivos de segurança da informação e, respectivamente, para se atingir os objetivos de negócio. Esses pontos comuns servem de embasamento para os questionários de pesquisas que constam nos APÊNDICES A e B, bem como são exemplificados nos ANEXOS B e C deste estudo e que também servem para verificar a eficácia de uma organização em relação à GSI.

3 METODOLOGIA

A pesquisa realizada seguiu a classificação de Collis e Hussey (2005, p. 23), abaixo definidas e justificadas de acordo com os objetivos atendidos por este estudo:

a) o objetivo da pesquisa – os motivos pelos quais é realizada – tipo de pesquisa adotada para este estudo: pesquisa exploratória, que conforme Gil (1999, p. 46):

> Um trabalho é de natureza exploratória quando envolver levantamento bibliográfico, entrevistas com pessoas que tiveram (ou tem) experiências práticas com o problema pesquisado e análise de exemplos que estimulem a compreensão. Possui ainda a finalidade básica de desenvolver, esclarecer e modificar conceitos e idéias para a formulação de abordagens posteriores.

Portanto, busca a compreensão dos fenômenos que envolvem o comportamento das organizações sob regulação ou não em relação à GSI bem como aos outros construtos que compõem este estudo;

b) o processo da pesquisa – a maneira pela qual se coleta e analisa seus dados – Tipo de Processo adotado para este estudo: Pesquisa Qualitativa, justamente para se focar na investigação do comportamento dos processos que envolvem a GSI;

c) a lógica da pesquisa – movimento do geral para o específico ou vice-versa - Tipo de lógica adotada para este estudo: Pesquisa dedutiva, para Grubits e Noriega (2004, p. 81) trata-se de "[...] a partir de teoria conhecida, procurar a confirmação ou informação de hipóteses previamente conhecidas." Justamente a proposta de basear-se nos teóricos de governança, governança de TI e Governança em Segurança da Informação para buscar a confirmação da presença desta no mercado brasileiro;

d) o resultado da pesquisa – resolve um determinado problema ou faz uma contribuição geral para o conhecimento - Tipo de resultado adotado para este estudo: Pesquisa básica.

Segundo Oliveira e Correa (2008, p.29) a metodologia consiste em:

> Descrição de métodos e técnicas utilizadas para a coleta de dados, para permitir a compreensão e a interpretação dos resultados, assim como a reprodução de procedimentos e, ou , a utilização do método por outros pesquisadores. (OLIVEIRA; CORREA, 2008, p.29).

Vieira e Zouain (2006, p. 17) definem a pesquisa qualitativa como "[...] a que se fundamenta principalmente em análises qualitativas, caracterizando-se, em princípio, pela não utilização de instrumental estatístico na análise de dados." alinhando se a Godoy (1995) que relata que a pesquisa qualitativa é proveniente da sociologia e antropologia, portanto a pesquisa qualitativa não procura medir eventos ou empregar instrumentais estatísticos.

Godoy (1995, p. 58) acrescenta que a pesquisa qualitativa "[...] considera o ambiente como fonte direta dos dados e o pesquisador como instrumento chave; possui caráter descritivo; o processo é o foco principal de abordagem e não o resultado ou o produto [...]".

Denzin e Lincoln (1994, p.2) informam que a pesquisa qualitativa é em si mesma um campo de investigação, envolve o estudo do uso e coleta de uma série de materiais empíricos como estudos de caso, introspecção, experiência de vida, entrevistas, textos, e outros.

Para as entrevistas a serem utilizadas nos estudos de múltiplos casos, planeja-se utilizar uma abordagem direta, não encoberta, onde conforme Malhotra (2004, p. 157), os objetivos do projeto ficam evidentes aos respondentes pela própria natureza da entrevista.

As entrevistas serão realizadas em profundidade onde segundo Malhotra (2004) trata-se de:

> Uma entrevista não-estruturada, direta, pessoal em que um único respondente é testado por um entrevistador altamente treinado, para descobrir motivações, crenças, atitudes e sentimentos subjacentes sobre um tópico. (MALHOTRA, 2004, P. 163).

A figura abaixo ilustra os procedimentos da pesquisa qualitativa conforme Malhotra (2004) com destaque específico para os procedimentos adotados neste trabalho.

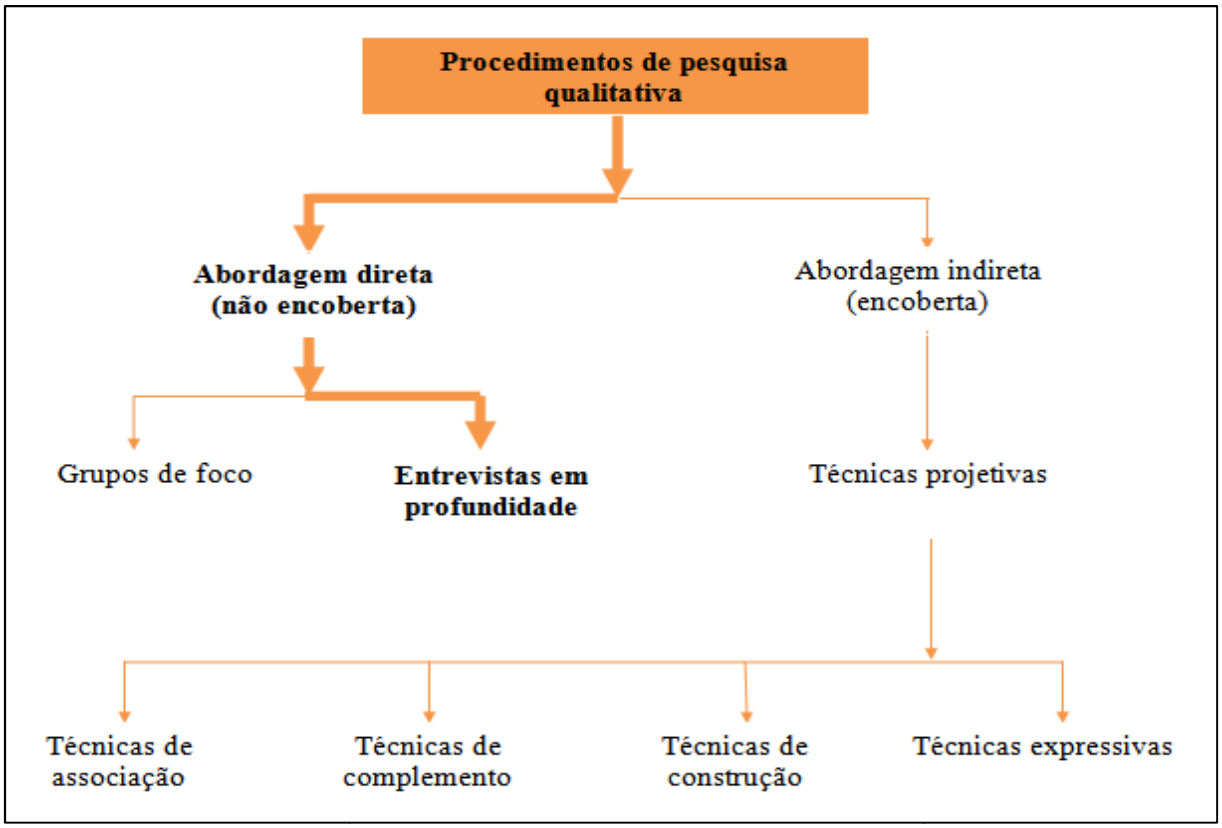

FIGURA 5– Procedimentos de pesquisa qualitativa
Fonte: MALHOTRA, 2004, p. 156.

3.1 A Pesquisa

O foco desse projeto foi determinar o comportamento do nível de maturidade em GSI nas organizações sujeitas ou não à regulação.

O referencial teórico acusou algumas lacunas a serem preenchidas, como a dificuldade em encontrar ferramentas consolidadas, o pouco referencial prático para o mercado brasileiro, a necessidade de adoção de práticas de segurança e de conformidade, dentre outros, que permitiram julgar que a metodologia de caráter qualitativo, a pesquisa exploratória, e os estudos de múltiplos casos, foram suficientes para se atingir os objetivos estabelecidos.

Segundo Malhotra (2004, p. 156) há várias razões para se utilizar uma pesquisa qualitativa, pois nem sempre é possível utilizar métodos estruturais ou até mesmo

convenientes, além disto, as pessoas podem não querer responder as perguntas, detalhe que pode ter muita influencia neste trabalho a partir do momento que assuntos de segurança muitas vezes causam constrangimentos aos respondentes. Finaliza o argumento informando que os entrevistados também podem ocultar respostas verdadeiras na tentativa de evitar que haja invasão de sua privacidade.

Para Yin (2009, p.8) o estudo de múltiplos casos ganha campo quando as questões são focadas no "como" e "por que" tal fenômeno vem acontecendo ou não, sendo focada em assuntos contemporâneos, portanto, utiliza-se o método de estudos de múltiplos casos com investigação através de análise de conteúdo para estabelecer um panorama real das organizações brasileiras que aderiram às práticas de governança corporativa. Esse panorama é visto sob a ótica crítica da GSI, portanto segue os conceitos relativos à consolidação desta.

White e Slam (2008, p. 65) informam que em uma pesquisa qualitativa um número reduzido de questões pode ser muito eficaz para a entrevista estruturada, este argumento se encaixa nos critérios utilizados para a montagem das questões utilizadas pelo ITGI (2006) para entrevistar gestores da área de segurança e executivos que são *stakeholders* com pouco tempo disponível e muita responsabilidade corporativa.

Assuntos relativos à segurança da informação são demasiadamente delicados por envolverem o tratamento dos riscos que de certa forma expõe a organização ou a sua imagem a julgamentos relativos aos cuidados com ativos próprios e de terceiros.

Conforme Vergara (2005) as etapas seguintes constituem a metodologia onde inicialmente parte-se das referências teóricas para embasamento dos procedimentos de pesquisa trazendo a reflexão conceitos como alinhamento estratégico, governança em TI, governança corporativa e Governança em Segurança da Segurança da Informação. A meta neste momento é elencar os conceitos, teorias, práticas e conformidades, além do levantamento de oportunidades servindo como guia teórico na chegada aos objetivos.

As práticas do COBIT, da ISO 17799, e do CGTF (2006), adotadas pelo ITGI (2006) para a base teórica e para investigação do comportamento dos níveis de maturidade em GSI, serviram de apoio para a formulação das perguntas de pesquisa de campo detalhadas nos APÊNDICES A e B.

Para estabelecer-se a ligação entre a transparência exigida pela governança corporativa, o alinhamento estratégico de TI, a proteção dos acervos informacionais, e finalmente, a conformidade com a regulação, assim estabelecendo o vínculo necessário que sustenta a GSI, utilizou-se de informações existentes nos ANEXOS A, B, C, e APÊNDICES A e B para o correto relacionamento entre os construtos citados.

Através dos dados relacionados nos ANEXOS B e C, entre os requisitos de segurança existentes na ISO/IEC 17799 com os requisitos de negócio do COBIT que são atendidos pela respectiva ISO, juntamente com as questões de pesquisa baseadas em todo o referencial teórico, se obteve o arcabouço necessário para a verificação do comportamento do nível de maturidade em GSI.

Na mesma linha de raciocínio, onde são cruzadas as informações de cada *framework* com o modelo de maturidade do ITGI (2006), as questões de pesquisa também refletiram os *baselines* de Pironti (2007) e foram adaptadas e enquadradas em domínios para facilitar a análise do comportamento de cada nível de maturidade conforme apresentado no QUADRO 3.

Foi utilizado como critério para enquadramento o *ISG Framework* do CGTF (2006) que embora tenha caráter de pesquisa quantitativa respalda a classificação das questões adotadas neste trabalho por utilizar-se das mesmas *baselines* de Pironti (2007) e que envolvem pessoas, processos, procedimentos, tecnologia, e conformidade.

Adotaram-se domínios, ou assuntos, que são os resultados esperados de uma efetiva GSI conforme ISACA (2008, p. 78) e ITGI (2006, p. 29) e que foram avaliados em cada nível de maturidade facilitando a análise interpretativa.

Em virtude desta pesquisa estar classificada como um assunto estratégico abordando a relação entre segurança da informação, conformidade e alinhamento estratégico, a descrição adotada para os domínios seguiu o modelo do ISACA (2008, p.78) devido à descrição utilizada pelo ITGI (2006) sobre os mesmos ser mais técnica em alguns desses.

A conformidade, foco do ISACA (2008), foi um dos valiosos componentes para a eficácia deste estudo indicando relacionamentos entre os modelos uma vez que os requisitos para o alinhamento estratégico de segurança da informação são muito amplos.

De qualquer modo a análise dos dados em cada nível de maturidade seguiu o consenso entre os dois modelos por não haver diferenças quanto à classificação dos mesmos, mas sim para as descrições adotadas.

Os respectivos domínios também são encontrados nas normas ISO 27001 e ISO 27002 além de estarem em conformidade com Allen e Carnegie (2007), são eles:

a) Alinhamento estratégico – Alinhamento da segurança da informação com estratégia de negócio para suportar os objetivos organizacionais. Para alcançar o alinhamento, os seguintes itens deverão estar em conformidade:

   – requisitos de segurança dirigidos por requisitos da organização completamente desenvolvidos para orientar no que deve ser feito e uma medida de quando ele foi alcançado,

   – soluções de segurança aptas para os processos organizacionais que levem em conta a cultura, estilo de governança, tecnologia e a estrutura da organização,

   – investimentos na segurança da informação alinhados com a estratégia organizacional com ameaças bem definidas e um perfil de vulnerabilidades e riscos;

b) Gestão de riscos – Gerenciar e executar medidas necessárias para mitigar riscos e reduzir potenciais impactos nos recursos de informação para um nível aceitável. Para alcançar o gerenciamento de risco considerar:

   – entendimento coletivo das ameaças, perfis de vulnerabilidades e riscos organizacionais,

   – entendimento da exposição aos riscos e potenciais consequências do compromisso incluindo regulação, aspectos legais, e impactos na imagem,

   – consciência da priorização do gerenciamento de riscos baseada nas consequências,

   – mitigação de riscos suficiente para atingir consequências aceitáveis de riscos residuais,

- aceitação/Consideração baseado no entendimento das consequências potenciais de riscos residuais;

c) Entrega de Valor – Aperfeiçoar investimentos em segurança no suporte aos objetivos de negócios. Para alcançar a entrega de valor, considerar o seguinte:

- um conjunto padrão de políticas e práticas, isto é, requisitos dos *baselines* de segurança seguindo adequadas e suficientes práticas proporcionais aos riscos,

- corretamente priorizar e distribuir esforço para áreas com maiores impactos e benefícios aos negócios,

- soluções e produtos baseados em padrões,

- soluções completas cobrindo a organização, os processos de negócios bem como, a tecnologia, baseadas no negócio fim da organização,

- uma contínua melhoria cultural baseada no entendimento que segurança é um processo e não um evento;

d) Gestão de Recursos – Utilizar o conhecimento e a infraestrutura de segurança da informação de forma eficiente e eficaz. Para alcançar a Gestão de Recursos, considerar:

- assegurar que o conhecimento seja obtido e disponibilizado,

- documentar processos e práticas de segurança,

- desenvolver a arquitetura de segurança para definir e utilizar os recursos de infraestrutura eficientemente;

e) Medição de Desempenho – Medir, monitorar e relatar processos de segurança da informação para assegurar que os objetivos sejam alcançados. Para atingir a Medição de Desempenho, verificar que:

- um definido, acordado e significativo conjunto de métricas que sejam apropriadamente alinhadas com os objetivos estratégicos,

- um processo de medição que ajude a identificar deficiências e proporcionem retorno sobre os processos realizados na resolução de problemas,

- garantias fornecidas por meio de avaliações independentes e auditorias externas.

O enquadramento das questões de pesquisa aos cinco domínios acima é apresentado no quadro abaixo:

QUADRO 2
Enquadramento de perguntas nos domínios/resultados de efetiva GSI
(Continua – Parte I)

Domínio	Referência	Perguntas do Questionário
Alinhamento Estratégico	Questionário Gestão	P1 - Como o conselho é informado das questões de segurança da informação? Quando foram passadas ao conselho as últimas instruções sobre riscos e melhoria no estado de segurança? P6- O CEO pediu alguma avaliação de segurança da informação? Foram analisados os resultados dessa avaliação e foram comunicados ao conselho de administração? P10 - Existe um processo contínuo para garantir o alinhamento das informações de segurança com os objetivos de negócio? Como funciona?
	Questionário Executivo	P1- O valor e a importância da segurança da informação são assimilados pela alta gestão? P2 - A organização tem uma estratégia de segurança? Se assim for, é alinhada com a estratégia global de negócios? Esta também é alinhada à Tecnologia da Informação? P5- A segurança da informação aparece como um item de pauta da diretoria? Há um cronograma para relatar o status do programa de segurança da informação para o conselho?

QUADRO 2
Enquadramento de perguntas nos domínios/resultados de efetiva GSI
(Continuação – Parte II)

Domínio	Referência	Perguntas do Questionário
Gestão de riscos	Questionário Gestão	P4 - Quando foi a última avaliação dos riscos feita baseada na criticidade e sensibilidade dos ativos de informações de segurança? Quando é a próxima avaliação de risco prevista? P5 - A avaliação de risco considerou que a entidade possa continuar a funcionar se não estiver disponível a informação crítica, comprometida ou perdida? Foram consideradas as consequências de um incidente de segurança em termos de receitas, perda clientes e a confiança dos investidores? Foram determinadas quais as consequências haveria se a infra-estrutura torna-se inoperante? P8- A avaliação de risco considera que os ativos de informação estão sujeitos a leis e regulamentos? Isto resulta em procedimentos adequados para assegurar cumprimento dessas leis e regulamentos? P9 - A informação sobre a avaliação de risco é um item na agenda regular de TI? Como isto acontece?
	Questionário Executivo	P3- O conselho compreende as potenciais responsabilidades da organização no caso de descumprimento da regulação? Entende também a potencial responsabilidade quando a informação sigilosa é comprometida?
Entrega de Valor	Questionário Gestão	P2- As funções de segurança e responsabilidades são claramente definidas e comunicadas? Como? P11 - Como são feitos os programas de conscientização para garantir que o pessoal está consciente das suas responsabilidades de segurança e das expectativas da gestão? P14 - A organização implementa práticas de segurança de mercado para implementar projetos de tecnologia desde o início dos mesmos? Quais são as práticas adotadas? Estas práticas também são adotadas durante a aquisição ou desenvolvimento e manutenção de software? P14 - A organização implementa práticas de segurança de mercado para implementar projetos de tecnologia desde o início dos

QUADRO 2
Enquadramento de perguntas nos domínios/resultados de efetiva GSI
(Continuação – Parte III)

Domínio	Referência	Perguntas do Questionário
Entrega de Valor	Questionário Gestão	mesmos? Quais são as práticas adotadas? Estas práticas também são adotadas durante a aquisição ou desenvolvimento e manutenção de software?
	Questionário Executivo	P4 - Se houve algum incidente grave de segurança, foi determinado o custo do incidente para a organização? P9 - Existe um CISO (*Chief Information Security Officer*) ou funcionário especialmente encarregado da gestão de segurança da informação na organização? P10 - Há uma formação adequada e programas de conscientização para garantir que o pessoal está consciente das suas responsabilidades de segurança?
Gestão de Recursos	Questionário Gestão	P3- A organização já teve sua segurança de rede controlada por terceiros? P12 - Existe um processo de classificação de ativos de informação para assegurar que ativos críticos estão adequadamente protegidos? P13 - A organização implementa controles de segurança física e lógica? P15 - A organização implementa requisitos de segurança no gerenciamento de operações e comunicações, tais como gestão de mudanças, segregação de funções, segregação de ambientes de produção/homologação/desenvolvimento? Implementa ainda recursos de proteção de infra-estrutura para dispositivos portáteis, computadores e equipamentos de redes e teleprocessamento?
	Questionário Executivo	P6 - Existe uma política de segurança da informação aprovada? É constantemente revisada?
Medição de Desempenho	Questionário Gestão	P7 - Existe um processo eficaz e testado para tratar da segurança da informação em incidentes / emergências?

QUADRO 2
Enquadramento de perguntas nos domínios/resultados de efetiva GSI
(Conclusão – Parte IV)

Domínio	Referência	Perguntas do Questionário
Medição de Desempenho	Questionário Gestão	P16 - Há um ISMS – *Information Security Management System Systems* (ISO/IEC 27001) implantado ou em implantação na organização?
	Questionário Executivo	P7 - Pode a organização continuar a operar se a informação crítica ficar indisponível, comprometida ou perdida? Quais seriam as consequências de um incidente de segurança em termos de receitas, perda de clientes e confiança dos investidores? P8 - A auditoria compreende claramente o seu papel na segurança da informação?

Fonte: Elaborado pelo Autor.

Na avaliação dos questionários, o comportamento do nível de maturidade foi analisado primeiramente no escopo dos domínios em cada empresa criando-se quadros contendo as respostas para as perguntas acima classificadas verificando-se o comportamento dos *baselines* existentes em cada pergunta.

Os *baselines* estão contidos nos critérios existentes em cada nível de maturidade e a análise dos comportamentos desses foi realizada comparando-se as respostas contidas nos quadros de cada domínio com os seus respectivos critérios.

Para contextualização, pode-se aferir que se não há indícios da ocorrência das *baselines* referentes à avaliação de riscos, então há fortes indicativos de que, segundo a QUADRO 3 a seguir, para o domínio de gestão de risco da referida empresa, o nível de maturidade neste seja classificado como inexistente, entretanto, uma vez que os domínios são compostos por vários outros *baselines*, os mesmos irão compor a análise de forma a consolidar a classificação em determinado nível de maturidade.

A FIG. 6 ilustra a composição da metodologia partindo-se da necessidade de avaliar o comportamento do nível de maturidade em GSI utilizando-se de conceitos de diferentes modelos discutidos no referencial teórico a exemplo dos domínios utilizados pelo ISACA (2008), dos questionários e níveis de maturidade utilizados pelo modelo de

Governança de Segurança da Informação do ITGI (2006), das *baselines* utilizadas por Pironti (2007) e pelo *ISG Framework* do CGTF (2006).

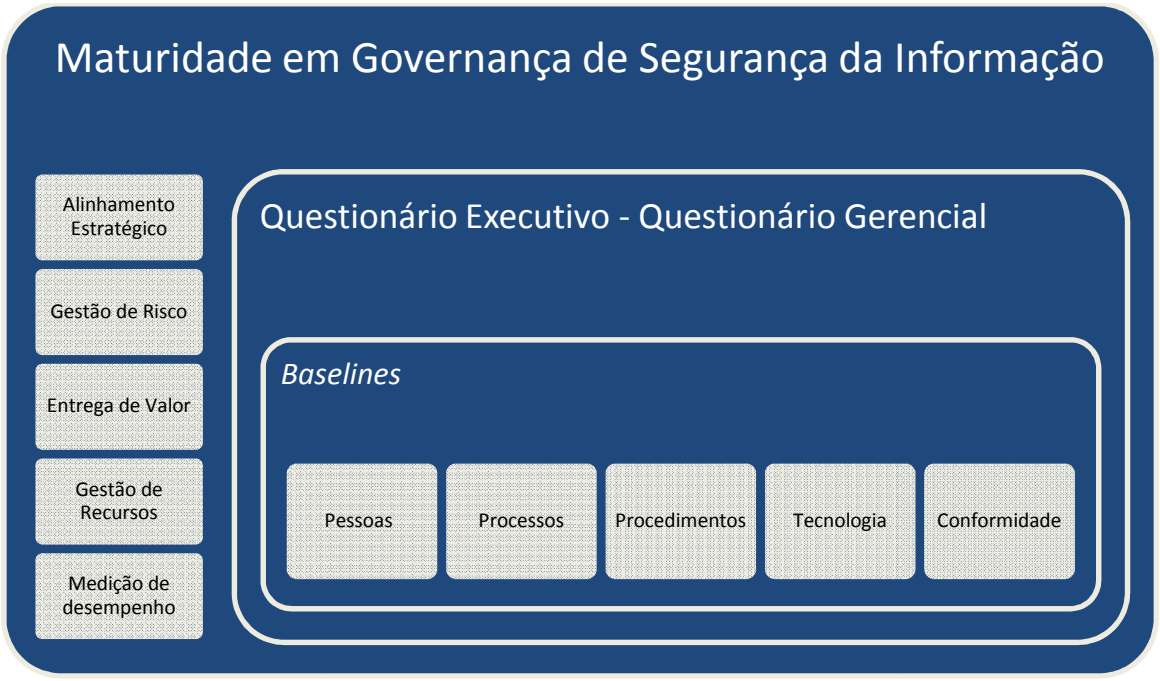

FIGURA 6 – Ilustração da metodologia
Fonte: Elaborado pelo Autor.

A maturidade em Governança de Segurança da Informação é dada, segundo o ISACA (2008) e ITGI (2006), em virtude de resultados eficazes nos domínios citados e, para cada um destes, existem conjuntos de *baselines* que se encontram intrinsecamente inseridos nas questões de pesquisa que apóiam a análise das respostas.

Em relação ao nível de maturidade propriamente dito, nota-se a existência dos assuntos abordados nos domínios e em cada questão, bem como nas *baselines* utilizadas para as mesmas na pesquisa, de forma que as respostas foram classificadas conforme apresentado nos critérios existentes em cada nível.

Não foi o propósito na análise de dados a realização categórica da classificação segundo o nível de maturidade, embora possa constar em alguns casos, mas baseado em todo o referencial teórico apontou-se o comportamento dos domínios e respectivos *baselines* perante os mesmos níveis de maturidade.

Ao final, para cada organização, foi realizada a conclusão sobre o comportamento dos cinco domínios apresentados com a finalidade de realizar o batimento entre as diversas

questões levantadas a fim de encontrar compatibilidades, controvérsias, além de outros aspectos relevantes para este estudo.

Na discussão geral, foi realizado um resumo das análises de cada organização comparando-as e classificando-as em cada nível de maturidade realizando a discussão dos domínios estudados.

No item 5 – Conclusões, os aspectos relevantes dos resultados e que envolvem a pergunta de pesquisa e os objetivos foram resumidamente esclarecidos e consolidados com seus respectivos pareceres apresentando uma contextualização do comportamento geral dos níveis de maturidade da Governança de Segurança da Informação.

QUADRO 3
Níveis do modelo de maturidade em GSI

(Continua – Parte I)

Nível	**Descrição / Critérios**
0 – Inexistente	• A avaliação de riscos para os processos e decisões de negócios não ocorre. A organização não considera no negócio impacto associados a vulnerabilidades de segurança e incertezas do projeto de desenvolvimento. A gestão de riscos não tem sido identificada como relevante para a aquisição de soluções de TI e fornecimento de serviços de TI. • A organização não reconhece a necessidade de segurança da informação. Responsabilidades e obrigações não são atribuídas para garantir a segurança. Medidas de apoio à gestão da segurança da informação não são implantadas. Não há relatórios de segurança da informação e não há respostas aos processos de falhas de segurança à informação. Há uma completa falta de um reconhecível processo de administração do sistema de segurança. • Não existe a compreensão dos riscos, vulnerabilidades e ameaças das operações de TI ou o impacto da perda dos serviços de TI para o negócio. O serviço de continuidade não é considerado como necessário de atenção da administração.
1 - Inicial / *Ad hoc*	• A organização considera os riscos de uma forma ad hoc, sem seguir processos definidos ou políticas. Avaliações informais do risco do projeto têm lugar determinado por cada projeto. • A organização reconhece a necessidade de segurança da informação, mas a segurança é um conhecimento individual. A segurança da informação é abordada em uma base reativa e não é mensurada. Violações de segurança da informação invocam

QUADRO 3
Níveis do modelo de maturidade em GSI
(Continuação – Parte II)

Nível	Descrição / Critérios
1 - Inicial / *Ad hoc*	respostas pontuais, se detectadas, porque as responsabilidades não são claras. As respostas às violações de segurança da informação são imprevisíveis.
2 – Repetível (intuitivo)	• Existe um entendimento emergente que riscos de TI são importantes e precisam ser considerados. Uma abordagem de avaliação de risco existe, mas o processo ainda está imaturo e em desenvolvimento. • Responsabilidades são atribuídas a um coordenador de segurança sem autoridade de gestão. A conscientização da segurança é fragmentada e limitada. As informações de Segurança da Informação são geradas, mas não analisadas. A segurança tende a ser reativa a incidente de segurança da informação com adoção de ofertas de terceiros sem abordar as necessidades específicas da organização. As políticas de segurança estão sendo desenvolvidas, mas as habilidades e ferramentas inadequadas ainda estão sendo utilizadas. Informações relativas a segurança é incompleta, enganosa ou não pertinentes. • Responsabilidades para serviços contínuos são atribuídas. As abordagens para serviço contínuo são fragmentadas. O Relatório sobre a disponibilidade do sistema é incompleto e não leva em conta o impacto no negócio.
3 - Processo Definido	• Uma política de gestão de risco organizacional define quando e como é a conduta para avaliações de riscos. A avaliação de riscos segue um processo definido que é documentado e disponível para todos os funcionários através de treinamento. • A sensibilização de segurança existe e é promovida pela gerência. Instruções de sensibilização de segurança têm sido padronizadas e formalizadas. Informações e procedimentos de segurança são definidos e se encaixam em uma estrutura para políticas de segurança. Responsabilidades de segurança da informação são atribuídas, mas não são aplicadas de forma coerente. Um plano de segurança da informação existe com a condução de análise de risco e soluções de segurança. Informações relativas à segurança são com foco em TI, em vez de serem focadas em negócios. O Teste de intrusão é realizado *ad hoc*.

QUADRO 3
Níveis do modelo de maturidade em GSI
(Continuação – Parte III)

Nível	Descrição / Critérios
3 - Processo Definido	• A gestão comunica constantemente a necessidade de serviço contínuo. Componentes de alta disponibilidade e redundância do sistema estão para serem aplicadas de forma fragmentada. Um inventário dos sistemas e componentes críticos são rigorosamente mantidos.
4 - Gerenciado e Mensurável	• A avaliação de risco é um procedimento padrão e as exceções seguem os procedimentos que são observados pela gestão de TI. É provável que a gestão de riscos de TI seja uma função de gestão definida com nível sênior de responsabilidade. O órgão de direção e gestão de TI tem determinados os níveis de risco que a organização irá tolerar e tem como padrão medidas de risco / razão do retorno. • As responsabilidades de segurança da informação são claramente atribuídas e a gestão é aplicada. Informações sobre os riscos de segurança e análise de impacto são consistentemente realizados. Políticas e práticas de segurança são cumpridas, com específicas *Baselines* de segurança. Instruções de consciência de segurança são obrigatórias. Identificação, autenticação e autorização são padronizadas. É certificado que a segurança está estabelecida entre os colaboradores. Testes de intrusão são padronizados e os processos formalizados conduzindo a melhorias. Análises de custo-benefício apóiam a implantação de medidas de segurança e são cada vez mais utilizadas. Processos de segurança da informação são coordenados com o objetivo global em função da segurança da organização. Informações relativas à segurança estão ligadas a objetivos do negócio. • Responsabilidades e normas de serviço contínuo são aplicadas. Práticas de redundância, incluindo o uso de componentes de alta disponibilidade, são consistentemente implantados.
5 – Otimizado	• A gestão de risco foi desenvolvida de forma estruturada para o estagio atual e o processo organizacional é aplicado, seguido regularmente, e bem gerido.

QUADRO 3
Níveis do modelo de maturidade em GSI
(Conclusão – Parte IV)

Nível	Descrição / Critérios
5 – Otimizado	• A segurança da informação é uma responsabilidade conjunta de negócios e gestão de TI e é integrada com os objetivos de negócio da empresa. Requisitos de segurança da informação estão claramente definidos, otimizados e incluídos num plano de segurança existente. Funções de segurança são integradas com aplicações na fase de projeto e os usuários finais estão cada vez mais responsáveis para gerenciar a segurança. Informações de relatórios de segurança fornecem cedo avisos de mudança e de risco emergentes através de monitoramento ativo automatizado com abordagens para sistemas críticos. Incidentes são prontamente corrigidos com procedimentos formalizados e a resposta aos mesmos apoiados por ferramentas automatizadas. Existem avaliações periódicas de segurança para avaliar a eficácia da execução do plano de segurança. Informações sobre novas ameaças e vulnerabilidades são sistematicamente coletados e analisados e os controles adequados prontamente comunicados e implantados. Testes de intrusão, de causa raiz, análise de incidentes de segurança e identificação pró-ativa de riscos são as bases para melhorias contínuas. Processos e tecnologias de segurança são organizacionalmente integrados. • Os planos de serviço contínuo e de planos de continuidade de negócios são integrados, alinhados e mantidos rotineiramente. A compra de serviços é continuamente assegurada a partir de avaliação de fornecedores.

Fonte: ITGI, 2006, p. 36, *tradução do autor*.

Nota-se no QUADRO 3 uma incidência elevada de assuntos relacionados à gestão de riscos e para o entendimento das atitudes dos gestores e executivos das empresas brasileiras frente às práticas padrão de mercado que sustentam os princípios de governança, propositalmente ilustra-se, conforme Westerman e Hunter (2008, p. 44), a gestão de riscos existentes nas mesmas organizações para melhor contextualização dos incidentes apresentados anteriormente.

Visando aumentar a compreensão sobre as teorias que permeiam os riscos corporativos, bem como a evidenciar as práticas de Governança em Segurança da Informação e os mecanismos de governança de TI presentes na literatura, procede-se na análise das respostas a identificação dos controles de segurança para mitigação dos riscos corporativos.

Para Yin (2009, p.14) determinar as questões mais significantes para um tópico da entrevista requer muita preparação, portanto, consideram-se aqui algumas perguntas já existentes, homologadas pelo ITGI (2006, p. 34-35) e adaptadas pelo autor, relacionadas nos APÊNDICES A e B, juntamente com modelos citados e as respostas obtidas como base para a análise de conteúdo realizada.

A transparência, juntamente com as ações sociais, conforme Dias, Pardini e Aguiar (2005), alavancam as iniciativas de governança o que pode ser verificado pelo perfil das organizações integrantes da amostra.

Lins e Wajnberg (2007) também respaldam a argumentação de Dias, Pardini e Aguiar (2005) dando um panorama do segmento financeiro onde informam que a transparência perante seus acionistas e a responsabilidade social deste segmento são fortes motivadores de governança justamente por serem os mesmos grandes estimuladores de desenvolvimento junto a seus clientes.

Foram realizadas 6 entrevistas de gestão e 6 entrevistas de executivos das organizações justamente pelo fato do assunto GSI ser de responsabilidade da alta direção e, que por ser parte integrante da estratégia de segurança, necessariamente foi preciso ter a visão da gestão de segurança para a devida ilustração do cenário corporativo.

Todas as entrevistas foram transcritas e analisadas buscando também responder aos objetivos propostos.

Finalmente através da análise de conteúdo adicionalmente ao ferramental acima citado conclui-se com os estudos de múltiplos casos objetivando dar um cunho além de teórico, mas também mercadológico para este estudo.

3.2 Universo e amostra

Nessa parte foi realizado o levantamento dos dados e a seleção das organizações que participaram da pesquisa referendada por Freitas e Moscarola (2002), que afirmam:

> A atividade de pesquisa hoje deixa de pertencer somente aos centros acadêmicos e instituições especializadas para se incorporar no dia-a-dia das empresas e demais organizações. Frente a um ambiente de negócios amplo e turbulento, a pesquisa passa a representar um recurso de grande poder para se coletar, analisar e extrair informações valiosas de dados, tanto externos como internos às organizações. (FREITAS; MOSCAROLA, 2002, p.2).

Esta afirmação é reforçada por Guerra (2006, p. 37) quando alega que a pesquisa qualitativa tem simultaneamente um papel teórico e estratégico, portanto, seguindo o dia-a-dia das empresas, para a seleção da amostra foi adotado como critério principal o estudo da Pricewaterhousecoopers (2010) que aponta o *Compliance* (conformidade) como maior motivador de investimentos em segurança da informação em suas organizações.

Portanto, justamente pela importância da conformidade e da segurança da informação para a GSI, merece relatar que a pesquisa foi focada nas organizações pertencentes aos segmentos sob regulação, mas comparativamente abordou outras organizações que não estão sob regulação. Cita-se também o acesso do pesquisador aos entrevistados das empresas adicionalmente facilitado por vários anos de atuação no ramo de segurança com amplo conhecimento do mercado.

Vergara (2000) também referenda o critério adotado quando informa que em uma amostra não interessa o número de populações da amostra, mas sim as características comuns entre essas, ou seja, além de terem maior investimento, o que pode demonstrar uma crescente preocupação na mitigação dos riscos, também se preocupam na maior aderência à governança de TI e governança corporativa a exemplo de estatais, empresas de capital misto e de organizações financeiras.

Utilizando-se as argumentações anteriores, selecionaram-se três empresas de grande porte e sujeitas à regulação para comporem a amostragem primária dos seguintes setores/segmentos: Financeiro, Telecomunicações e Energético. Adicionalmente, a titulo comparativo e para dar maior diversidade e visibilidade mercadológica ao assunto, foram

selecionadas mais três empresas que não estão diretamente sujeitas à regulação, sendo pertencentes aos seguintes segmentos: Industrial, Tecnologia da Informação e Regulação.

Corroborando a pesquisa anterior, conforme a Pricewaterhousecoopers (2009a), 94% dos executivos brasileiros informam que a clareza e a estabilidade das regras fiscais são os principais aspectos da regulação para as decisões de investimentos.

O Gartner (2010) coloca esses mesmos segmentos da amostragem como os que mais investem em TI, entretanto, a segurança aparece em sétimo lugar no ranking de priorizações de investimento. Isto respalda a argumentação de que a estruturação da área de segurança da informação não deve estar subordinada a estrutura de TI para não sofrer restrições da mesma, mas sim diretamente ao alto escalão das organizações.

Outra pesquisa global também realizada pela Pricewaterhousecoopers (2009b) já apontava que os segmentos de Telecomunicações e Financeiro foram dos que mais relataram casos de fraudes diversas, respectivamente, em primeiro lugar e terceiro lugar no ranking apontado pela pesquisa.

Pelo caráter exploratório da pesquisa também se procurou selecionar organizações de diferentes localidades do Brasil, mas a maioria da amostra obtida é predominante de Minas Gerais. O ponto atenuador e que contribui na diversidade cultural pretendida é o fato de que a maior parte das empresas da amostra é classificada pelo BNDES como grandes empresas, de capital aberto, sujeitas a um controle acionário diversificado, além de possuírem outras características semelhantes como a governança corporativa e a prestação de contas perante órgãos fiscalizadores. Ao final da seleção a amostra primária ficou da seguinte forma:

- São Paulo/SP – Segmento de Telecomunicações;
- Belo Horizonte/MG – Segmento Financeiro;
- Belo Horizonte/MG – Segmento Energético.

Excepcionalmente, para efeito ilustrativo de comparação e de maior diversidade cultural foram adicionados os seguintes segmentos:

- Belo Horizonte/MG – Segmento de Tecnologia da Informação, que indiretamente é obrigado a manter conformidade em seus sistemas por atender empresas de segmento sob regulação;

- Belo Horizonte/MG – Segmento de Regulação, instituição pública reguladora, com características peculiares em relação a todas as outras, pois é agente fiscalizador de conformidades em determinado segmento;

- Belo Horizonte/MG – Segmento Industrial, que não está sujeita a qualquer regulação.

QUADRO 4
Perfil dos entrevistados

Empresa	**Funcionário**	**Referência**	**Cargo/Função**	**Data da Entrevista**
A	1	EAG	Gestor de Segurança	01/10/2010
A	2	EAE	Diretor Executivo	06/10/2010
B	1	EBG	Gestor de Segurança	24/09/2010
B	2	EBE	CISO	24/09/2010
C	1	ECG	CISO	01/09/2010
C	2	ECE	Diretor de Segurança	01/09/2010
D	1	EDG	Gestor de Segurança	17/09/2010
D	2	EDE	Superintendente de TI	17/09/2010
E	1	EEG	Gestor de Segurança	06/08/2010
F	1	EFG	Gestor de Segurança	31/08/2010
F	2	EFE	Diretor de TI	31/08/2010

Fonte: Dados da pesquisa.

Em alguns os casos houve apenas um respondente, entretanto, houve autorização do executivo para que o mesmo pudesse responder os dois questionários principalmente por dois motivos encontrados: 1) A empresa não tem um conselho diretor ou o executivo desconhece qualquer assunto relativo à segurança da informação; 2) O executivo entende que não deve participar das respostas delegando ao responsável imediato pelo assunto.

Embora o porte da empresa não seja critério para a seleção da amostra, existe o entendimento que maiores requisitos de segurança da informação e *compliance* estão ligadas ao segmento aos quais as organizações pertencem. Portanto, apenas adota-se esse critério para a devida classificação quanto ao porte das organizações envolvidas na pesquisa o critério utilizado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES), que leva em consideração a receita operacional bruta (ROB) conforme ilustrado no quadro abaixo:

QUADRO 5
Classificação de porte empresarial

Porte da Empresa	**Receita Operacional Bruta (ROB)**
Microempresa	inferior ou igual a R$ 2,4 milhões
Pequena Empresa	superior a R$ 2,4 milhões e inferior ou igual a R$ 16 milhões
Média Empresa	superior a R$ 16 milhões e inferior ou igual a R$ 90 milhões
Empresa Média-Grande	superior a R$ 90 milhões e inferior ou igual a R$ 300 milhões
Grande Empresa	superior a R$ 300 milhões.

Fonte: BNDES (2010).

3.3 Empresas pesquisadas

3.3.1 Empresa A – Segmento de tecnologia da informação

Associação privada, de capital fechado, com controle nacional, do segmento de tecnologia da informação, classificada como Pequena Empresa pelo BNDES.

Embora a empresa A não esteja diretamente sujeita à regulamentação e fiscalização por algum órgão regulador, vale destacar que a mesma é a principal e exclusiva fornecedora de TI para um grupo de cooperativas, classificada como Grande Porte pelo BNDES, que estão sujeitas a regulação do Banco Central do Brasil, portanto, mesmo que indiretamente a empresa A sofre influências do órgão regulador em suas soluções e serviços de TI.

A empresa A, pelo fato de ser fornecedor de TI, tem estruturação de assuntos de segurança focados nas práticas de TIC além de estar em constante investimento em projetos que aprimorem e inovem seus produtos e serviços.

3.3.2 Empresa B – Segmento financeiro

Empresa privada, de capital aberto, com controle acionário nacional, do segmento financeiro, classificada como Grande Empresa pelo BNDES.

Tem um forte alinhamento de sua estrutura de TI ao negócio, muitas vezes, sugerindo melhorias ao mesmo. Adota práticas de mercado mais voltadas para a TI, mas que repercutem na estratégia de segurança.

Sujeita a regulação do Banco Central do Brasil (BACEN) responsável por toda a regulamentação e fiscalização do segmento.

A organização tem preocupação crescente e vigilante sobre seus principais ativos como a informação, a imagem, e a custódia das finanças de seus clientes. Com forte atuação em segurança da informação e *compliance*, também é referenciada no ramo por sua desenvoltura, contribuição e participação em comitês e demais entidades ligadas à segurança.

3.3.3 Empresa C – Segmento de telecomunicações

Empresa privada, de capital aberto, com controle acionário estrangeiro, do segmento de telecomunicações classificada como Grande Empresa pelo BNDES.

Sujeita a regulação da Agência Nacional de Telecomunicações (ANATEL) responsável por toda a regulamentação e fiscalização do segmento.

Assim como organizações de outros segmentos que investem em segurança da informação há crescente preocupação com a proteção dos acervos informacionais principalmente pelo fato da empresa oferecer aos seus clientes uma grande variedade de serviços disponíveis pela internet bem como em manter a conformidade com o órgão regulador.

A empresa C é uma das maiores empresas de telecomunicações do Brasil com forte atuação em todo o mercado nacional.

3.3.4 Empresa D – Segmento energético

Empresa pública, de capital aberto, multinacional, com controle acionário nacional, classificada como Grande Empresa pelo BNDES.

Sujeita a regulação de órgão do governo federal responsável por toda a regulamentação e fiscalização do segmento.

A empresa tem se destacado em seu segmento sendo referencia nacional na prestação de serviços bem como expandindo suas operações para fora do território nacional.

A empresa D é uma das maiores empresas em seu segmento com forte atuação em alguns estados do território nacional e internacional.

3.3.5 Empresa E – Segmento de regulação

Empresa pública, de capital fechado, nacional, com controle do governo do estado de Minas Gerais, por ser órgão regulador não foi classificada conforme tabela de porte empresarial do BNDES.

O órgão regulador tem sua importância destacada na normatização e fiscalização de produtos e serviços básicos à sociedade.

3.3.6 Empresa F – Segmento industrial

Empresa privada, de capital aberto, com controle acionário nacional, do segmento industrial, classificada como Grande Empresa pelo BNDES.

Não está sob regulação.

A organização vive o bom momento da construção civil diversificando seu portfólio de obras em todo o território nacional. Com boa atuação nos requisitos que envolvem a segurança da informação e *compliance*, também é referenciada no ramo por sua desenvoltura no mercado.

4 ANÁLISE DE RESULTADOS E DISCUSSÕES

Para determinar o nível de maturidade de GSI em que se encontra a organização pesquisada utilizou-se de um conjunto de perguntas a serem respondidas em dois formulários, o primeiro voltado para questões de nível executivo (EXE)[18] e o segundo voltado para questões de nível gerencial (EXG)[19]. Os questionários fornecem um roteiro cujo objetivo maior é obter dos respondentes informações sobre os construtos citados que compõe este estudo de GSI.

4.1 Empresa A – Segmento de tecnologia da informação

4.1.1 Alinhamento estratégico

QUADRO 6
Respostas a alinhamento estratégico – Empresa A – TI
(Continua – Parte I)

Referência	Respostas
EAG	R1- O conselho é informado apenas quando ocorre algum tipo de problema. Não existe área ou métodos para avaliação e melhoria contínua das questões de segurança na empresa R6 – Nunca foi realizado. Estamos iniciando um POC junto a um parceiro. R10- Não. Os projetos são executados conforme necessidade e momento da organização.

[18] EXE – Leia-se E=Empresa, X=[Identificador da Empresa], E=Nível Executivo
[19] EXG – Leia-se E=Empresa, X=[Identificador da Empresa],G=Nível Gestor

QUADRO 6
Respostas a alinhamento estratégico – Empresa A – TI
(Conclusão – Parte II)

Referência	Respostas
EAE	R1 - Sim. A alta gestão acompanha o mercado de instituições financeiras e está ciente dos riscos financeiros e de imagem existentes nas transações eletrônicas. R2 – Sim. A estratégia de segurança está alinhada a estratégia de negócios e o alinhamento com tecnologia se concretizou ao contratarmos para solução de segurança para auxiliar na construção de nossa nova solução de *frontend*. R5 – Não existe o item segurança na pauta de forma regular. O assunto é discutido com frequência, mas não é item fixo da pauta da diretoria.

Fonte: Dados da pesquisa.

Após análise dos dados da entrevista realizada na empresa A, verifica-se inicialmente a pouca participação de executivos nos assuntos estratégicos de segurança da informação, fato verificado em acordo com as respostas de EAG. Mesmo informando o respondente EAE que a alta gestão assimila o valor e a importância da segurança da informação, verifica-se já no início da entrevista que a referida segurança é voltada para segurança em tecnologia da informação ilustrando uma evidente distância entre a percepção do alinhamento da estratégia global de negócio com alinhamento estratégico de segurança que em determinados momentos chega a ser confundido com alinhamento de TI ao negócio.

A área de segurança da informação não existe no organograma da empresa A e embora não exista um setor específico para tratar do assunto ou um CISO ou profissional de SI nomeado, o tratamento das *baselines* de segurança existem discretamente nos assuntos de TI.

O fato de o executivo EAE responder que a segurança da informação não aparece como um item regular na pauta da diretoria, mas que é frequentemente abordada nas reuniões ilustra um pouco da tentativa de alinhamento, entretanto, pela resposta da gestão verifica-se que o alinhamento entre segurança e negócio é pontual e de acordo com a demanda dos projetos dando o parecer de que realmente não é tratada como um processo contínuo com abordagem *top-down* de implementação.

Vê-se que diante deste cenário, que um dos pontos mais positivos do alinhamento estratégico justamente a utilização deste como diferencial competitivo ainda tem longo caminho a percorrer na empresa A.

Tomando-se por base que o alinhamento existente entre a estratégia de segurança com a estratégia global de negócios na empresa A existe apenas em poucos *baselines* que são inclusive existentes em segurança de TI e que mesmo assim há indícios de um distanciamento entre as estratégias pode-se aferir que a empresa A está em um nível inicial no domínio de alinhamento estratégico.

4.1.2 Gestão de riscos

QUADRO 7
Respostas a gestão de riscos – Empresa A – TI

Referência	Respostas
EAG	R4 – Nunca foi realizada e não existe programação em andamento. R5 – Não. Não temos metodologia para avaliação de boas práticas e riscos. R8 – Não temos processo efetivo implantado para este fim. R9 – Não existem avaliações de risco programadas.
EAE	R3 – Sim. A alta gestão tem conhecimento de todos os normativos ligados ao sigilo de informações e conhece as responsabilidades no que tange a proteção dos dados dos correntistas.

Fonte: Dados da pesquisa

O fato da empresa A não ter um ERM, ou mesmo um modelo de gestão de riscos, insere-a em uma situação de vulnerabilidade a riscos corporativos que podem ir desde violação de requisitos legais e de conformidade até de riscos que comprometam a continuidade dos negócios impactando em perdas financeiras e de credibilidade repercutindo negativamente em sua imagem e de seus clientes.

A inexistência de avaliações de riscos periódicas, nem mesmo uma única realizada até a data da entrevista, dá a entender que todo o tratamento dos riscos é realizado de forma *ad-hoc* com forte apoio da auditoria e controles internos podendo estar sobrecarregando os mesmos e até estar sendo realizado de forma pontualmente reativo.

Portanto, na governança da gestão de risco a empresa necessita tomar atitudes emergenciais para a instauração de um modelo de gestão de riscos para mitigar seus riscos principalmente por ser este um requisito de conformidade para o segmento financeiro ao qual a empresa A está indiretamente ligada.

Considera-se que a empresa A ainda está na fase de transição de um nível onde a gestão de riscos é inexistente para um nível onde a mesma passará a ser inicial / ad hoc isto porque não há sequer a avaliação de riscos, mas que de certa forma há iniciativas pontuais vinculadas a projetos.

4.1.3 Entrega de valor

QUADRO 8
Respostas a entrega de valor – Empresa A – TI
(Continua – Parte I)

Referência	Respostas
EAG	R2 – Não existe política estabelecida. Estamos em processo de iniciar a estruturação do processo. R11- Iniciamos um processo de geração de termos de responsabilidade e campanha de conscientização referente à utilização dos recursos de TI da empresa, entretanto, ainda é uma ação sem resultados efetivos. R14 – Não temos práticas definidas. Realizamos recentemente um curso que treinou 15 colaboradores em "Segurança no desenvolvimento de aplicações críticas". Esperamos que a partir de então as aplicações desenvolvidas internamente começam a possuir um nível mínimo de quesitos de segurança.

QUADRO 8
Respostas a entrega de valor – Empresa A – TI
(Conclusão – Parte II)

Referência	Respostas
EAE	R4 – A Cooperativa nunca sofreu qualquer tipo de fraude eletrônica. As fraudes pontuais que aconteceram estão ligadas a clonagem e roubo de cartões de débito. R9 – Não existe. O setor de controles internos faz o monitoramento das operações, mas não existe a figura do CISO. R10 – Sim. Todos os colaboradores assinaram termo de compromisso e código de ética onde ficam cientes da política de segurança da informação da empresa. O nosso programa de capacitação prevê como objeto a segurança das informações.

Fonte: Dados da pesquisa.

A diferente visão dos entrevistados sobre *baselines* relativos ao domínio de entrega de valor invoca a análise de outras disciplinas que deveriam compor as mesmas como a estruturação da segurança da informação, a adoção de modelos consolidados de mercado, a segregação de funções, dimensionamento dos seus riscos, campanhas de conscientização de segurança voltadas para segurança e não TI, dentre outros, e que compõem as práticas da ISO 27002, não foram encontrados nas respostas.

Diante do contexto sobre o domínio de entrega de valor que proporcionaria diferenciais de competitividade, e criação de novos ativos de conhecimento, com a consolidação de uma cultura de segurança, sugere-se que a empresa A ainda encontra-se em um nível inicial de maturidade neste domínio.

4.1.4 Gestão de recursos

QUADRO 9
Respostas a gestão de recursos – Empresa A – TI

Referência	Respostas
EAG	R3 – Sim. O ex-gestor de infra era PJ, entretanto nunca tivemos um fornecedor (consultoria) realizando esta atividade. R12 – Não. Existe pouca documentação disponível na empresa. R13 - A segurança física está sob responsabilidade do *Data Center* e a Segurança lógica é realizada através dos usuários nominados. R15 – Parcialmente. Possuímos ambientes de desenvolvimento / qualidade e produção diferentes. Entretanto, a segregação de funções de pessoal não está bem definida. Utilizamos também bloqueio de acesso a dispositivos portáteis apenas na rede de projetos, a rede operacional está aberta.
EAE	R6 – Sim existe. Não é constantemente revisada, pois é uma política recentemente criada.

Fonte: Dados da pesquisa.

Prosseguindo-se nas análises, agora no escopo da gestão de recursos, verifica-se uma distorção a respeito da existência, ou até mesmo da eficácia, da suposta política de segurança da informação. Analisando-se todo o contexto existente, pode-se argumentar que se a mesma existe, está em processo de estruturação em virtude de todas as características de segurança da informação que foram apontadas para a empresa A até este ponto.

Nota-se uma evolução maior na gestão dos recursos, talvez fruto do objetivo maior que é a prestação de serviços de tecnologia às cooperativas, isto pode ser constatado por *baselines* de segurança existentes nas respostas sobre segregação de ambientes, segurança física e lógica (mesmo que incipiente), dentre outros.

Talvez o maior fator negativo para a gestão dos recursos seja justamente a ausência da classificação da informação para gestão de um dos maiores ativos de uma empresa, entretanto, em virtude do nível de maturidade apontado nos domínios anteriores, não

havia muito que se esperar desta disciplina, tornando a empresa A com nível de maturidade repetível, no domínio de gestão de recursos.

4.1.5 Medição de desempenho

QUADRO 10
Respostas a medição de desempenho – Empresa A – TI

Referência	Respostas
EAG	R7 – Não. R16 – Não, nenhuma iniciativa nesta linha.
EAE	R7 – Sem os dados relativos à operação fica inviável a continuidade. As consequências são de altíssimo impacto principalmente no que diz respeito à imagem da empresa. R8 – A Auditoria independente tem plena ciência, pois somos auditados nos níveis de processo e de sistema de TI. O mesmo para o setor de controle interno da empresa.

Fonte: Dados da pesquisa.

No domínio de medição de desempenho, pelas respostas do executivo EAE, constata-se que há entendimento da alta direção a respeito da criticidade da disponibilidade, comprometimento ou perda da informação, o que de certa forma induz a concluir que, devido ao nível de maturidade no alinhamento estratégico, esse mesmo entendimento da importância da informação pode estar chegando ao executivo via auditoria e controles internos, pois os mesmos têm entendimento claro de seus papéis na segurança da informação.

Por outro lado, e contraditoriamente ao apresentado, as ações no tratamento de incidentes e emergências não são processos definidos e testados, fundamentados pela avaliação de riscos inexistentes e pela baixa maturidade na estratégia de segurança bem como pela ausência completa do ISMS denotando por tudo isto uma maturidade em medição e desempenho a nível repetível.

4.1.6 Análise e conclusões

Conclui-se na análise da empresa A que praticamente a maioria dos domínios resultados de uma GSI eficaz encontra-se em níveis de maturidade muito iniciais, ainda com fatores mais agravantes como a falta de aderência à modelos práticos de segurança da informação que poderiam nortear as iniciativas relativas até mesmo à *baselines* de segurança voltados para TI.

Diante desse contexto, a empresa A, deve adotar e priorizar uma estratégia de segurança que inicie e respalde ações que possam colaborar positivamente para a governança de TI, para a GSI e consequentemente para a governança corporativa. Sem alinhamento estratégico entre esses três construtos a empresa estará fortemente sujeita às mudanças do ambiente que a envolve bem como aos riscos que explorarão suas vulnerabilidades visivelmente apresentadas.

4.2 Empresa B – Segmento financeiro

4.2.1 Alinhamento estratégico

QUADRO 11
Respostas a alinhamento estratégico – Empresa B – Financeiro
(Continua – Parte I)

Referência	Respostas
EBG	R1 – O conselho é informado sobre questões de segurança através dos relatórios de auditoria interna e externa do último semestre. R6- O CEO não pediu nenhuma avaliação de segurança, portanto não foram avaliados resultados de alguma avaliação pelo mesmo.

QUADRO 11
Respostas a alinhamento estratégico – Empresa B – Financeiro
(Conclusão – Parte II)

Referência	Respostas
EBG	R10- Sim. O alinhamento das informações de segurança com os objetivos do negócio é baseado no portfólio de projetos corporativos e na gestão de governança.
EBE	R1 - Sim. Existe o Comitê de Segurança em Canais que trata de assuntos de segurança aplicados ao negócio, incluindo contextos de fraudes e indicadores de gestão de segurança. R2 – A estratégia corporativa é consolidada no modelo de BSC (*Balanced Scorecard*). TI também tem BSC que associa objetivo estratégico de TI com negócio e a segurança. Dentro dos objetivos estabelecidos de TI existem os indicadores de segurança. R5 – Sim as informações de segurança aparecem na pauta da diretoria sendo inclusive auditadas e as não conformidades chegam ao conselho.

Fonte: Dados da pesquisa.

As respostas obtidas a partir do CISO juntamente com as respostas do coordenador de segurança respaldam um parecer a nível estratégico bem como da gestão da segurança na prática.

A estruturação da gerência de segurança hierarquicamente posicionada dentro da diretoria de TI, conforme Sêmola (2003, p. 27), não é um modelo adequado em virtude de encapsular o orçamento e ações de segurança ao Plano Diretor de Informática (PDI) ou Plano Estratégico de TI.

Essa estrutura de certa forma é atestada pela resposta do entrevistado EBG, de que o CEO não solicita informações sobre avaliações de risco, uma vez que a própria gerência de segurança pode distanciar-se dos altos executivos no acompanhamento destes nos assuntos relativos a esta gestão. Vale destacar que, perante a governança corporativa, os executivos são responsáveis por ações e conseqüências que envolvam a transparência e conformidade das organizações sendo assim crucial o acompanhamento dos assuntos ligados a mesma.

Entretanto, a empresa B, através de Comitês, minimiza alguns aspectos negativos dessa estrutura, pois se utiliza os mesmos para priorizar ações de segurança. Um ponto de observação é que estes Comitês são específicos, a exemplo do Comitê de Segurança em Canais Eletrônicos o que realmente dá a impressão de que são voltados para aspectos de

segurança ligados a TI. Aspectos físicos e humanos potencializam vulnerabilidades que também necessitam ser tratadas na estratégia de segurança principalmente por ter-se no segundo aspecto o elo mais frágil.

Devido ao porte da empresa B, recomenda-se o estabelecimento de um Comitê Corporativo de Segurança no qual haveria a representatividade de toda a organização abrangendo todos os aspectos de segurança e não só de segurança em TI. Este mesmo Comitê, coordenado e mediado pelo CISO, estaria posicionado na estrutura hierárquica ao lado do Comitê Executivo composto pelo CEO, CIO e conselho.

A estrutura poderia estar causando impactos negativos no alinhamento estratégico de segurança da informação com a estratégia de negócio na medida em que a estrutura organizacional causa certa distância entre os dois.

Por outro lado, esses problemas são minimizados por ações do CISO e Comitês existentes juntos ao forte apoio do alinhamento de TI com a estratégia de negócio. Isto também pode ser verificado pelos modelos de BSC que, segundo o CISO, alinham TI, segurança (mais focada em TI), e negócio, bem como adicionadas ao apoio das auditorias que fazem com que as não conformidades cheguem ao conselho.

No segmento financeiro vê-se o uso da tecnologia como um dos principais diferenciais competitivos, portanto, para a empresa B o alinhamento existente entre TI e estratégia de negócio acaba refletindo positivamente nos requisitos de segurança em TI.

A sujeição à regulação do BACEN também demanda da empresa B forte atuação em *compliance*, auditorias e segurança fato que é confirmado pela frequência dos relatórios de auditoria interna e externa e pelos princípios de governança existente na empresa.

Pelos aspectos positivos e negativos aqui pontuados para a empresa B pode-se classificá-la no nível gerenciado e mensurável, embora apresente também características de alinhamento estratégico no nível de processo definido, principalmente pela sua estruturação e pelo foco de segurança da informação em TI, este que de certa forma, bem alinhado ao negócio conduz alguns *baselines* de segurança no mesmo alinhamento, mas a desejar no escopo da segurança corporativa.

4.2.2 Gestão de riscos

QUADRO 12
Respostas a gestão de riscos – Empresa B – Financeiro

Referência	Respostas
EBG	R4 – Não tem a data prevista para a próxima avaliação de riscos, mas faz parte do processo de desenvolvimento de produtos e serviços. R5 – Na avaliação de riscos foi considerada a possibilidade de interrupção por não haver disponibilidade de informação crítica assim como foram consideradas as consequências de um incidente de segurança em termos de receitas. Além disto, foram determinadas as consequências de uma estrutura inoperante. Isso embasa o projeto de contingenciamento da empresa. R8 – A avaliação considera as leis e regulamentos, ainda mais com a fiscalização do órgão regulador. R9 – Sim, a avaliação de riscos é item regular na agenda de TI porque a avaliação de risco é feita em um processo contínuo de desenvolvimento de produtos e serviços e nas auditorias periódicas.
EBE	R3 – Sim o conselho compreende as responsabilidades perante a regulação, no ramo financeiro isto é certo!

Fonte: Dados da pesquisa.

Sobre os assuntos relacionados à gestão de riscos verifica-se uma preocupação em relação à segurança da informação em TI. O fato da avaliação de riscos não ter data prevista e estar vinculada ao desenvolvimento de produtos e serviços pode levar a empresa a uma perspectiva reativa do tratamento do risco o que pode tornar essa vinculação perigosa na medida em que Campos (2007, p. 98) corrobora que as avaliações de riscos são processos regulares em virtude das constantes mudanças que compõem o contexto organizacional de Pettigrew (1973) e em virtude de que as mudanças são oportunidades para revisar todo o sistema ou a parte mais diretamente afetada.

Seguindo na gestão de riscos, Westerman e Hunter (2008, p. 43) relatam que uma cultura de consciência do risco é construída a partir do topo da empresa, pois "[...] os executivos mostram - mediante suas ações, investimentos e comportamentos - que a governança do risco e a aceitação dos riscos calculados são parte da maneira de a empresa

fazer negócios.", entretanto, ao mesmo tempo alegam que isto não é uma prática fácil de ser realizada.

Por ser a TI um dos alicerces dos negócios do segmento bancário, principalmente ao serviço prestado no *internet banking*, verifica-se a aderência a Campos (2007, p. 57) que defende que uma maior preocupação com processos, serviços, e ativos mais relevantes para a organização é porque os mesmos tendem a ter maior impacto no caso de comprometimento e esta relação medida/risco parece ser bem estruturada na empresa B.

Especificamente sobre a relevância dos processos não foi possível verificar pelas respostas se a empresa tem algum tipo de metodologia para modelagem de processos, tais como BPM (*Business Process Model*), UML (*Unified Modeling Language*), dentre outras, entretanto, na visita realizada à empresa B foi possível detectar que as duas ferramentas são utilizadas, mas não sendo possível verificar quais os níveis de maturidade na utilização das mesmas.

Denota-se certa preocupação em relação à governança dos riscos com foco em TI (e não com foco em atendimento a toda a estrutura organizacional) bem como na ausência de informações mais consistentes sobre como o processo de classificação da informação ocorre.

Pelo contexto da gestão de riscos apresentado pelos respondentes, pela avaliação de riscos um processo que não segue uma periodicidade definida, fundamentados por uma segurança ainda focada em TI, vê-se que a empresa B está amadurecendo do nível gerenciado e mensurado para o nível otimizado neste domínio.

4.2.3 Entrega de valor

QUADRO 13
Respostas a entrega de valor – Empresa B – Financeiro
(Continua – Parte I)

Referência	Respostas
EBG	R2 – Sim as funções de segurança e responsabilidades são claramente definidas com a descrição dos cargos e ato normativo com criação da área de segurança da informação e suas responsabilidades.

QUADRO 13
Respostas a entrega de valor – Empresa B – Financeiro
(Conclusão – Parte II)

Referência	Respostas
EBG	R11- Através de comunicado interno são passadas as campanhas de segurança para todos os colaboradores. R14 – Sim implementa práticas de mercado, mas tem modelo próprio de análise de risco inserido no nosso processo de produtos e serviços. São levadas em consideração durante aquisição, desenvolvimento e manutenção de software.
EBE	R4 – Foi determinado o custo do incidente. R9 – Sim, existe um CISO encarregado da gestão de segurança da informação. R10 – Sim, na forma de comunicação corporativa as informações de segurança são levadas aos colaboradores.

Fonte: Dados da pesquisa.

A respeito da entrega de valor, outro resultado esperado de uma GSI, pode-se aferir que, mesmo com detalhes acima especificados que podem dificultar o trabalho do CISO, atestam-se pelas respostas que há resultados consideráveis nesse domínio, principalmente com o dimensionamento dos incidentes e a estruturação e normatização de segurança de forma a contribuir nos projetos da organização de forma positiva para a competitividade. O ponto de atenção aqui se volta para o impacto da estrutura de segurança ligada a TI e para o processo de comunicação referente aos programas de conscientização em segurança da informação e consequentemente nas responsabilidades de cada colaborador, pois as respostas dão a entender que o processo de comunicação está ocorrendo em sentido único e isto pode prejudicar o acompanhamento da cultura de segurança dentro da empresa.

Portanto, no domínio de entrega de valor, a empresa B também está na transição do nível gerenciado e mensurável para o nível otimizado, necessitando para a passagem de nível, que haja melhoria no domínio de alinhamento estratégico que sofre impacto da estrutura de segurança ligada a TI e no acompanhamento da conscientização de segurança, no processo de comunicação, e enfim na melhoria da cultural de segurança.

4.2.4 Gestão de recursos

QUADRO 14
Respostas a gestão de recursos – Empresa B – Financeiro

Referência	Respostas
EBG	R3 – Sim. Já teve segurança de rede controlada por terceiros. R12 – Sim, existe um processo de classificação da informação e é feita através da gestão dos serviços críticos de negócio. R13 – Sim, controles físicos e lógicos são adotados e implantados. R15 – Sim, implementa os requisitos de segurança no gerenciamento de operações e comunicações, segregação de funções, segregação de ambientes, bem como protege toda a infraestrutura. Sim para todos os ítens.
EBE	R6 – Sim, a política de segurança é revisada a cada 2 anos.

Fonte: Dados da pesquisa.

Na gestão dos recursos verifica-se que a empresa fez uso de terceiros para o controle da segurança de redes. Seguindo-se orientações da norma ISO 17799, ou 27002 e conforme Beal (2008, p 130), uma vez que o controle de segurança de rede pode levar a acessos de boa parte de informações privilegiadas, a empresa B de certa forma pode ter multiplicado os riscos inerentes ao tratamento da CID (tratamento da confidencialidade, integridade e disponibilidade) das informações. Não foram fornecidas informações sobre o controle nos serviços terceirizados, provavelmente não fazem parte dos controles de segurança lógica informada como adotado pela empresa.

Requisitos de segurança no gerenciamento de operações e comunicações foram atestados durante a visita respaldando o que é aconselhado pelos modelos de segurança da informação de forma eficaz e eficiente com processos, atividades e demais fluxos bem definidos para toda a infraestrutura computacional.

O estabelecimento de um Comitê de Crise na empresa B demonstra um planejamento estratégico, conforme Peixoto (2008, p. 10), para as forças e fraquezas relacionadas a fatores internos e a oportunidades e ameaças relacionadas a fatores externos,

logo a presença deste Comitê colabora positivamente no posicionamento da empresa em relação à gestão de riscos e à competitividade.

Há que se perscrutar sobre a resposta da *baseline* de classificação da informação em relação à atualização da política de segurança da informação (a cada dois anos), uma vez que a primeira é parte integrante da segunda e esta que sofre influência restritiva diretamente proveniente da estrutura onde a área de segurança se encontra, ou seja, ligada diretamente à diretoria de TI.

A classificação da informação é fundamental para a gestão dos riscos corporativos, uma vez que o modelo de segurança adotado é focado em TI perde-se na abrangência de mitigar riscos que não somente envolvem tecnologia da informação e isto impacta negativamente também na gestão de recursos atribuindo-se um nível de maturidade neste domínio como inicialmente otimizado ressalvando-se o tratamento dado à classificação da informação.

4.2.5 Medição de desempenho

QUADRO 15
Respostas a medição de desempenho – Empresa B – Financeiro

Referência	Respostas
EBG	R7 – Sim, o tratamento de incidentes e emergências é realizado através do Comitê de Crise. R16 – O ISMS não é baseado no modelo ISO, mas recorta trechos de vários frameworks.
EBE	R7 – A organização não continuaria a operar se a informação crítica ficar indisponível, comprometida ou perdida. Seria trágico! R8 – Ainda precisam alinhar a integração entre auditoria x segurança x *compliance* para que todos possam compreender claramente seus papéis.

Fonte: Dados da pesquisa.

As respostas colaboram para aferir-se que há garantias embasadas por meio de avaliações independentes e auditorias, entretanto, um processo de medição que ajude a identificar deficiências e proporcionem o retorno sobre os processos utilizados na resolução

de problemas não foi visualizado pelas respostas dificultando a análise das mesmas neste domínio.

O ISMS que ajudaria justamente na medição, identificação de deficiências, retorno sobre os investimentos, enfim na consolidação da SI, não é baseado, segundo o respondente EBG, na ISO 27001 e maiores informações não foram passadas a respeito, portanto, aqui se atribui um nível transitório de gerenciado e mensurável para otimizado.

4.2.6 Análise e conclusões

Finalmente, em análise holística das respostas obtidas pode-se entender que o modelo adotado foi concebido originalmente voltado para segurança em TI em vista de todo conteúdo respondido pelos dois entrevistados.

Por todos os domínios e respectivos *baselines* levantados nas questões respondidas pela empresa B, pode-se aferir que a mesma se enquadra em transição para o nível otimizado de maturidade em GSI.

4.3 Empresa C – Segmento de telecomunicações

4.3.1 Alinhamento estratégico

QUADRO 16
Respostas a alinhamento estratégico – Empresa C– Telecomunicações

Referência	Respostas
ECG	R1 - Tanto para o conselho de acionistas, quanto para a diretoria existe reuniões periódicas de repasse de *status* do Plano Diretor de Segurança da Informação com a apresentação de métricas e indicadores. R6- As métricas, indicadores e planos de ação resultantes do processo de gestão de riscos de segurança da informação são acompanhados pelo CEO e *board*. R10- Sim. Todos os produtos e serviços lançados e mantidos pela área de negócio passam por avaliação de segurança da informação tanto em nível estratégico quanto operacional. Esse processo reforça a necessidade de alinhamento constante dos objetivos.
ECE	R1 - Sim. Atualmente existe uma preocupação com segurança da informação como requisito do negócio de maneira, inclusive, a beneficiar o cliente. R2 - A estratégia de segurança da informação, fundamentada na estratégia de negócio, foi instituída corporativamente e aprovada formalmente pela alta administração, juntamente com o modelo de gestão de segurança da informação. R5 - Sim. Fundamentado na estratégia de segurança da informação e de negócio, um plano diretor de SI, que determina as prioridades a serem cumpridas no ano, é conduzido e acompanhado pela diretoria.

Fonte: Dados da pesquisa.

Após análise dos dados da entrevista realizada na empresa C, primeiramente, é possível verificar pelo conteúdo das respostas que os respondentes têm conhecimento dos assuntos que envolvem a segurança da informação e que são inerentes à responsabilidade de cada um. Tanto as respostas do questionário para executivo quanto às respostas do

questionário para gestor, há sintonia sobre a importância do assunto no âmbito executivo quanto gerencial.

Vê-se o estabelecimento da estrutura de GSI alinhada à estrutura organizacional da empresa, muito semelhante à proposta pela FIG. 4 – Conteúdo do Cobit, modelo que ajudou na concepção da GSI, principalmente, quanto a atender o alinhamento ao negócio com requisitos de segurança da informação. O alto escalão é ciente dos requisitos de segurança bem como participam de forma proativa no acompanhamento das métricas e indicadores dos mesmos além de manterem uma constante comunicação entre os envolvidos.

Sêmola (2003, p. 86) define que o planejamento existente no Plano Diretor de Segurança é fator crítico de sucesso para gerir a segurança da informação, portanto, na empresa C, o mesmo é fundamentado na estratégia de negócios e na estratégia de segurança da informação. Embora seja uma tarefa complexa manter a afinidade entre negócio e segurança, mostra que a empresa C, segundo suas respostas, trata a disciplina estrategicamente em um Comitê Executivo de Segurança.

Um detalhe muito interessante na Empresa C é que já coloca a estratégia de segurança da informação como um diferencial competitivo na medida em que considera seus resultados como fator agregador aos clientes em acordo com Campos (2007), Alves (2006) e Porter (1986), quando inserem a estratégia como oportunidade para competitividade nos negócios, portanto, pode-se considerar que a empresa C está em um nível otimizado de alinhamento estratégico tanto pela estrutura de GSI quanto pelos *baselines* que indicam a comunicação estabelecida bidirecionalmente, à participação da alta gestão nos assuntos de segurança envolvendo-os nos requisitos de negócios e na criação de uma cultura de segurança da informação.

4.3.2 Gestão de riscos

QUADRO 17
Respostas a gestão de riscos – Empresa C – Telecomunicações

Referência	Respostas
ECG	R4 - Última avaliação de riscos nos ativos críticos de informações ocorreu no primeiro semestre de 2010. Através de um processo cíclico, as avaliações são anuais para um acompanhamento da evolução do índice de segurança e nível de maturidade. R5 - A avaliação de riscos é precedida de mapeamento de ameaças e análises de riscos onde são considerados os prováveis gaps relacionados à continuidade de negócios e definidos os controles necessários para tratamento dos riscos. Sob as atividades relacionadas a gestão de continuidade ao negócio, são realizadas ações de risk assessment e de business impact analysis.
ECG	R8 - Existe um forte apoio do conselho sobre o processo de conformidade com leis e regulamentações, não só na própria organização, mas também em parceiros e fornecedores (*due diligence / due care*). R9 - Após execução do *risk assessment*, inicia-se a fase de tratamento dos riscos com a seleção dos controles a serem priorizados. Quinzenalmente, há o acompanhamento deste trabalho em fórum de segurança da informação e TI.
ECE	R3 - Esse entendimento existe e é um dos fortes motivos para o forte apoio do conselho no processo de conformidade com leis e regulamentações, não só na própria organização, mas também em parceiros e fornecedores (*due diligence / due care*).

Fonte: Dados da pesquisa.

Como a empresa C está sujeita à regulamentação, verifica-se a constante preocupação de todo o corpo diretor em estar em conformidade, bem como alinhado às boas práticas que envolvem a governança corporativa, nota-se que há a necessidade de acompanhamento de métricas e indicadores de segurança o que de certa forma indica que os executivos estão cientes de suas responsabilidades perante seus *stakeholders* estando os mesmos atentos a gestão dos riscos.

Embora não haja confirmação da adoção de um modelo padrão de gestão de riscos, vê-se que há um alinhamento entre Avaliação de Riscos (*risk assessments)* x TI x BIA (*Business Impact Analysis*) a serem realizados ciclicamente, inclusive com a adoção de nível de maturidade e acompanhamento do Comitê Executivo de Segurança. Isto indica que nos processos elencados para se mitigar os riscos corporativos, existe padronização, estabelecimento de métricas e relatórios que podem revelar também se a gestão de riscos leva em conta a avaliação de riscos alinhada a TI e ao negócio de forma a suprir também a continuidade deste.

O acompanhamento dos riscos corporativos por parte dos executivos da empresa C indicam que o processo de governança do risco já é realidade na mesma, já no início do nível otimizado, pois ainda existe a necessidade de uma maior automação nos processos de monitoramento, acompanhamento e mitigação dos riscos pelo ISMS, o que permite ações de mitigação no âmbito superior, bem como, no âmbito da gestão com independência na administração dos riscos mais próximos conforme Westerman e Hunter (2008, p. 32).

4.3.3 Entrega de valor

QUADRO 18

Respostas a entrega de valor – Empresa C – Telecomunicações

(Continua – Parte I)

Referência	Respostas
ECG	R2 - Através de estratégia de SI formalmente aprovada e comunicada para a companhia através das mídias oficiais do endomarketing, foi instituído o modelo de gestão de segurança da informação tendo as funções e responsabilidades de SI definidas. R11- Foi instituído um processo cíclico que inicia com pesquisa em conscientização de SI dos colaboradores. Essa pesquisa norteia a elaboração de um programa de conscientização, educação e treinamento para todos os colaboradores. Após a execução do programa, ocorre outra pesquisa para acompanhamento da evolução.

QUADRO 18
Respostas a entrega de valor – Empresa C – Telecomunicações
(Conclusão – Parte II)

Referência	Respostas
ECG	R14 - Todos os novos projetos críticos, de áreas de negócio ou de TI, há o envolvimento da segurança da informação *end-to-end*, no sentido de garantir que se definam os requisitos de SI e que eles sejam devidamente cumpridos. As práticas adotadas são fundamentadas nas políticas de segurança da informação e em normas e padrões internacionais.
ECE	R4 - Existe um processo formal para tratamento de incidentes e impactos. R9 - O CISO é atualmente ligado à vice-presidência da companhia. R10 - Foi instituído um processo cíclico que inicia com pesquisa em conscientização de SI dos colaboradores. Essa pesquisa norteia a elaboração de um programa de conscientização, educação e treinamento para todos os colaboradores. Após a execução do programa, ocorre outra pesquisa para acompanhamento da evolução.

Fonte: Dados da pesquisa.

Allen e Carnegie (2007, p. 6) informam que a efetiva Governança de Segurança da Informação deverá obedecer à segregação de funções, que conforme Beal (2008, p.54) devem estar introduzidas nos espaços organizacionais de Mintzberg (Cúpula Estratégica, Tecnoestrutura, Assessoria de Apoio, Linha Intermediária, e Núcleo Operacional). Na empresa C, papéis e responsabilidades são claramente atribuídos e segregados com linhas de comunicação estabelecidas e fluentes, inclusive com acesso direto de um profissional de segurança, o CISO, ligado diretamente à vice-presidência da empresa assim em conformidade com os modelos de GSI.

Um detalhe interessante é que na empresa C há um setor de auditoria exclusiva para tratamento de assuntos de segurança da informação o que respalda a preocupação dos *stakeholders* na preservação da CIDAL (Confidencialidade, Integridade, Disponibilidade, Autenticidade, Legalidade) da informação e conformidade.

Através da estratégia de SI, as campanhas de conscientização dos colaboradores são realizadas com a utilização de ferramentais como pesquisas que indicam os pontos

cruciais a serem abordados para uma nova campanha e após sua realização sendo feito o acompanhamento do resultado obtido.

Portanto, na empresa C existe uma forte cultura de segurança disseminada por todas as camadas da organização de forma coesa.

Durante o ciclo de vida dos projetos, aquisições, e prestação dos serviços, a entrega de valor se dá pela consciência dos envolvidos na cultura da segurança. O fato é que tendo colaboradores imersos na cultura de segurança, a entrega de valor também se dá através da mitigação dos riscos e dos investimentos respaldados por normas e padrões.

Um ponto de atenção no quesito de entrega de valor bem como na gestão de riscos da empresa C passa a ser o dimensionamento dos custos de eventuais incidentes, uma vez que nas respostas não foram encontrados indícios de que isto acontece na prática. Acredita-se que haja o dimensionamento citado justamente pelo modelo interno adotado, entretanto, pode ser que esteja refletindo negativamente no nível de maturidade da gestão de riscos da mesma. Segundo Campos (2007, p. 57) a relevância dos ativos, serviços e processos são a base para o dimensionamento do impacto de um incidente.

Não há um detalhamento desse dimensionamento na empresa C, mas a informação, ainda que recôndita, do respondente é aceitável por serem detalhes de domínio interno. Cabe a empresa verificar os impactos desse item porque o mesmo é escopo para a implantação do ISMS.

Atesta-se que a empresa já se encontra na fase inicial do nível otimizado da entrega de valor, justamente por ter praticamente um PDCA estabelecido para conscientização e comprometimento de pessoal sobre segurança da informação com a condução de processos resultando em melhorias com participações efetivas desde o início dos projetos.

4.3.4 Gestão de recursos

QUADRO 19
Respostas a gestão de recursos – Empresa C – Telecomunicações

Referência	Respostas
ECG	R3 - A segurança da rede é gerida e conduzida por colaboradores próprios, podendo ter parcerias com empresas terceiras no âmbito de atividades operacionais com o devido controle e monitoração. R13 - Controles de segurança física e lógica são instituídos com base em priorizações definidas dentro do processo de gestão de riscos. R12 - O processo de classificação da informação está instituído através da Política de Classificação de Informação, onde são definidas as responsabilidades e atribuições. R15 - Sobre o gerenciamento de operações e comunicações os requisitos inclusive passam por avaliações constantes de conformidade com leis e regulamentações e *risk assessment*. A proteção da infraestrutura é prioridade documentada no plano diretor de segurança da informação.
ECE	R6 - A revisão da política de segurança é anual.

Fonte: Dados da pesquisa.

Verifica-se que há controles de segurança física e lógica, tendo atuação de terceiros de forma operacional e não na gestão dos recursos envolvidos, o que de certa forma respalda a preservação da inteligência organizacional.

Entretanto, na gestão de recursos, não foi relatado como é o processo de revisão da classificação da informação o que pode denotar um adicional fator de risco uma vez que a informação, um bem ou ativo de grande valor (CAMPOS, 2007, p.21) e alvo de constantes violações, sofre alterações na sua classificação ao longo do tempo.

Uma das primeiras ações da gestão de riscos é levantar, revisar, e controlar seus ativos, principalmente, a informação. Logo, se há um descompasso nessas mesmas ações, preponderantes na classificação da informação, há de se preocupar com riscos eminentes que possam explorar essa vulnerabilidade comprometendo a gestão de recursos, portanto, ainda percebe-se a transição para o nível otimizado neste domínio.

4.3.5 Medição de desempenho

QUADRO 20
Respostas a medição de desempenho – Empresa C – Telecomunicações

Referência	Respostas
ECG	R7 - O processo de tratamento de incidentes e de problemas existente demonstra bastante eficácia e tem gerado ótimos resultados, principalmente no que se refere ao tratamento e mitigação de fraudes. O processo de avaliação e melhoria contínua está incluído como uma prioridade no plano diretor de segurança da informação. R16 - A organização instituiu estratégia e um modelo de gestão de segurança da informação que iniciou a implantação do ISMS na companhia, com a preocupação de aderência a ISO/IEC 27001.
ECE	R7 - A organização atua de maneira a estar preparada a manter a continuidade do negócio, pois entende que as consequências de graves incidentes podem gerar desgastes à marca, prejuízos financeiros e indisponibilidade dos serviços que são prestados aos clientes. R8 - Na organização existe uma divisão de auditoria específica para esse assunto de SI.

Fonte: Dados da pesquisa.

Finalmente, em conformidade com as informações levantadas para os domínios já citados, a empresa utiliza-se de técnicas e instrumentos de medição de desempenho de métricas de SI com respaldo na priorização do Plano Diretor de SI. A visão da gestão como era de se esperar é mais focada nos recursos que disponibilizam os controles para a efetiva GSI alinhada à visão executiva mais focada na continuidade dos negócios, na imagem, prejuízos financeiros e principalmente nos clientes. O respaldo da importância relatada pelo executivo é acompanhado por auditorias internas e externas, e excepcionalmente, pela auditoria específica para SI conforme relatado na resposta do mesmo.

A adoção do ISMS (em fase de inicial) é fator de consolidação que, conforme Campos (2007, p.31), dá sustentabilidade a SI de forma automática e cíclica, baseada no PDCA, deve ser fator de continuidade na empresa C visando a consolidação da maturidade em GSI, entretanto, neste ponto é o principal fator, juntamente com a classificação da informação, que impedem a consolidação no nível otimizado.

4.3.6 Análise e conclusões

Ao final da análise dos *baselines* existentes nas respostas da empresa C é notável a presença de adoção de práticas de mercado para apoio aos domínios de uma GSI eficaz bem como a efetiva participação do corpo executivo da empresa aliado ao CISO subsidiando positivamente toda a estratégia de segurança da informação.

Por todos os domínios e respectivos *baselines* levantados nas questões respondidas pela empresa C, pode-se aferir que a mesma se enquadra na parte intermediária do nível 5-otimizado de maturidade em GSI.

4.4 Empresa D – Segmento energético

4.4.1 Alinhamento estratégico

QUADRO 21
Respostas a alinhamento estratégico – Empresa D – Energético
(Continua – Parte I)

Referência	Respostas
EDG	R1- Não, o CEO nunca pediu uma avaliação de risco. R6 – O conselho não é informado sobre questões de segurança da informação. R10- Temos um processo de segurança da informação, mas que ainda não funciona de forma continua.
EDE	R1 - Sim, o valor e a importância da segurança da Informação são assimilados pela alta gestão.

QUADRO 21
Respostas a alinhamento estratégico – Empresa D – Energético
(Conclusão – Parte II)

Referência	Respostas
EDE	R2 – Sim, a organização possui uma estratégia de segurança através de seu plano diretor de segurança da informação. É alinhado com a estratégia de negócio porque foi construído com os gestores das áreas de negócio. O alinhamento com a tecnologia da informação precisa ser melhorado. R5 - Não. A segurança da informação só aparece em pauta de diretoria quando há algum assunto específico e urgente. Não existe procedimento para relatar resultados/acontecimentos ao conselho.

Fonte: Dados da pesquisa.

Após análise dos dados da entrevista realizada na empresa D, verifica-se inicialmente a pouca, ou ausente, participação do CEO e conselho nos assuntos de segurança da informação, embora segundo o respondente EDE a alta gestão assimile o valor e a importância da segurança da informação.

Decorre desse distanciamento entre alta gestão e gestão de segurança que a estratégia de segurança da informação, embora esteja vinculada ao Plano Diretor de Segurança da Informação, pode estar em descompasso com a estratégia de negócios da empresa, até mesmo porque o processo que garantiria o alinhamento das informações de segurança da informação com os objetivos de negócio ainda não está consolidado.

Isso pode ser respaldado também pela informação de que o alinhamento entre tecnologia da informação, segurança da informação, e estratégia global de negócios precisam ser melhoradas dando indícios de um nível repetível de maturidade neste domínio.

Embora não conste nas respostas, a posição hierárquica da área de segurança parece ainda estar vinculada à diretoria de TI, portanto, ainda poderia estar sofrendo impactos negativos, dentre estes, justamente o distanciamento da alta gestão.

4.4.2 Gestão de riscos

QUADRO 22
Respostas a gestão de riscos – Empresa D – Energético

Referência	Respostas
EDG	R4 – A última avaliação de riscos foi em 2008. A próxima está prevista para 2011. R5 – Sim, a avaliação de riscos considerou a importância da informação e construímos um plano de continuidade dos negócios. R8 – A avaliação de riscos ainda não considera que os ativos de informação estão sujeitos a leis e regulamentos. Ainda não. R9 – A avaliação de riscos ainda não é um item regular na agenda de TI. Estamos apagando incêndios.
EDE	R3 – As responsabilidades são claramente definidas em uma política. Entretanto acredito que o conselho não tem um claro conhecimento sobre o descumprimento da regulação. Apesar de termos uma política de classificação das informações também acredito que ele não tenha um claro entendimento das responsabilidades quando uma informação sigilosa for comprometida.

Fonte: Dados da pesquisa.

Na governança da gestão de risco nota-se um período muito longo, de três anos, entre as avaliações de riscos, consequentemente conforme apresentado nas respostas o tratamento dos riscos é reativo o que torna a empresa sujeita a complicações mais graves para manter a continuidade do negócio.

Há um longo caminho para que a gestão de riscos na empresa D atinja um alto nível de maturidade neste quesito, pois não somente pelos problemas apresentados na avaliação de riscos, há ainda a pouca percepção dos ativos informacionais da empresa.

Além disto, o alinhamento entre segurança da informação, tecnologia da informação, e estratégia global, ainda em processo de crescimento torna mais complicado o envolvimento conjunto na gestão de riscos.

A percepção de que o Conselho não tenha um claro conhecimento sobre o descumprimento da regulação é um dos principais fatores de riscos a serem enfrentados na empresa D.

A gestão de riscos verificada na empresa D ainda está em um nível repetível e precisa rapidamente de melhorias e principalmente do estabelecimento de uma cultura de risco disseminada em uma abordagem *Top-down.*

4.4.3 Entrega de valor

QUADRO 23
Respostas a entrega de valor – Empresa D – Energético

Referência	Respostas
EDG	R2 – Sim, as funções e responsabilidades de segurança são claramente definidas através da política de Segurança da Informação. R11- Os programas de conscientização são realizados através de treinamentos presenciais e online e mais duas campanhas anuais. R14 – Geralmente a segurança é envolvida apenas no final. Isto é cultural, mas está mudando.
EDE	R4 – Já tivemos alguns incidentes, mas os valores não foram apurados. R9 – Sim existe um CISO e temos um núcleo com seis pessoas para a segurança da informação. R10 – Sim, há formação e programas de conscientização e temos programas presenciais com regularidade anual, duas campanhas também anuais e treinamento online.

Fonte: Dados da pesquisa.

Com a política de segurança estabelecida criando a estrutura de segurança da informação devidamente formalizada, percebe-se o esforço da empresa para alavancar a consciência do risco e os requisitos de segurança.

Pelos aspectos apresentados no alinhamento estratégico, inclusive na posição da área de segurança ligada a TI, na gestão de riscos, e pela cultura de segurança ainda em

formação é importante a empresa verificar os processos de treinamentos e conscientização de todos os colaboradores, partindo-se da alta gestão, a fim de fazer com que a segurança passe a ser utilizada com a devida prioridade e com diferencial estratégico que possa agregar valor e como consequência sair de um nível repetível para um nível de processo definido de maturidade neste domínio de entrega de valor.

4.4.4 Gestão de recursos

QUADRO 24
Respostas a gestão de recursos – Empresa D – Energético

Referência	Respostas
EDG	R3 – Temos alguns serviços atualmente controlados por terceiros. R12 – Sim, temos um processo de classificação das informações ativo desde 2007. R13 - Sim, temos controles de segurança da informação tanto para segurança física quanto lógica. R15 – Sim, implementa requisitos de segurança no gerenciamento de operações e comunicações, todos estes controles desta pergunta são utilizados na empresa.
EDE	R6 – Sim, existe uma política de segurança da informação, revisada anualmente e aprovada pela diretoria.

Fonte: Dados da pesquisa.

Na gestão dos recursos, conforme já informado, a política de segurança é o instrumento inicial para alavancar a segurança da informação, o ponto positivo é que a mesma sofre atualizações frequentes e em períodos determinados, mas acredita-se que sua abrangência seja focada nos requisitos práticos da segurança da informação contidas na ISO 27002. Embora haja um processo de classificação da informação desde 2007, acredita-se que o mesmo sofre as consequências existentes nos desalinhamentos apontados entre TI, SI e estratégia global de negócio e talvez não reflita a realidade deste.

Pode-se atribuir um nível partindo-se de definido para gerenciado e mensurável de maturidade na gestão de recursos isto porque ainda não se consegue concluir pelas respostas apresentadas que essa mesma gestão é capaz de gerar melhorias nos processos de TI e de segurança.

4.4.5 Medição de desempenho

QUADRO 25
Respostas a medição de desempenho – Empresa D – Energético

Referência	Respostas
EDG	R7 – Sim, existe processo para tratar da segurança da informação em incidentes e emergências através do processo de incidentes do ITIL associado ao de segurança da informação. R16 – Temos um processo definido para ISMS, mas ainda não roda automaticamente.
EDE	R7 – Se a empresa perder informações relacionadas a operação dos sistema os prejuízos financeiros, de imagem serão muito altos podendo levar até a perda de concessão. R8 – Sim, a auditoria é muito atuante no assunto de segurança da informação e compreende seu papel.

Fonte: Dados da pesquisa.

Sobre a medição do desempenho, vale ressaltar que o ITIL para requisitos de segurança é pouco significativo se comparado com outros modelos como, por exemplo, o COBIT e a ISO 27001 E ISO 27002, portanto, embora seja um bom caminho a adoção de modelos, há todo o cuidado para não se focar em modelos mais voltados para outros fins.

Por todo o contexto apresentado, fica difícil a adoção do ISMS, seguindo um PDCA definido e de forma automatizada, isto pode ser atestado quando o respondente EDG informa que há o processo, porém não cumpre os requisitos principais do mesmo.

Devido ao contexto na qual está inserida, riscos eminentes podem comprometer a continuidade de parte dos negócios da mesma, entretanto, um detalhe interessante que pode estar colaborando para amenizar um pouco todo este contexto apresentado pode estar apoiado na atuação da auditoria que segundo o respondente EDE é muito frequente e compreende claramente o seu papel e, justamente, por estes corrobora na atribuição de um nível de maturidade gerenciável e mensurável para este domínio até mesmo por se acreditar que sua maturidade é que realmente esteja amenizando complicações maiores para a empresa D.

4.4.6 Análise e conclusões

Percebe-se que a empresa D sofre, assim como algumas outras já relacionadas, da falta de envolvimento do corpo diretor da empresa com a estratégia de segurança da informação. A estrutura na qual está inserida a área de segurança da informação da empresa ligada a TI já dá indícios dos aspectos negativos que comprometem o nível de maturidade em todos os domínios. Pontos positivos são obtidos através do provável alinhamento de TI ao negócio e pelo papel da auditoria dando a entender ser uma abordagem *down-top* e focada em *baselines* de segurança em TI. Por todos os aspectos apresentados e o comportamento dos níveis anteriores de maturidade da empresa D, pode-se atribuí-la no nível de processo definido em GSI.

4.5 Empresa E – Segmento de regulação

4.5.1 Alinhamento estratégico

QUADRO 26
Respostas a alinhamento estratégico – Empresa E – Regulação

Referência	Respostas
EEG	R1- Não existe um conselho. R6 – Sim, a solicitação de mudança de servidor de e-mail hospedado no *google,* bem como de domínio hospedado por terceiros, foram transferidos para a processadora de dados do estado. Caso contrário, poderiam comprometer com vazamento de informações importantes. R10- Não, a maioria das organizações públicas possui um caráter político que prejudica o incentivo de projetos tecnológicos e projetos de segurança da informação.
EEE	R1 – Não. Porque a cultura da gestão de segurança da informação que agrega valor e importância está associada diretamente a organização, se essa possui um perfil tecnológico a alta gerência se preocupara com segurança. R2 – Sim. Mas nas organizações públicas suas diretrizes são políticas e não tecnológicas e estão alinhadas com serviços públicos e sociais. Pode existir estratégia de segurança, mas voltada para segurança e não para o negócio. R5 – Não. Apesar do Núcleo de informática adotar medidas de segurança e políticas dentro do possível isso não é o suficiente para ser inserido como item de pauta da direção. Espera-se adotar medidas de um projeto de segurança da informação que possam conscientizar a direção.

Fonte: Dados da pesquisa.

Após análise dos dados da entrevista realizada na empresa E, verifica-se praticamente uma participação mínima de executivos nos assuntos estratégicos de segurança da informação tendo como atenuante uma pontual solicitação ligada à segurança de TI. As informações de alinhamento de estratégia global de negócios e estratégia de segurança da informação não são existentes, fato verificado nas respostas de EEG. Portanto, na mesma linha de Porter (1979) a empresa A não alinha oportunidades e ameaças, portanto, não sendo compartilhados os objetivos que mapeiam os riscos pela mesma. Isto é verificado na gestão de riscos a seguir.

Uma das consequências da alta gestão não assimilar o valor e a importância da segurança da informação, acaba sendo refletida na estruturação da área de segurança da informação que não existe no organograma da empresa E bem como na ausência de responsável devidamente formalizado para tratamento do assunto na mesma apesar de um colaborador compartilhar atribuições de outras funções com as de segurança. Este modelo, conforme Sêmola (2003, p. 63), não é adequado e corrobora as dificuldades encontradas por este profissional para tratamento de assuntos de segurança da informação internamente.

Ainda assim, nas respostas apontadas em EEE parece haver uma estratégia de segurança, mas que essa não é alinhada ao negócio, nem mesmo é pauta de reunião de diretoria, portanto, conforme Allen (2005) pode-se entender que essa possível estratégia, por não ser alinhada ao negócio, não poderá servir como sustentação para uma cultura de segurança a ser preservada para se atingir os objetivos de negócio.

Na empresa E existe apenas em poucos *baselines* que são inclusive existentes em segurança de TI e que mesmo assim há indícios de um distanciamento entre as estratégias pode-se aferir que a empresa está em um nível muito inicial no domínio de alinhamento estratégico.

4.5.2 Gestão de riscos

QUADRO 27
Respostas a gestão de riscos – Empresa E – Regulação
(Continua – Parte I)

Referência	Respostas
EEG	R4 – Não existem políticas de mitigação de risco, apesar de existir processos adotados. R5 – Apesar da indisponibilidade da informação não ser crucial, o vazamento da informação pode acarretar mais danos do que a sua falta. R8 – Apesar de existir uma normatização legalmente publicada, não existe um procedimento para assegurar o cumprimento dessas leis e regulamentos.

QUADRO 27
Respostas a gestão de riscos – Empresa E – Regulação
(Conclusão – Parte II)

Referência	Respostas
EEG	R9 – Apesar da avaliação de risco ser um item na agenda do Núcleo de Informática, fatores com quantidade profissionais, estrutura física, e outros impedem que esse e vários outros projetos na organização prossigam.
EEE	R3 – Sim pode até compreender as responsabilidades da organização no caso da normatização de regulação. Os incidentes de segurança certamente serão tratados como um processo administrativo normal, isso se da pelo desconhecimento técnico sobre segurança da informação pelo gestor ou pela própria cultura da organização.

Fonte: Dados da pesquisa.

Existe na empresa a preocupação com o ativo informacional não quanto à sua disponibilidade, mas quanto à sua integridade e confidencialidade, segundo o respondente EEG, isto em virtude de ser a empresa E um agente fiscalizador e regulador.

Entretanto, quando não há um alinhamento entre estratégia de segurança e estratégia global de negócios, evidencia-se dentre os resultados o comprometimento na gestão dos riscos, pois este depende fundamentalmente do conhecimento dos ativos dos negócios e como há um descompasso entre o que se tem e o que se quer proteger, a empresa E torna-se muito vulnerável nas suas principais *baselines* de integridade e confidencialidade, inclusive, conforme Westerman e Hunter (2008, p.126), a ausência de uma consciência de risco aumenta riscos evidentes de vazamento de informação, pois há certo descontrole sobre esta e sobre o colaborador.

A avaliação de risco de cunho específico para tratamento de segurança em TI existe, mas não é um processo regular bem como se pode atestar que não há um modelo de gestão de riscos na empresa E, ficando à mesma suscetível a reação reativa no tratamento de riscos.

Um fator muito preocupante é que a empresa E, como regulador e fiscalizador, aparenta deixar de cumprir as próprias normatizações não levando em consideração as leis e regulamentos às quais esta inserida. De certa forma também pode repercutir negativamente perante a sociedade a desestruturação na segurança da informação atestada pelos respondentes.

Considera-se que a empresa A ainda está na fase de transição de um nível inexistente para um nível inicial / *ad hoc*, porque apesar de haver avaliação de riscos a mesma não é um processo regular, alinhado com o negócio, e tem sua base reativa bem como de certa forma não existe uma compreensão dos riscos, ameaças e impactos relativos à potenciais consequências do comprometimento da informação em um órgão regulador e fiscalizador.

4.5.3 Entrega de valor

QUADRO 28
Respostas a entrega de valor – Empresa E – Regulação

Referência	Respostas
EEG	R2 – Não existe uma política de segurança publicada, muito menos papéis definidos ou divulgados. R11 – Existem processos paliativos para incentivar uma adoção de medidas de segurança com o propósito de divulgar a necessidade de uma cultura de segurança. R14 – Sim. Uso de certificado digital em transações financeiras, adoção de configuração de rede e sistemas de configuração de estações de trabalho e servidores, quanto a aquisição de software segue padrões definidos pela secretaria (pregão eletrônico). Aplicações centradas na processadora de dados do estado (mainframe). Políticas de segurança de senhas.
EEE	R4 – Não. Para se determinar um incidente de segurança é necessário que haja pelo menos conhecimento técnico com um suporte físico e pessoal específico para tal fim. Vontade política e administrativa da Direção suficiente para determinar uma política de Segurança para a organização. R9 – Não, apesar de ter um funcionário qualificado, ele é voltado para atender todos os serviços. R10 – Não, existem processos adotados para conscientizar e tentar passar a cultura de segurança da informação.

Fonte: Dados da pesquisa.

Na análise de *baselines* referentes a uma estrutura e política de segurança da informação, segundos os respondentes os mesmos não existem, inclusive não havendo

funções e responsabilidades devidamente formalizadas o que reforça um nível inexistente para entrega de valor, entretanto, *baselines* referentes à segurança de TI são adotados em menor escala como uma herança do controle de infraestrutura de TI, seguindo-se alguns padrões já estabelecidos e primeiros movimentos de uma cultura de segurança da informação ainda incipiente sendo que neste ponto já é sentida uma melhoria da entrega de valor passando para inicial /ad hoc.

Neste domínio, especificamente a entrega de valor agregaria muito na transparência e na efetividade da empresa E em suas ações reguladoras e fiscalizadoras dando à sociedade uma percepção da eficácia do órgão nas suas ações.

4.5.4 Gestão de recursos

QUADRO 29
Respostas a gestão de recursos – Empresa E – Regulação

Referência	Respostas
EEG	R3 – Sim, Houve época em que o servidor de e-mail estava hospedado no *google*, após uma reunião chegou se ao consenso de mudança. R12 – Não, não existe um processo de classificação de ativos. R13 – Existem controles físicos de pouca importância e processos lógicos com algumas medidas de segurança. R15 – Apesar de adotar gerenciamento de segurança por terceiros que envolve segurança em operações e comunicações, que envolve ambientes de produção e homologação externos, existem deficiências internas na infraestrutura de rede para dispositivos portáteis.
EEE	R6 – Não. Existem processos adotados de outros órgãos com políticas publicadas e adotadas, sendo necessário uma elaboração de uma política própria da organização.

Fonte: Dados da pesquisa.

Quanto à gestão de recursos pode-se alegar que a empresa herda da infraestrutura de TI os *baselines* mais básicos de segurança provenientes da ISO 27002, com controles ainda

embrionários, mas com algumas medidas de segurança, porém com deficiências visíveis e que ainda estão sob a gestão de terceiros. A falta de uma política de segurança, consequentemente também de uma classificação de ativos, requisitos primordiais para se estabelecer os *baselines* de segurança reforça todo o contexto descrito até este ponto resultando em um nível inicial / ad hoc também para a gestão de recursos.

4.5.5 Medição de desempenho

QUADRO 30
Respostas a medição de desempenho – Empresa E – Regulação

Referência	Respostas
EEG	R7 - Não, não existe um processo eficaz e testado para tratar de segurança. R16 - Não, não existe um ISMS.
EEE	R7 – Sim. Por ser um órgão fiscalizador com o negócio voltado ao atendimento ao público, o vazamento de informação pode acarretar mais danos do que a indisponibilidade da informação. R8 - Não, não existe um setor de Auditoria específico para segurança da informação no momento.

Fonte: Dados da pesquisa.

No domínio de medição de desempenho a consequência da inexistência de processos para incidentes e emergências, bem como a inexistência de um ISMS consolidam riscos eminentes para as vulnerabilidades apontadas na gestão de riscos, porém com um agravante que é a inexistência de uma auditoria que possa minimizar alguns impactos negativos .

Tendo o acompanhamento de alguns *baselines* de segurança acompanhados por empresa terceira de TI, há um fator mitigante a respeito do acompanhamento e monitoração dos ativos de TI, entretanto, para o risco maior apontado, ou seja, o vazamento de

informações, não há qualquer iniciativa que possa atenuar a vulnerabilidade desse *baseline* de segurança.

Consolidando fatores negativos em maioridade com pouca atenuação nos quesitos de medição e desempenho chega-se a conclusão que não existe compreensão dos riscos e o serviço de continuidade não é considerado, mas a responsabilidade pela continuidade dos serviços é informal e com autoridade limitada, portanto respaldando a classificação da empresa E neste domínio como inexistente em transição para *ad hoc*.

4.5.6 Análise e conclusões

Conclui-se na análise da empresa E, assim como na empresa A, que praticamente a maioria dos domínios resultados de uma GSI eficaz encontra-se em níveis de maturidade muito iniciais, porém o agravante da primeira é justamente a inexistência de auditoria interna ou externa que poderia atenuar alguns dos problemas encontrados.

Diante desse contexto, a empresa E, poderia priorizar ações *top-down* que respaldem a criação de uma estratégia de segurança alinhada ao negócio da regulação criando *baselines* específicos para a política de segurança, avaliações de riscos, classificação de ativos, dentre outros requisitos que dariam maior conforto à atividade fiscalizadora e reguladora perante a sociedade.

4.6 Empresa F – Segmento industrial

4.6.1 Alinhamento estratégico

QUADRO 31
Respostas a alinhamento estratégico – Empresa F – Industrial

Referência	Respostas
EFG	R1 - Não tenho conhecimento se nas reuniões do conselho, questões de segurança são tratadas. Não tenho esse registro. R6- Sim, o CEO solicitou e a diretoria foi comunicada dos resultados. R10- Sim, através do planejamento estratégico e operacional de cada área, informações de segurança e objetivos de negócio são alinhadas.
EFE	R1 – Sim, o valor e a importância da segurança da informação são assimilados pela alta gestão. R2 – Sim, tem estratégia de segurança e está alinhada com as estratégias de negócios e também com a TI. R5 – Sim, é um item de pauta da diretoria através dos acompanhamentos semanais e mensais.

Fonte: Dados da pesquisa.

Após análise dos dados da entrevista realizada na empresa F, primeiramente, é possível verificar pelo conteúdo de algumas respostas que os entrevistados realizam determinado esforço no sentido de responderem as perguntas, mas deixam de esclarecer como os processos são realizados, as ações e decisões executadas, ou o funcionamento de tal *baseline* de segurança. Em alguns casos, há suposição que determinado requisito seja atendido e em virtude dessa suspeita fica a cargo do entrevistador, baseado nas referências bibliográficas, a decisão sobre o atendimento ou não a determinados requisitos de segurança.

Não fica muito clara a estruturação da área de segurança na empresa, se está vinculada estruturalmente a TI ou se já está ligada diretamente ao alto escalão da organização conforme recomendações apontadas por Laurindo *et al.* (2001), alinhado com Sêmola (2003) e Alves (2006).

Tomando-se por base a resposta R1 de EFG, justamente o gestor de segurança da empresa, informando desconhecer se as reuniões de conselho tratam questões de segurança, vê-se certo distanciamento em relação ao conselho, entretanto, todas as outras respostas deste domínio indicam já haver aspectos de alinhamento estratégico de segurança com estratégia global de negócios.

O fato é que o peso negativo do desconhecimento de questões de segurança em reuniões do alto escalão, indicam que o alinhamento estratégico possa ser fruto dos *baselines* ligados a TI, da regulação, do planejamento estratégico das áreas (e não corporativo), e não de uma estratégia de segurança propriamente dita, o que leva a deduzir que a maturidade no alinhamento estratégico da empresa F encontra-se em transição do nível repetível para um nível de processo definido.

4.6.2 Gestão de riscos

QUADRO 32
Respostas a gestão de riscos – Empresa F–Industrial

Referência	Respostas
EFG	R4 – A última avaliação de riscos foi na área de Engenharia em 2007. A próxima ainda não está definida. R5 - Sim, os riscos foram considerados e medidas de mitigação estão sendo implementadas. R8 – Sim, e os procedimentos são criteriosamente analisados para que estejam conformes com a legislação. R9 – Sim, a avaliação de riscos é item regular na agenda de TI e os projetos são avaliados com os responsáveis pela tomada de decisão considerando os riscos de cada um.
EFE	R3 - Entendo que a diretoria compreenda as responsabilidades da organização no descumprimento da regulação e trabalha nas medidas de proteção.

Fonte: Dados da pesquisa.

Embora não haja regulação para este segmento especificamente, alguns aspectos ligados à leis e normas desse contribuem para alavancar positivamente os *baselines* da gestão de riscos, pois nas respostas verifica-se uma preocupação evidente dos executivos em manter a conformidade e a legalidade. Por outro lado, vê-se que o *baseline* que indica a frequência da avaliação de riscos é inexistente, conforme respondido por EFG preocupa na medida em que há um período muito longo entre avaliações de riscos sendo que a próxima inclusive encontra-se indefinida. Paradoxalmente, cita que a última avaliação de riscos foi realizada na engenharia em 2007, que a próxima não está definida, mas que a avaliação de riscos é um item regular na agenda de TI.

Esta discrepância entre o que se deseja e o que se tem, é uma contradição entre o interesse da alta gestão e a operacionalização de requisitos de conformidade e legalidade que compõem a GSI principalmente por serem estes passíveis de mudanças e factíveis de auditorias frequentes.

Não há confirmação da adoção de um modelo padrão de gestão de riscos tendo o tratamento dos mesmos com base em riscos de TI, talvez em aspectos de conformidades e legalidades também ligados a TI, mas em detrimento de outros componentes da gestão de riscos, principalmente na classificação da informação, que será apontada a seguir na gestão de recursos.

Através da ausência de respostas que evidenciem o alinhamento entre estratégia de segurança e estratégia global de negócios, corroborando Sêmola (2003, p.33) que afirma ser a estratégia de segurança uma etapa da GSI composta de vários componentes, pode-se deduzir que no domínio de gestão de riscos na empresa E há um processo de transição de maturidade de nível repetível, para um nível de processo definido, mas ainda com uma gestão de riscos reativa, não mensurada, considerando os riscos de TI como importante, mas com processo de avaliação ainda em desenvolvimento.

4.6.3 Entrega de valor

QUADRO 33
Respostas a entrega de valor – Empresa F–Industrial

Referência	Respostas
EFG	R2 - Sim, as funções e responsabilidades de segurança são definidas e comunicadas através de decisões de diretoria, procedimentos e normas internas definidas pela empresa. R11- Programas de conscientização ocorrem através do plano para ação anual da área de SI, onde são considerados palestras de conscientização e de integração em praticamente todos os projetos e colaboradores recém contratados, em conjunto com a área de comunicação empresarial. R14 - Entendemos que cada vez mais a segurança da informação é considerada no inicio dos projetos, através do envolvimento e participação da área de SI. Em relação à aquisição, desenvolvimento e manutenção de softwares, também a SI participa indicando os requisitos de segurança para a TI.
EFE	R4 – Não existe um processo formal para tratamento de incidentes e impactos. R9 - Sim, coordenador, gestor, grupo de trabalho e comitê de SI. R10 - Sim, existem as campanhas anuais em todos os projetos e as integrações para os recém admitidos.

Fonte: Dados da pesquisa.

A estruturação da SI, inclusive com gestor, grupos de trabalhos e comitê de SI, são os responsáveis pelo plano de ação, políticas, e padrões de segurança da informação a serem seguidos o que direciona um caminho para se alterar o foco da segurança na empresa F baseada em TI para uma segurança estratégica alinhada aos objetivos de negócio respaldando os princípios de GSI, TI e governança corporativa. Isso pode mudar para melhor todos os níveis de maturidade já comentados e fazer com que a empresa F tenha mais atuação em GSI proporcionando mais entrega de valor à organização.

Já relacionado a outros casos, um ponto de atenção no domínio de entrega de valor bem como no domínio de gestão de riscos da empresa F passa a ser o dimensionamento dos custos de eventuais incidentes, uma vez que nas respostas não foram encontrados indícios

de que isto acontece na prática bem como também não foram encontradas evidências da avaliação de risco de forma proativa.

Por outro lado, um dos *baselines* para a entrega de valor é justamente a existência de processos formais para tratamento de incidentes e impactos e neste quesito a empresa não apresenta consenso entre os respondentes.

Dentro de uma gestão de riscos com base reativa há um maior dimensionamento de vulnerabilidades e ameaças, entretanto, respostas ligadas à conscientização, responsabilidades, programas e envolvimento da área de segurança indicam que a empresa F encontra-se em um nível de processo definido para a entrega de valor, mas com tratamento de incidentes ainda em nível repetível.

4.6.4 Gestão de recursos

QUADRO 34
Respostas a gestão de recursos – Empresa F – Industrial

Referência	Respostas
EFG	R3 – Não teve a segurança de rede controlada por terceiros, mas monitorada sim. R12 - Não temos um processo de classificação da informação. R13 – Sim, implementa controles de segurança física e lógica. R15 - Sim, estamos estruturando a segregação desses ambientes.Já fazemos proteção para dispositivos portáteis e equipamentos móveis de armazenamento de dados.
EFE	R6 - Sim existe política de SI aprovada e as revisões podem ocorrer quando se fizerem necessários ou quando planejadas.

Fonte: Dados da pesquisa.

Na gestão de recursos, apesar da existência de segurança física e lógica, do trabalho de terceiros apenas para monitoramento, verificam-se a ausência da classificação da

informação e a iniciação da segregação de ambientes, fatores que potencializam vulnerabilidades e riscos atrelados a estes *baselines*.

A existência da política de segurança da informação sem um processo de revisão estabelecido denota para um esforço na implementação de requisitos práticos contidos na norma 27002, mas que ainda podem ser embrionários ou inexistentes.

Portanto, perante as características apontadas pode-se aferir que a empresa F está no ponto intermediário entre o nível repetível e o nível de processo definido para o domínio de gestão de recursos.

4.6.5 Medição de desempenho

QUADRO 35
Respostas a medição de desempenho – Empresa F – Industrial

Referência	Respostas
EFG	R7 - Sim, existe processo para tratamento de incidentes/emergências, mas como todo processo, pode ser melhorado. R16- Já temos normas e procedimentos baseados na ISO/IEC 27001.
EFE	R7 - Entendemos que pode continuar a operar, mas dependendo do incidente as operações seriam prejudicadas. Um impacto grande nos negócios. R8 - Entendemos que sim, que a auditoria compreenda seu papel na segurança da informação, mas deveriam participar mais efetivamente.

Fonte: Dados da pesquisa.

Em relação ao domínio de medição de desempenho, apesar do posicionamento divergente entre os entrevistados a respeito dos procedimentos de tratamento de incidentes / emergências, a empresa relata a adoção de algumas práticas do sistema de gestão de segurança da informação, que não foram esclarecidas nas respostas, que podem estar comprometidas em virtude dos problemas apontados, e que não concretizam um existente nível de maturidade em ISMS, mas que já dão indícios de primeiros trabalhos nesse assunto.

Outro fator importante para a medição de desempenho é o papel da auditoria que no caso é apontado sucintamente, mas com o desejo de que possa ser mais atuante em assuntos se segurança da informação o que denota falta de certas garantias a respeito de conformidades.

Diante do cenário de medição de desempenho, da imprecisão acerca de métricas e de desempenho, além de indefinições sobre garantias e alinhamentos aos objetivos dos negócios pode-se aferir que as mesmas informações trazem a tona um cenário de continuidade fragmentado sem levar em conta o impacto no negócio, portanto, respaldado por fatores antecedentes chega-se a conclusão que o nível repetível seria mais adequado à este domínio.

4.6.6 Análise e conclusões

As indefinições apresentadas pelos respondentes perante algumas questões levantadas respaldam um nível de maturidade baixo para o alinhamento estratégico que logicamente repercute por todos os outros domínios.

Assim pela caracterização exposta do contexto de segurança da empresa F com seus respectivos *baselines* levantados nas questões respondidas, pode-se aferir que a mesma se enquadra em um em um nível repetível de GSI, mas com ações e melhorias em alguns *baselines* que já atingem o nível de processos definidos.

4.7 Discussão geral

Já no início da análise de dados elegendo-se primeiramente a empresa A, do segmento de TI, que não está diretamente sob regulação, vê-se de início que o primeiro resultado esperado de uma Governança de Segurança da Informação eficaz, justamente o

alinhamento estratégico entre os construtos é incipiente e influencia negativamente toda a estrutura dos outros domínios ou resultados esperados da GSI eficaz.

Essa mesma percepção da alta direção a respeito dos assuntos de segurança da informação como sendo uma disciplina de TI corrobora negativamente em alguns casos analisados e justifica até mesmo a estrutura na qual a área de segurança da informação está inserida dentro da organização.

Mesmo sendo a empresa A de menor porte na pesquisa, é importante frisar que indiretamente a mesma tem que atender requisitos da regulação do segmento financeiro em seus sistemas bem como se ressalta sua importância para este estudo em virtude de pertencer ao segmento que mais investiu em tecnologia da informação além de estar entre os quatro segmentos mais visados para fraudes.

Dentre as organizações pesquisadas, chama a atenção o comportamento dos critérios adotados no nível de maturidade existente nos domínios resultantes da efetiva GSI da empresa C (segmento de telecomunicações), dando fortes indícios de alinhamento estratégico, estratégico de segurança, estratégico de TI, seguindo princípios da Governança Corporativa, gerando valor ao negócio e que a qualificam altamente nos níveis de maturidades podendo ser uma referência em GSI neste segmento.

Na mesma linha da empresa C, a empresa B também se destaca por bons níveis de maturidade nos domínios da efetiva GSI e tendo as mesmas em comum o fato de estarem sujeitas à regulação, terem forte apoio da auditoria interna e externa, e terem força no alinhamento estratégico de TI ao negócio. Estes aspectos respaldam os modelos de governança corporativa visto que nos mesmos visualizam-se os construtos de alinhamento estratégico, governança de TI e GSI.

Alguns pontos de atenção na empresa B respaldam a necessidade de se entender a estratégia de segurança da informação como parte da estratégia global de negócios e não da estratégia de TI, pois caso contrário, o impacto negativo nos resultados esperados de uma GSI afeta o nível de maturidade nos domínios pela restrição de escopo que a segurança da informação passa a ter vinculada a TI.

Por outro lado, também foi possível notar que a empresa D tem relevantes problemas no alinhamento entre TI, SI, e estratégia global de negócios. Assim como uma

segurança da informação basicamente focada em requisitos práticos, o desalinhamento reflete negativamente na gestão de riscos e o impacto só não é maior devido à forte atuação da auditoria.

O aparente desconhecimento de aspectos regulatórios, leis e demais normas, pela alta gestão da empresa D eleva os riscos referentes à conformidade bem como reflete em toda a cultura de risco organizacional, dado este que precisa de atuação imediata do CISO no sentido de fazer com que a segurança da informação passe a ser uma cultura com abordagem *top-down* de implantação.

Na primeira ilustração, fora dos três segmentos primários, ou sob regulação, vê-se o contexto de segurança na qual está envolvida a empresa E que tem como atividade fim a regulação e a fiscalização de outras empresas.

A avaliação da maturidade em GSI da empresa E expõe vulnerabilidades sobre a principal preocupação apontada que é o vazamento de informação corroborando nos riscos apontados nos casos de corrupção que foram relatados nas justificativas deste estudo. Nem mesmo os *baselines* referentes à segurança da informação foram bem avaliados e podem dar a dimensão da urgência no tratamento da segurança principalmente por ser a mesma uma reguladora e fiscalizadora de outras empresas.

A empresa E foi inserida na amostra para contextualizar o comportamento de um órgão fiscalizador perante os domínios esperados da GSI eficaz e para ilustrar as vulnerabilidades e riscos que alguns órgãos públicos estão sujeitos e que podem culminar em fraudes pela falta de controle do ativo maior que os mesmos detêm: a informação.

Já para a empresa F verificam-se indícios da estruturação da área de segurança, programas de conscientização, porém com abrangência pouco definida e que pode ser refletida diretamente de um sucinto alinhamento estratégico de segurança com o alinhamento da estratégia global de negócios. Essa restrição afeta todos os outros domínios analisados para a empresa F que mostra ainda pouca participação de auditorias para gerar garantias e mitigar riscos ligados a leis e normas.

Com características peculiares, a empresa F, denota certa confusão no tratamento da estratégia de segurança, mesmo que fragmentada, na tentativa de aderir às práticas, mas aparentemente sem um roteiro para tanto, na adoção de requisitos de segurança, mas sem

medidas que ateste que o objetivo tenha sido alcançado, na gestão de riscos ainda como um processo intuitivo e reativo, dentre outros *baselines* ainda em fase de concepção e estruturação.

A empresa F é inserida na amostra como representante de um segmento que não está sob qualquer regulação, mas consegue merecido destaque na medida em que obtém um razoável nível de maturidade em GSI.

Além disto, tem-se o intuito de esclarecer e reforçar que empresas que estejam sujeitas a órgãos reguladores podem ter na auditoria e controles internos importantes aliados para se fazer com que estratégia de segurança seja parte da estratégia global de negócios, desde que tenham forte atuação e compreendam seu papel na segurança da informação, porém não é o caso da empresa F.

Tendo-se por base o comportamento do nível de maturidade em GSI, conforme modelo do ITGI (2006), dado em virtude de resultados eficazes nos domínios citados e, para cada um destes, no conjunto de *baselines* que se encontram intrinsecamente inseridos nas questões de pesquisa tem-se:

a) maturidade em alinhamento estratégico: Em quase todas as empresas foram encontrados indícios de alinhamento estratégico de segurança da informação com a estratégia global de negócios, entretanto, em muitos casos há predominância de requisitos de *baselines* existentes na governança de TI a exemplo da empresa B, C, D e F e mais discretamente na empresa A. Outro caminho encontrado para que os *baselines* de segurança chegassem ao executivo foi através de ações das áreas de controles internos e auditorias, principalmente, na empresa B e C e D que sofrem forte regulação. O alinhamento estratégico na empresa E é muito inicial e torna-se fator preocupante por ser a mesma um órgão público regulador sujeita à riscos frequentes, dentre estes, o vazamento de informações. Destaca-se a empresa C, com fortes indícios de alinhamento estratégico de segurança com a estratégia global de negócios proveniente da auditoria exclusiva para segurança da informação, do controle interno, da acessibilidade do CISO à vice-presidência, do comitê executivo de segurança, e da governança de TI, consolidando a segurança da informação dentro da estrutura organizacional

de forma eficaz e eficiente inclusive a ponto de ser diferencial de competitividade em um nível de maturidade otimizado. Notoriamente, a maturidade neste alinhamento acaba refletindo nos demais por ser a GSI de abordagem *top-down;*

b) maturidade em gestão de riscos: Assim como no alinhamento estratégico, há uma predominância da gestão de riscos de TI, vinculados logicamente pelos *baselines* de segurança provenientes da governança de TI. A empresa B apresenta forte gestão de riscos baseada em TI, mas com certa abrangência aos negócios espelhada pelo alinhamento dos requisitos de regulação e governança de TI com a estratégia de negócio. Entretanto, a estrutura organizacional desta empresa influencia diretamente sobre os domínios apresentados, pois é mais voltada para TI, talvez aí um pouco da falta de integração entre segurança, auditoria e *compliance*, mas que não a impede de ter um nível de maturidade na gestão de riscos muito bom. Novamente a empresa C apresenta-se com bom nível de maturidade para a gestão de riscos corporativos, pois apresenta os mesmos aspectos positivos da empresa B, mas com diferenciais como integração entre áreas com respaldo de uma auditoria exclusiva para segurança e do comitê executivo de segurança. O ponto de atenção às empresas B e C na gestão de riscos é a classificação da informação necessária ao ERM com maior preocupação em relação a primeira empresa pela sua localização na estrutura organizacional. A empresa D tem como agravante as avaliações de riscos por longos períodos e a ausência de percepção do Conselho sobre o descumprimento da regulação é o principal fator de risco estabelecendo-a em um nível intermediário de maturidade neste quesito. As empresas A e E, com níveis baixos de maturidade, se destacam pela ausência de um modelo de gestão de riscos, com a iniciação, ou inexistência, das avaliações de riscos, estando as empresas sujeitas ao tratamento reativo dos riscos ou sujeita à efetividade de auditorias que possam ajudar, o que não é o caso da empresa E;

c) maturidade em entrega de valor: As empresas A e E não tem muitos pontos positivos neste domínio uma vez que ainda se encontram em um nível inicial de maturidade na entrega de valor. No caso da empresa A, por pertencer a um segmento que mais investe em segurança, contraditoriamente, os recursos não são refletidos na priorização dos assuntos de segurança corporativamente.

Para a empresa E, um órgão regulador, como a entrega de valor envolve conscientização, ou uma cultura de segurança, nota-se que riscos relativos a vazamento de informação são agravados quando esta é fraca justamente por ser o colaborador, em muitos casos, o agente do vazamento. Embora a empresa F ainda esteja em um nível repetível neste domínio, notoriamente as respostas indicam que os problemas apontados para esta empresa podem ser sanados rapidamente influenciando em outros domínios por haver certo destaque nos programas e na cultura de segurança da informação. Exatamente por essa força neste quesito outros *baselines* existentes neste domínio para a mesma podem sofrer melhorias rapidamente. Ao mesmo tempo este processo de treinamento e conscientização é ponto de atenção na empresa B, embora em outros *baselines* deste domínio a mesma tenha bons resultados. A empresa C aparece com forte cultura de segurança disseminada por toda estrutura organizacional, fruto do alinhamento estratégico informado anteriormente e da própria estruturação da segurança da informação. Há um ponto de atenção no dimensionamento dos custos relativos a incidentes que aliás, assim como outras empresas, foram respondidos de forma sucinta, entretanto, é um assunto a ser considerado na gestão de riscos das mesmas. Acredita-se que o dimensionamento dos incidentes exista na empresa C por todo o contexto positivo de GSI apresentado pela empresa, mesmo se contrário, não desabona uma classificação no nível otimizado para a mesma;

d) maturidade em gestão de recursos: Em praticamente todas as empresas houve bons resultados nos níveis de maturidade deste domínio nos *baselines* de segurança em infraestrutura referidos na ISO 27002. Entretanto, os *baselines* referentes à classificação da informação de certa forma estavam ausentes ou foram respondidas de forma evasiva ou distorcidas em algumas empresas. Ressalta-se o desempenho da empresa C em transição para o nível otimizado e a empresa B já no nível otimizado, mas ainda em amadurecimento no mesmo;

e) maturidade em medição de desempenho: Notoriamente na maioria das empresas o papel da auditoria e dos controles internos influenciou positivamente alguns *baselines* de segurança deste domínio, mesmo nos casos onde foi detectado mais atuação das mesmas, com destaque para a empresa C que tem auditoria exclusiva para segurança da informação. Seguindo-se na

empresa C há praticamente uma consolidação de um modelo PDCA de segurança onde os *baselines* são avaliados periodicamente embora o ISMS ainda esteja em fase inicial. Já no nível de maturidade otimizado neste domínio a empresa C caminha para a consolidação da GSI. Outras empresas como a B e D sugerem a adoção de modelos próprios, entretanto, baseado no conjunto de respostas obtido, de certa forma não garante sua eficácia, mas acredita-se que estejam em fase inicial de operação. Na empresa E o nível de maturidade tem um comportamento pior, pois nem mesmo conta com suporte de auditoria para melhor desempenho e tampouco apresenta processos de incidentes e emergências. Caso mais peculiar encontrado neste domínio é referente às expectativas existentes entre o executivo e a gestão, da empresa F, pois as respostas apontam certa divergência na questão do tratamento de incidentes/emergências, entretanto, seguindo-se o contexto na qual a mesma está inserida e baseando-se nos níveis de maturidade que já foram apresentados para a mesma denota que há um nivelamento repetível (intuitivo para a mesma. A empresa F apresenta iniciativas para um ISMS, mas aparentemente confuso em suas características em virtude de pouca informação apresentada sobre o mesmo, ainda assim apresenta um cenário de continuidade de negócios fragmentado com imprecisão em métricas e desempenho.

A consolidação dos resultados obtidos nas análises das organizações em cada nível de maturidade em GSI ressalta de forma comparativa o comportamento das mesmas em relação aos *baselines* existentes em cada nível.

5 CONCLUSÕES

Alguns entrevistados demonstraram na prática que a segurança da informação é assunto delicado, restrito, e isto se justifica pela ausência de explicações maiores sobre determinados pontos da pesquisa principalmente em como os requisitos são atendidos.

Embora haja casos onde a GSI já está em nível mais elevado, inclusive com potencial utilização da mesma como diferencial de competitividade, há notoriamente uma predominância da preocupação com a segurança da informação em si, ou seja, nos requisitos práticos de segurança apontados pela ISO 17799:2005 ou a 27002.

Essas mesmas empresas que hoje se preocupam com os aspectos práticos da segurança da informação deveriam adotar uma postura mais estratégica incorporando o quadro de diretores, conselho, e acionistas na estratégia de segurança da informação fazendo com que a GSI seja governada como parte crítica das organizações.

Notoriamente, a maioria dos executivos entrevistados revelou comportamento de desconhecimento quanto à necessidade e priorização do alinhamento estratégico de segurança da informação à estratégia global da empresa, fator preocupante, pois os mesmos são responsáveis diretos pelos valores da governança corporativa que depende intrinsecamente da GSI na preservação dos mesmos.

Há um entendimento emergente sobre a necessidade de se tratar melhor a gestão dos riscos, entretanto, ainda reativamente e focado em segurança de TI. Fato complicador que releva aspectos importantes do alinhamento da estratégia de segurança da informação com a estratégia de negócios, pois o alinhamento de TI ao negócio como apoio e motivador às ações de GSI passa a ser uma relação de dependência direta e única para a existência da GSI.

O posicionamento da área de segurança da informação na estrutura organizacional, na maioria dos casos estudados, ainda é vinculado à área de TI refletindo negativamente nos níveis de maturidade em GSI, pois somente *baselines* de segurança em TI é que chegam à cúpula da empresa denotando que segurança da informação é assunto de TI.

A adoção dos modelos que compõem a GSI, em muitos casos, ainda é dispersa e não faz parte de uma estratégia global, é focada em modelos de TI, portanto, sendo usada em escopo restrito, de forma difusa e pontual, pois como não fazem parte de uma estratégia global, que é iterativa, ficam vinculados aos orçamentos e projetos de TI com início e fim.

O papel positivo da auditoria e da regulação ficou evidente nos estudos, pois na maioria dos casos foram atenuadores de riscos principalmente nos casos onde os níveis de maturidade em GSI não foram convincentes fazendo com que as normas, leis, e regulamentos fundamentados no COSO, BACEN, e outros marcos regulatórios chegassem à alta gestão alavancando a cultura de segurança da informação.

Organizações que estão sob fiscalização e controle de órgãos reguladores mostraram níveis de maturidade mais positivos em relação às outras que não estão sob este tipo de conformidade, fato que comprova a importância da regulação, entretanto, as organizações que não estão diretamente sob regulação, mas que indiretamente acabam necessitando da conformidade são pontos de atenção pelos resultados apresentados na maturidade em GSI.

Exatamente pela importância da regulação, deixa-se aqui um ponto relevante a ser mais esclarecido sobre o comportamento dos mesmos órgãos reguladores perante GSI em sua própria estrutura interna, pois na pesquisa os resultados encontrados são preocupantes na medida em que justamente a organização reguladora demonstrou níveis baixos de maturidade em GSI.

Positivamente, ficou evidente que assuntos de segurança da informação, principalmente de gestão de riscos, têm chegado ao alto escalão das empresas via *baselines* de segurança em TI e através da gestão do risco operacional, que inclui a atuação dos controles internos, auditoria e *compliance*, e todos esses atores evidenciam a importância do alinhamento dos mesmos na GSI.

Vê-se que a GSI é muito mais do que somente uma prática contida nas ISOs, *baselines* de segurança em TI, ou adoção de modelos quaisquer, sendo também um governo e conjunto de responsabilidades a partir do conselho e executivo às camadas mais inferiores da organização, bem como ações contínuas e estratégicas de segurança e, principalmente, de uma cultura organizacional voltada para segurança como fator de diferencial competitivo.

Conclui-se que o comportamento do nível de maturidade em GSI resultante deste estudo de múltiplos casos indica evolução em um nível 2 - repetível, mesmo nos segmentos sujeitos à regulação, embora haja exceções que indicam um nível de maturidade 5-otimizado em alguns domínios. A conseqüência direta desse comportamento resulta na alegação de que algumas empresas, que informam optar pelas práticas da governança corporativa, podem estar comprometendo a eficácia no tratamento dos valores desta, ou seja, no senso de justiça, na transparência, na prestação de contas, e na conformidade, na medida em que não priorizam estrategicamente a adoção da Governança de Segurança da Informação.

Intrinsecamente sobre este trabalho, por mais que haja planejamento em um projeto desta importância, verificam-se alguns pontos que podem ser melhorados a fim de contribuir mais com o tema.

O tema segurança da informação por si só é restritivo e causa constrangimento quando levantado junto às empresas, mesmo preservando a confidencialidade dos envolvidos, portanto, a forma de abordagem para a realização da pesquisa é um dos fatores de sucesso.

O estudo apresentou certa diversidade cultural entre os segmentos, pois foram selecionados três segmentos sujeitos à regulação, adicionando-se a amostra, outros três segmentos que foram selecionados para enriquecerem o comportamento da exceção à diversidade apresentada. Além disso, na amostra constam três segmentos onde há maior incidência de fraudes diversas colaborando para ressaltar a importância do tema para as empresas da amostra.

O estudo qualitativo de caráter exploratório envolve muitas variáveis para o correto dimensionamento das análises e para a apresentação destas exigindo um referencial teórico muito rico e que foi conseguido com muita dedicação neste estudo.

Finalmente, não foi foco estabelecer pontualmente o nivelamento de cada resultado de uma GSI eficaz, mas sim contextualizar o comportamento de cada nível deixando-se aqui o convite para novos desbravamentos no desafio de se encarar um estudo quantitativo a respeito deste rico tema.

REFERÊNCIAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS E TÉCNICAS. NBR 17799: **Tecnologia da informação: código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2005.

ALBERTIN, Alberto L; SANCHEZ, Otávio P. **Outsourcing de TI**. Impactos, dilemas, discussões e casos reais. Rio de Janeiro: FGV, 2008.

ALBUQUERQUE, R.; RIBEIRO, B. **Segurança no desenvolvimento de software**. Ed. Campus. Rio de Janeiro, 2002.

ALLEE, V. **The knowledge evolution**: expanding organizational intelligence. Newton: Butterworth-Heinemann, 1997.

ALLEN, J. H. **Governing for enterprise security**. (CMU/SEI-2005-TN-023). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 2005. Disponível em: <http://www.sei.cmu.edu/library/abstracts/reports/05tn023.cfm.>. Acesso em: 01 abr. 2010

_____.; CARNEGIE, M. **Governing for enterprise security (GES) implementation guide** - Article 1: Characteristics of Effective Security Governance Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2007; Disponível em: <http://www.cert.org/archive/pdf/GES_IG_1_0702.pdf>. Acesso em: 26 abr. 2010.

ALVES, Gustavo. **Segurança da informação:** uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna, 2006.

ANDRADE, A.; ROSSETTI J. P. **Governança corporativa:** fundamentos, desenvolvimento e tendências. 4. ed. São Paulo: Atlas, 2009.

ASHFORTH, Blake *et* al. Special topic forum on “corruption in organizations": re-viewing organizational corruption. **The Academy Of Management Review (amr),** Mississippi, v. 33, n. 3, p.670-684, 01 Jul. 2008.

BEAL, Adriana. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

BERGAMINI JUNIOR, S. Controles internos como um instrumento de governança corporativa. **Revista do BNDES,** Rio de Janeiro, v.12, n.24, p.149-188, dez. 2005.

BERNARDES, Mauro C.; MOREIRA, Edson S. **Um modelo para inclusão da governança da segurança da informação no escopo da governança organizacional**. 2005. Disponível em: < www.neoreader.com.br/item/doc/349/pdf/Segur_inf.pdf>. Acesso em: 10 jun. 2010.

BETTARELLO, Flávio C. **Governança corporativa**: fundamentos jurídicos e regulação**.** São Paulo: Quartier Latin, 2008.

BNDES. **BNDES modifica a classificação do porte de empresa**. 23 jun. 2010. Disponível em: < http://www.bndes.gov.br/SiteBNDES/bndes/bndes_pt/Institucional/Sala_de_Imprensa/Noticias/2010/institucional/20100622_modificacao_porte_empresa.html>. Acesso em: 11 set 2010.

BRAND, Koen; BOONEN, Harry. **IT governance based on Cobit 4.1**: a management guide. 3th ed. [S.l.]: Van Haren, 2007.

BRODBECK, A. *et al.* Práticas de alinhamento estratégico promovidas em organizações do estado do Rio Grande do Sul. In: ENANPAD, 2005, Brasília. **Anais**.. .Porto Alegre: ENANPAD, 2005. p.1-16.

CALDER, Alan; WATKINS, Steve. **IT governance**: a manager's guide to data security and BS 7799/ISO 17799. 3th ed. [S.l.]: [s.n.], 2005.

_____. **Information security based on ISO 27001/ISO 27002**: a management guide. 2nd ed. [S.l.]: Van Haren Publishing, 2009.

CAMPOS, André. **Sistema de segurança da informação:** controlando os riscos. 2. ed. Florianópolis: Visual Books, 2007.

CERT. **Governing for enterprise security:** implementation guide. 2010. Disponível em: < http://www.cert.org/governance/ges.html >. Acesso em: 10 jul 2010.

CGTF - CORPORATE GOVERNANCE TASK FORCE. **Information security governance:** a call to action. 2004. Disponível em: <http://www.criminal-justice-careers.com/resources/InfoSecGov4_04.pdf >. Acesso em: 11 Jun 2010.

CHAMBERS, Andrew; GRAHAM, Rand. **Operational auditing handbook:** auditing business and IT process. 2nd. ed. [S.l.]: United Kingdom, 2010.

CHAN, Y.; REICH, B. IT alignment: what have we learned? **Journal of Information Technology**, [S.l.], v. 22, p.297-315, 2007.

CHANDLER, A. D. **Strategy and structure.** [S.l.]: MIT Press, 1962.

CIAMPA, Mark. **Security+ Guide to Network Security Fundamentals.** 3nd ed. [S.1.]:Cengarge Learning, 2009.

COLLIS, Jill; HUSSEY, Roger. **Pesquisa em Administração**: um guia prático para alunos de graduação e pós-graduação. 2. ed. Porto Alegre: Bookman,2005.

CORTÊS, Bernardo G. W. **Haja Ignorância 2 - Ainda mais picante... ainda mais mal-humorado.** São Paulo: Physys Editora Ltda, 2010.

D'AVILA, Marcos Zahler; OLIVEIRA, Marcelo A. M. **Conceitos e técnicas de controles internos de organizações**. São Paulo: Nobel, 2002.

DALKIR, K., **Knowledge management in theory and practice**. Amsterdam: Elsevier/Butterworth Heinemann, 2005.

DAVENPORT, T.H.; PRUSAK, L**. Information ecology**: mastering the information and knowledge environment. [S.l.]: Oxford University Press, 1997.

DAVIS M.M; AQUILANO N.J.; CHASE R.B. **Fundamentos da administração da produção**. 3. ed. São Paulo: Bookman. 2001.

DENZIN, N. K.; LINCOLN, Y. S. **Hand-book of qualitative research**. [S.l.]: Thousand Oaks, 1994.

DIAS, Albélio N. F; PARDINI, Daniel J.; AGUIAR, Afrânio. **Mecanismos de controle e avaliação de projetos sociais corporativos em siderúrgicas mineiras**. 2005. Disponível em: <http://revista.newtonpaiva.br/pos/index.php/RevistaPos/article/viewFile/25/24>. Acesso em: 12 jun 2010.

DOBB, Maurice. **Studies in the development of capitalism**. London: Routledge and Kegan Paul, 1963.

FAGUNDES, E. M. **Cobit:** um kit de ferramentas para excelência na gestão de TI. 2008. Disponível em: <http://www.efagundes.com/artigos/cobit.htm>. Acesso em: 10 jun. 2009.

FARHAT, Said. **Dicionário parlamentar e político**. O Processo Político e Legislativo no Brasil. São Paulo: Fundação Petrópolis, 1996.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz. **Implantando a governança de TI:** da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.

FLEURY, M. T. L. *et al*. **As pessoas na organização.** 9. ed. São Paulo: Gente , 2002.

FREITAS, H.; MOSCAROLA, J. Da observação à decisão: métodos de pesquisa e análise quantitativa e qualitativa dos dados. **RAE Eletrônica**, São Paulo, v. 1, n. 1, jul./dez. 2002.

GALLEGOS, Frederick; SENFT, Sandra**. Information tecnology control and audit**. 3nd ed. [S.l.]: Tailor e Francis Books, 2009.

GARTNER, Group. **O futuro da tecnologia**: a justificativa econômica da TI. [S.l.]: [s.n.], 2005. (Conferência Anual)

_____. **The Gartner 2010 cyber threat landscape**. 2010. Disponível em: <http://www.dts.ca.gov/pdf/news_events/sec_awareness/Gartner_CyberThreat_landscape_2010.pdf> Acesso em: 01/07/2010

GIL, A.C. **Métodos e técnicas de pesquisa social.** São Paulo: Atlas, 1999.

GODOY, Arilda. S. Introdução à pesquisa qualitativa e suas possibilidades. **Revista de Administração de Empresas**, São Paulo, v.35, n.2, p. 57-63, abr. 1995.

GRUBITS, Sonia; NORIEGA José A. V. **Método qualitativo**: epistemologia, complementariedade e campos de aplicação. São Paulo: Vetor Editora Psico-pedagógica, 2004.

GUERRA, Isabel C. **Pesquisa qualitativa e análise de conteúdo**: sentidos e formas de uso. Portugal: Princípia, 2006.

HENDERSON, J. C.; VENKATRAMAN, N. Strategic alignment: leveraging information technology for transforming organizations. **IBM Systems Journal**, New York, v. 32, n. 1, 1993.

IBGC - INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa.** 4. ed. São Paulo: IBGC, 2009.

IMONIANA, Joshua. **Auditoria de sistemas de informação**. 2. ed. São Paulo. Atlas, 2008.

ISACA. **COBIT**. 2007. Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx>. Acesso em: 01 mar 2010.

_____. **CISA review manual 2008**. [S.l.]: [s.n.], 2008.

ISG. **Information security governance assessment tool**. Security Task Force. 2004. Disponível em: <http://net.educause.edu/ir/library/pdf/SEC0421.pdf>. Acesso em: 21 Abr. 2010.

ITGI - INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. **COBIT 4.0:** rolling meadows. [S.l.]: [s.n.], 2005.

_____. **Information security governance:** guidance for boards of directors and executive management. 2nd ed. [S.l.]: [s.n.], 2006. Disponível em:<http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=34997>. Acesso em: 01 Abr. 2010.

_____. **COBIT 4.1.** [S.l.]: [s.n.], 2007.

_____. **Aligning Cobit, ITIL, and ISO 17799 for business benefit.** [2010] Disponível em: <http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf>. Acesso em: 21 jun 2010.

JAMIL, George. **Gestão da informação e do conhecimento em empresas brasileiras**: estudo de múltiplos casos. 2005. Tese. (Tese Doutorado em Ciência da Informação) – Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2005

JENSEN, Michael C.; MECKLING, William. Theory of the firm: managerial behavior, agency costs and ownership structure. **Journal of Financial Economics**, v. 3, 1976.

KERZNER, Harold. **Project management**: a systems approach to planning, scheduling, and controlling. 10. ed. New Jersey, USA: John Wiley & Sons, 2009. 1061 p.

KIELING, R. C. **A viabilidade de projetos em TI alinhada ao planejamento estratégico das empresas**. 2005. Monografia - Centro Universitário Feevale do Instituto de Ciências Exatas e Tecnológicas do curso de Ciência da Computação, Novo Hamburgo, 2005.

KLEIN, Benjamim. Contracting costs and residual profits: the separation of ownership and control. **Journal of Law & Economics**, [S.l.], v. 26, 1985.

LAHTI, Christian B.; PETERSON, Roderick. **Sarbanes-Oxley:** conformidade TI. São Paulo: Alta Books, 2006.

LARA, Consuelo Rocha Dutra de. **A atual gestão do conhecimento**: a importância de avaliar e identificar o capital humano nas organizações. São Paulo: Nobel, 2004.

LAURINDO, F. *et al.* O papel da tecnologia da informação (TI) na estratégia das organizações. **Gestão & Produção,** São Paulo, v.8, n.2, p.160-179, ago. 2001.

LIMA, Samantha. CVM rejeita acordo sobre vazamento de informações na Petrobrás. **Folha On-Line,** 26 mar. 2010. Disponível em: <http://www1.folha.uol.com.br/folha/dinheiro/ult91u712327.shtml>. Acesso em: 18 maio 2010.

LINS, Clarisse; WAJNBERG, Daniel. **Sustentabilidade corporativa no setor financeiro brasileiro**. Ago. 2007. Disponível em: <http://www.fbds.org.br/fbds/IMG/pdf/doc-243.pdf>. Acesso em: 02 Mai 2010.

LONSANE, Raj. B. **Information security governance**. 2010. Disponível em: < http://www.articlesbase.com/ecommerce-articles/information-security-governance-by-raj-b-lonsane-2033299.html>. Acesso em: 23 mar 2010.

LUFTMAN, J. N. Assessing business: it alignment maturity. **Communications of the Association for Information Systems,** Atlanta, v. 4, p. 1-50, 2000.

_____. **Managing the information technology resource**: upper saddle. River, NJ: Pearson, 2004.

MAGALHÃES, I. L.; PINHEIRO, W. B. **Gerenciamento de serviços de TI na prática**: uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

MALHOTRA. Naresh K. **Pesquisa de marketing:** uma orientação aplicada. 4. ed. Porto Alegre: Bookman, 2004.

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

MATTAROZZI, Victorio; TRUNKL, Cassio. **Sustentabilidade no setor financeiro**: gerando valor e novos negócios. São Paulo: Editora Senac, 2008.

MILES, R. E.; SNOW, C. C. Fit, Failure and the hall of fame. **California Management Review,** California, v. XXVI, n.3, spring 1984.

MINTZBERG, Henry. **Criando organizações eficazes:** estruturas em cinco configurações. 2. ed. São Paulo: Atlas, 2003.

_____. *et al.* **O processo da estratégia:** conceitos, contextos e casos selecionados. 4. ed. São Paulo: Artmed, 2003.

MISANGYI, Vilmos F. *et al.* Special topic forum on “corruption in organizations": ending corruption: the interplay between institutional logics, resources, and instituitional entrepreneurs. **The Academy Of Management Review (amr)**, Mississippi, v. 33, n. 3, p.771-800, 01 Jul. 2008.

MOELLER, Robert R. **Sarbanes-Oxley internal controls**: effective auditing with AS5, Cobit and ITIL. New Jersey, USA: John Wiley & Sons, 2008.

MONKS, Robert. A. G.; MINOW, Nell**. Corporate governance**. 4. ed. Wiley: United States, 2008.

MOTTA, P. R. F. **Agências reguladoras.** São Paulo: Manole, 2003.

NASCIMENTO, Blenda L. F. **Solução de controvérsias internacionais:** revisão do papel da ONU como pilar da segurança internacional. Curitiba: Juruá, 2007. 288p.

NONAKA, Ikujiro; TAKEUCHI, Hirotaka. **Criação de conhecimento na empresa**: como as

empresas japonesas geram a dinâmica da inovação. Rio de Janeiro: Campus, 1997. 358p.

OLIVEIRA, Luiz Claudio Vieira de; CORREA, Osvaldo. **Normas para redação de trabalhos acadêmicos, dissertações, e teses.** 2. ed. Belo Horizonte: Universidade FUMEC, 2008.

PAIVA, Mauricio Ferraz. **Sistemas de gestão da informação que armazenam imagens digitais de documentos com fidedignidade e confiabilidade**. São Paulo: Target Editora Gráfica, 2008.

PANNUNZIO, Antonio Carlos. **Brazil, entre linhas por Pannunzio**.Brasília, 2008.

PAULK, M.C. *et al.* **Capability maturity model for software, version 1.1**. [S.l.]: Technical Report, Carnegie Mellon Software Engeneering Institute, 1993. Disponível em: <http://www.sei.cmu.edu/cmm/>. Acesso em: 21 jul. 2010.

PEIXOTO, Mario César Pintaudi. **Criando um CSIRT**: Computer Security Incident Response Team. Rio de Janeiro: Brasport, 2008.

PETTIGREW, A. **The politics of organizational decision making**. [S.l.]: Tavistok, 1973.

_____.; WHIPP, R. **Managing chance for competitive sucess**. [S.l.]: Blackwell, 1991.

PFARRER, Michael D. *et al.* Special Topic Forum on “Corruption in Organizations": After The Fall: Reintegration The Corrupt Organization. **The Academy Of Management Review (amr)**, Mississippi, v. 33, n. 3, p.730-749, 01 jul. 2008.

PINTO, Jonathan *et al*. Special Topic Forum on “Corruption in Organizations": Corrupt Organizations or Organizations of Corrupt Individuals? Two Types of Organization-Level Corruption. **The Academy Of Management Review (amr**), Mississippi, v. 33, n. 3, p.685-709, 01 jul. 2008.

PIRONTI, John P. Developing Metrics for Effective Information Security Governance. **Journal**, v. 2, 2007. Disponível em: <http://www.isaca.org.>. Acesso em: 01 mai 2010.

PONCHIROLLI, Osmar. **Capital humano**: sua importância na gestão estratégica do conhecimento. Curitiba: Juruá, 2005.

PORTER, Michael E. How competitive forces shape strategy. **Harvard Business Review**, p. 137-145, Nov./Dec., 1979.

_____. **Vantagem competitiva.** 14. ed. Rio de Janeiro: Campus, 1986.

_____.; MILLAR, V. How information gives you competitive advantage. **Harvard Business Review**, [S.l.] p.149-160, July/Aug, 1985.

PRICEWATERHOUSECOOPERS. **The 2011 Global State of Information Security Survey**. 2010. Disponível em*:* <http://www.pwc.com/gx/en/information-security-survey/pdf/giss-2011-survey-report.pdf>. Acesso em: 14 jun 2010.

_____. **Redefinindo o sucesso.** 5ª Edição da Pesquisa de Líderes Empresariais Brasileiros. 2009a. Disponível em: < http://www.pwc.com/pt_BR/br/ceo-survey-brazil/assets/5-pesq-lideres-09-graficos.pdf.> Acesso em: 15 fev 2010.

_____.**The global economic crime survey**. Economic Crime in a downturn. 2009b. Disponível em: < http://www.pwc.com/gx/en/economic-crime-survey/download-economic-crime-people-culture-controls.jhtml.> Acesso em: 10 ago 2010.

PRIETO, V. C.; CARVALHO, M. M. Análise das contribuições de diferentes modelos para o alinhamento estratégico. In: ENANPAD, 30., 2006. **Anais...** Salvador, 2006.

PUGH, D.S.; HICKSON, D.J. **Os teóricos das organizações.** Tradução de Afrânio Carvalho Aguiar *et al.* Rio de Janeiro: Qualitymark, 2004.

RATHNAM, R. *et al.* Alignment of business strategy and IT strategy**:** a case study of a fortune 50 financial services company. **Journal of Computer Information Systems**, [S.l.], Winter 2005.

REBOUÇAS, A. C.; BRAGA, B.; TUNDISI, J. G. **Águas doces no Brasil**: capital ecológico, uso e conservação. 2. ed. São Paulo: Escrituras, 2002.

REICH, B. H.; BENBASAT, I. Measuring the linkage between business and information technology objectives. **MIS Quarterly**, [S.l.], v.20, n.1, p.55-81, Mar. 1996.

REZENDE, Denis Alcides. **Planejamento estratégico para organizações privadas e públicas**: guia prático para elaboração do projeto de plano de negócios. Rio de Janeiro: Brasport, 2008.

RIBEIRO, Carla Andréa; ANDRADE Maria Eugênia Albino. **Governança informacional como sustentação das ações de combate à corrupção.** Caracas: [s.n.], 2004. (XVIII Concurso del CLAD sobre Reforma del Estado y Modernización de la Administración Pública "Cómo combatir la corrupción, garantizar la transparencia y rescatar la ética en la gestión gubernamental en Iberoamérica".).

SANDER, Peter. **Madoff**: a história da maior fraude financeira de sempre**.** Tradução de Alexandra Cardoso. Portugal: Centro Atlântico, 2009.

SANTOS JUNIOR, Arthur R.; FONSECA, Fernando S. S; COELHO, Paulo E. S. **Entendendo e implementando a Norma ABNT NBR ISO/IEC 17799:200:** aspectos teóricos e práticos para a implantação da Norma ABNT NBR ISO/IEC 17799:2005. [S.l.]: Academia Latino-Americana de Segurança da Informação, 2006. Disponível em: <http://www.technetbrasil.com.br/academia/provas/materiais/Apostila_ISO17799_Modulo1.pdf>. Acesso em: 20 jun 2010.

SARBANES-OXLEY ACT. **Public Company Accounting Reform and Investor Protection Act of 2002**. [S.l.] (EUA), 2002.

SÊMOLA, Marcos. **Gestão de segurança da informação.** Rio de Janeiro, Campus, 2003.

_____. **GRC na prática**: a nova abordagem de governança, gerenciamento de risco e conformidade. 30 jun. 2008 Disponível em: <http://idgnow.uol.com.br/seguranca/firewall/idgcoluna.2008-06-30.9839068825/>. Acesso em: 10 jun 2010.

SILVA, Marconi Oliveira. **Imagem e Verdade**. Jornalismo, linguagem e realidade. São Paulo: AnnaBlume, 2006.

STATDLOBER, Juliano. **Help-Desk e SAC com qualidade.** Rio de Janeiro: Brasport, 2006.

SVEIBY, K. E**. A nova riqueza das organizações.** São Paulo: Campus, 1998

SOLMS, R. Von; SOLMS, S. H. Von. Information security governance. **South Africa**, Springer 2008.

VENKATRAMAN, N.; CAMILLUS, J. C. Exploring the concept of “fit” in strategic management. **Academy of Management**, Briarcliff Manor, v.9, n.3, p. 513-525, July 1984.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 3. ed. São Paulo: Atlas, 2000.

_____. **Métodos de pesquisa em administração**. São Paulo: Atlas, 2005.

VIEIRA, Marcelo M. F.; ZOUAIN, Deborah M. **Pesquisa qualitativa em administração**. 2. ed. Rio de Janeiro: FGV, 2006.

WATKINS, Steve G. **ISO 27001 Pocket Guide**.[S.l.]: ITGP, 2007

WEBER, Max. **A ética protestante e o espírito do capitalismo**. Tradução de Pietro Nassetti. 2. ed. São Paulo: Martin Claret, 2007.

WEILL, P.; ROSS, J.W. **Governança de TI:** tecnologia da informação. São Paulo: Makron Books, 2006.

WESTERMAN, George; HUNTER, Richard. **O risco de TI**: convertendo ameaças aos negócios em vantagem competitiva. São Paulo: Makron Books, 2008.

WHITE, Paul; ISLAM, Sadar M. N. **Formulation of appropriate laws:** a new integrated multidisciplinary approach and an application to electronic funds transfer regulation. [S.l.], Australia: [s.n.], 2008.

WOLCOTT, Group. **Raising the standard of information security governance with ISO 27001.** Moving to an effective, efficient, and sustainable information security management system based on the ISO 27001 international standard. 2007. Disponível em:<http://www.wolcottgroup.com/documents/WG_ISO27001PoV_0607C2.pdf>. Acesso em: 10 jun 2010.

WOLFFENBUTTEL, A. **Marco regulatório**. 2007. Disponível em: <http://desafios2.ipea.gov.br/desafios/edicoes/19/artigo14917-1.php> . Acesso em: 01 set 2010.

YIN, R. K. **Case study research:** design an methods. 4. ed. [S.l.]: SAG Publications, 2009.

APÊNDICE A – Efetividade da GSI. Questões para executivos[20]

Questões para os Executivos – Por favor, justifique as respostas mesmo sucintamente!

1. O valor e a importância da segurança da informação são assimilados pela alta gestão?

Referencial Teórico: Sêmola (2008), Alves (2006)

2. A organização tem uma estratégia de segurança? Se assim for, é alinhada com a estratégia global de negócios? Esta também é alinhada à Tecnologia da Informação?

Referencial Teórico: ITGI (2006), Sêmola (2008), Alves (2006), Mintzberg (2003), Porter (1986), Henderson e Venkatraman (1993), Weill e Ross (2006);

3. O conselho compreende as potenciais responsabilidades da organização na caso de descumprimento da regulação? Entende também a potencial responsabilidade quando a informação sigilosa é comprometida?

Referencial Teórico: ITGI (2006), Andrade e Rossetti (2009), Lahti e Peterson (2006), Fernandes e Abreu (2008)

4. Se houve algum incidente grave de segurança, foi determinado o custo do incidente para a organização?

Referencial Teórico: Westerman e Hunter (2008), CGTF (2006) , Sêmola (2008)

5. A segurança da informação aparece como um item de pauta da diretoria? Há um cronograma para relatar o status do programa de segurança da informação para o conselho?

Referencial Teórico: Sêmola (2008), Alves (2006), CGTF (2006)

---

[20] Fonte: ITGI, 2006,p. 34, *tradução do autor*.
Nota: Adaptado pelo Autor.

6. Existe uma política de segurança da informação aprovada? É constantemente revisada?

Referencial Teórico: Campos (2007), Sêmola (2008), Alves (2006)

7. Pode a organização continuar a operar se a informação crítica ficar indisponível, comprometida ou perdida? Quais seriam as consequências de um incidente de segurança em termos de receitas, perda de clientes e confiança dos investidores?

Referencial Teórico: Westerman e Hunter (2008), Fernandes e Abreu (2008), Peixoto (2008)

8. A auditoria compreende claramente o seu papel na segurança da informação?

Referencial Teórico: Imoniana (2008), Lahti e Peterson (2006)

9. Existe um CISO (*Chief Information Security Officer*) ou funcionário especialmente encarregado da gestão de informação segurança na organização?

Referencial Teórico: Sêmola (2008), Fleury *et al*. (2002)

10. Há uma formação adequada e programas de conscientização para garantir que o pessoal está consciente das suas responsabilidades de segurança?

Referencial Teórico: Beal (2008), Westerman e Hunter (2008), Fleury *et al*. (2002)

APÊNDICE B – Efetividade da GSI. Questões para gestores[21]

Questões para a Gestão – Por favor, justifique as respostas mesmo sucintamente!

1. Como o conselho é informado das questões de segurança da informação? Quando foram passadas ao conselho as últimas instruções sobre riscos e melhoria no estado de segurança?

Referencial Teórico: Alves (2006), Sêmola (2008), Allen e Carnegie (2007)

2. As funções de segurança e responsabilidades são claramente definidas e comunicadas? Como?

Referencial Teórico: Alves (2006), CGTF (2006), Sêmola (2008)

3. A organização já teve sua segurança de rede controlada por uma terceiros?

Referencial Teórico: ITGI (2006), CGTF (2006), Beal (2008), Campos (2007)

4. Quando foi a última avaliação dos riscos feita baseada na criticidade e sensibilidade dos ativos de informações de segurança? Quando é a próxima avaliação de risco prevista?

Referencial Teórico: Westerman e Hunter (2008), Sêmola (2008), Alves (2006), Moeller (2008), Campos (2007)

5. A avaliação de risco considerou que a entidade possa continuar a funcionar se não estiver disponível a informação crítica, comprometida ou perdida? Foram consideradas as consequências de um incidente de segurança em termos de

---

[21] Fonte: ITGI, 2006, p. 34-35, *tradução do autor*.
Nota: Adaptado pelo Autor.

receitas, perda clientes e a confiança dos investidores? Foram determinadas quais as consequências haveria se a infra-estrutura torna-se inoperante?

Referencial Teórico: Westerman e Hunter (2008), CGTF (2006), Campos (2007) , Moeller (2008) , Campos (2007), Peixoto (2008)

6. O CEO pediu alguma avaliação de segurança da informação? Foram analisados os resultados dessa avaliação e foram comunicados ao conselho de administração?

Referencial Teórico: Campos (2007), Sêmola (2008), Alves (2006)

7. Existe um processo eficaz e testado para tratar da segurança da informação incidentes / emergências?

Referencial Teórico: Fernandes e Abreu (2008), Beal (2008), Westerman e Hunter (2008)

8. A avaliação de risco considera que os ativos de informação estão sujeitos a leis e regulamentos? Isto resulta em procedimentos adequados para assegurar cumprimento dessas leis e regulamentos?

Referencial Teórico: Westerman e Hunter (2008), Alves (2006), Fernandes e Abreu (2008), Moeller (2008), Campos (2007)

9. A informação sobre a avaliação de risco é um item na agenda regular de TI? Como isto acontece?

Referencial Teórico: ITGI (2006), Westerman e Hunter (2008), Alves (2006) , Campos (2007)

10. Existe um processo contínuo para garantir o alinhamento das informações de segurança com os objetivos de negócio? Como funciona?

Referencial Teórico:ITGI (2006),CGTF (2006),Sêmola (2008), Porter (1986), Alves (2006)

11. Como são feitos os programas de conscientização para garantir que o pessoal está consciente das suas responsabilidades de segurança e das expectativas da gestão?

Referencial Teórico: ITGI (2006), CGTF (2006), Westerman e Hunter (2008)

12. Existe um processo de classificação de ativos de informação para assegurar que ativos críticos estão adequadamente protegidos?

Referencial Teórico: Sêmola (2008), Alves (2006), Beal (2008)

13. A organização implementa controles de segurança física e lógica?

Referencial Teórico: Torres (2003), Santos (2007), Beal (2008)

14. A organização implementa práticas de segurança de mercado para implementar projetos de tecnologia desde o início dos mesmos? Quais são as práticas adotas? Estas práticas também são adotadas para aquisição ou desenvolvimento e manutenção de software?

Referencial Teórico: Torres (2003), Santos (2007), Beal (2008)

15. A organização implementa requisitos de segurança no gerenciamento de operações e comunicações, tais como gestão de mudanças, segregação de funções, segregação de ambientes de produção/homologação/desenvolvimento? Implementa ainda recursos de proteção de infra-estrutura tais como servidores e equipamentos de redes e teleprocessamento?

Referencial Teórico: Torres (2003), Santos (2007), Beal (2008)

16. Há um ISMS – *Information Security Management System Systems* (ISO/IEC 27001) implantado ou em implantação na organização?

Referencial Teórico: Sêmola (2003), Alves (2006), Beal (2008)

ANEXO A – Domínios do COBIT: gestão e processos de TI

QUADRO 36
Domínios do COBIT, questões gerenciais, processos de TI
(Continua – Parte I)

	Questões Gerenciais	Processos de TI
PO (Planejamento e Organização)	. A estratégia de negócio e a TI estão alinhadas?	. PO-1 -> Definir um plano estratégico para TI
	. A empresa está otimizando a utilização dos seus recursos?	. PO-2 -> Definir a arquitetura da informação
	. Todos na organização compreendem as metas de TI?	. PO-3 -> Determinar a direção tecnológica
	. Os riscos relacionados a TI estão compreendidos e sendo gerenciados?	. PO-4 -> Definir a organização de TI, os seus processos e relacionamentos
	. A qualidade dos sistemas de TI está adequada às necessidades do negócio?	. PO-5 -> Gerenciar o investimento em TI
		. PO-6 -> Comunicar objetivos e direcionamentos gerenciais
		. PO-7 -> Gerenciar os recursos humanos
		. PO-8 -> Gerenciar a qualidade
		. PO-9 -> Avaliar e gerenciar os riscos de TI
		. PO-10 -> Gerenciar projetos

QUADRO 36
Domínios do COBIT: gestão e processos de TI
(Continuação – Parte II)

	Questões Gerenciais	Processos de TI
AI (Aquisição e Implementação)	. Os novos projetos conseguem entregar soluções que atendem as necessidades do negócio?	. AI-1 -> Identificar soluções automatizadas
	. Os novos projetos conseguem ser entregues dentro do prazo e orçamento planejados?	. AI-2 -> Adquirir e manter software aplicativo
	. Os novos sistemas funcionam adequadamente depois de implementados?	. AI-3 -> Adquirir e manter infra-estrutura tecnológica
	. As mudanças são conduzidas com baixo impacto nas operações de negócios correntes?	. AI-4 -> Viabilizar operação e utilização
		. AI-5 -> Adquirir recursos de TI
		. AI-6 -> Gerenciar mudanças
		. AI-7 -> Instalar e aprovar soluções e mudanças
DS (Entrega e Suporte)	. Os serviços de TI estão sendo entregues com alinhamento às prioridades do negócio?	. DS-1 -> Definir e gerenciar níveis de serviço
	. Os custos de TI estão otimizados?	. DS-2 -> Gerenciar serviços terceirizados
	. As equipes de trabalho são capazes de utilizar os sistemas de TI com segurança e produtividade?	. DS-3 -> Gerenciar desempenho e capacidade
	. Atributos como confidencialidade, integridade e disponibilidade estão implementados de forma adequada?	. DS-4 -> Garantir a continuidade dos serviços
		. DS-5 -> Garantir a segurança dos sistemas

QUADRO 36
Domínios do COBIT: gestão e processos de TI
(Conclusão – Parte III)

	Questões Gerenciais	Processos de TI
DS (Entrega e Suporte)		. DS-6 -> Identificar e alocar custos
		. DS-7 -> Educar e treinar usuários
		. DS-8 -> Gerenciar central de serviços e incidentes
		. DS-9 -> Gerenciar a configuração
		. DS-10 -> Gerenciar problemas
		. DS-11 -> Gerenciar dados
		. DS-12 -> Gerenciar ambiente físico
		. DS-13 -> Gerenciar operações
	. As medições de desempenho de TI detectam problemas antes que seja tarde demais?	. ME-1 -> Monitorar e avaliar o desempenho da TI
ME (Monitoração e Avaliação)	. Há garantias de que os controles internos sejam eficazes?	. ME-2 -> Monitorar e avaliar os controles internos
	. É possível associar diretamente o desempenho de TI às metas de negócio estabelecidas anteriormente?	. ME-3 -> Assegurar conformidade com requisitos externos
	. Existem controles para confidencialidade, integridade e disponibilidade adequados para garantir a segurança das informação?	. ME-4 -> Fornecer governança para a TI

Fonte: FERNANDES; ABREU, 2008, p. 179-181.

ANEXO B – Cobertura do COBIT com a ISO/IEC 17799

QUADRO 37
Cobertura do COBIT com a ISO/IEC 17799

COBIT 4.0		COBERTURA ISO/IEC 17799
PO1	Definir um plano estratégico para TI	N/A
PO2	Definir a arquitetura da informação	A
PO3	Determinar a direção tecnológica	A
PO4	Definir a organização de TI, os seus processos e relacionamentos	A
PO5	Gerenciar o investimento de TI	A
PO6	Comunicar objetivos e direcionamentos gerenciais	A
PO7	Gerenciar recursos humanos	A
PO8	Gerenciar a qualidade	A
PO9	Avaliar e gerenciar riscos de TI	A
PO10	Gerenciar projetos	N/A
AI1	Identificar soluções automatizadas	A
AI2	Adquirir e manter software aplicativo	A
AI3	Adquirir e manter infra-estrutura tecnológica	A
AI4	Viabilizar operação e utilização	A
AI5	Adquirir recursos de TI	A
AI6	Gerenciar mudanças	A
AI7	Instalar e aprovar soluções e mudanças	A
DS1	Definir e gerenciar níveis de serviços	A
DS2	Gerenciar serviços terceirizados	A
DS3	Gerenciar desempenho e capacidade	A
DS4	Gerenciar a continuidade dos serviços	A
DS5	Garantir a segurança dos sistemas	C
DS6	Identificar e alocar custos	N/A
DS7	Educar e treinar usuários	A
DS8	Gerenciar central de serviços e incidentes	A
DS9	Gerenciar a configuração	A
DS10	Gerenciar problemas	A
DS11	Gerenciar dados	A
DS12	Gerenciar ambiente físico	A
DS13	Gerenciar operações	A
ME1	Monitorar e avaliar o desempenho da TI	A
ME2	Monitorar e avaliar os controles internos	A
ME3	Assegurar conformidade com requisitos externos	A
ME4	Fornecer a governança para a TI	A

Fonte: FERNANDES; ABREU, 2008, p. 420-421.
Nota: (A)Vários aspectos abordados; (C) Cobertura completa; (E)Excede; (N/A) Não se aplica.

ANEXO C – ISO/IEC 17799 X COBIT

QUADRO 38
ISO/IEC 17799 x COBIT

(Continua – Parte I)

NBR ISO/IEC 17799:2000	COBIT V.3
Introdução	
O que é segurança da informação	
Por que a segurança da informação é necessária	
Avaliando os riscos de segurança	PO 9.1 Avaliação de Risco do Negócio
	PO 9.2 Aproximação da Avaliação de Risco
	PO 9.3 Identificação do Risco
	PO 9.4 Mensuração do Risco
	PO 9.5 Plano de Ação do Risco
	PO 9.6 Aceitação dos Riscos
Seleção de controles	PO 9.7 Seleção das Medidas de Segurança
Ponto de partida para a segurança da informação	
Fatores críticos de sucesso	PO 9.8 Compromisso da Avaliação de Risco
Desenvolvendo suas próprias recomendações	
1. Objetivo	
2. Termos e definições	
3. Política de segurança	
3.1 Política de segurança da informação	PO 4 Define a Organização de TI e seus relacionamentos
	PO 6 Gerencia a Comunicação das Direções de TI
4. Segurança organizacional	
4.1 Infra-estrutura da segurança da informação	PO 4 Define a Organização de TI e seus relacionamentos
	PO 6 Gerencia a Comunicação das Direções de TI
	AI 6 Gerencia as Mudanças
	M 3 Provê Auditoria Independente

QUADRO 38
ISO/IEC 17799 x COBIT

(Continuação – Parte II)

NBR ISO/IEC 17799:2000	COBIT V.3
4.2 Segurança no acesso para prestadores de serviço	PO 9 Avaliar os Riscos
	DS2 Gerencia os Serviços de Terceiros
4.3 Terceirização	DS1 Define e mantém os acordos de níveis de serviço (SLA's)
	DS2 Gerencia os Serviços de Terceiros
5. Classificação e controle dos ativos de informação	
5.1 Contabilização dos ativos	PO 4 Define a Organização de TI e seus relacionamentos
	DS 9 Gerencia a Configuração
5.2 Classificação da informação	PO 2 Define a Arquitetura da Informação
	DS 5 Assegurar Segurança dos Serviços
6. Segurança em pessoas	
6.1 Segurança na definição e nos recursos de trabalho	PO 4 Define a Organização de TI e seus relacionamentos
	PO 7 Gerencia Recursos Humanos
	AI 1 Identifica Soluções de Automação
	DS2 Gerencia os Serviços de Terceiros
6.2 Treinamento dos usuários	PO 6 Gerencia a Comunicação das Direções de TI
	PO 7 Gerencia Recursos Humanos
	AI 5 Instala e Certifica Softwares
	DS 7 Treina os usuários
6.3 Respondendo aos incidentes de segurança e ao mau funcionamento	DS 10 Gerencia os Problemas e Incidentes
7. Segurança física e do ambiente	
7.1 Areas de Segurança	DS 12 Gerencia a Infra-Estrutura
7.2 Segurança dos equipamentos	AI 3 Adquire e mantém a infra-estrutura tecnológica
	DS 5 Assegurar Segurança dos Serviços
	DS 12 Gerencia a Infra-Estrutura
7.3 Controles gerais	
8. Gerenciamento das operações e comunicações	

QUADRO 38
ISO/IEC 17799 x COBIT

(Continuação – Parte III)

NBR ISO/IEC 17799:2000	COBIT V.3
8.1 Procedimentos e responsabilidades operacionais	
8.1.1 Documentação dos procedimentos de operação	AI 4 Desenvolve e mantém os procedimentos
	DS 10 Gerencia os Problemas e Incidentes
	DS 11 Gerencia os Dados
	DS 13 Gerencia as Operações
8.1.2 Controle de mudanças operacionais	AI 6 Gerencia as Mudanças
8.1.3 Procedimentos para o gerenciamento de incidentes	DS 10 Gerencia os Problemas e Incidentes
8.1.4 Segregação de funções	PO 4 Define a Organização de TI e seus relacionamentos
8.1.5 Separação dos ambientes de desenvolvimento e de produção	AI 5 Instala e Certifica Softwares
8.1.6 Gestão de recursos terceirizados	PO 4 Define a Organização de TI e seus relacionamentos
	PO 11 Gerencia a Qualidade
	AI 1 Identifica Soluções de Automação
8.2 Planejamento e aceitação dos sistemas	DS 3 Gerencia o Desempenho e Capacidade do Ambiente
8.3 Proteção contra o software malicioso	AI 3 Adquire e mantém a infra-estrutura tecnológica
	AI 5 Instala e Certifica Softwares
	DS 5 Assegurar Segurança dos Serviços
8.4 Housekeeping	DS 10 Gerencia os Problemas e Incidentes
	DS 11 Gerencia os Dados
	DS 13 Gerencia as Operações
8.5 Gerenciamento da rede	DS 9 Gerencia a Configuração
	M 2 Analisa a adequação dos controles internos
8.6 Segurança e tratamento de mídias	PO 11 Gerencia a Qualidade
	DS 11 Gerencia os Dados
8.7 Troca de informações e software	PO 8 Assegura o alinhamento de TI com os requerimentos externos

QUADRO 38
ISO/IEC 17799 x COBIT

(Continuação – Parte IV)

NBR ISO/IEC 17799:2000	COBIT V.3
	AI 1 Identifica Soluções de Automação
	DS 1 Define e mantém os acordos de níveis de serviço
	DS 11 Gerencia os Dados
9 Controle de acesso	
9.1 Requisitos do negócio para controle de acesso	DS 5 Assegurar Segurança dos Serviços
9.2 Gerenciamento de acessos do usuário	DS 5 Assegurar Segurança dos Serviços
	DS 9 Gerencia a Configuração
	M 2 Analisa a adequação dos controles internos
9.3 Responsabilidade do usuário	DS 5 Assegurar Segurança dos Serviços
9.4 Controle de acesso a rede	DS 5 Assegurar Segurança dos Serviços
9.5 Controle de acesso ao sistema operacional	DS 5 Assegurar Segurança dos Serviços
9.6 Controle de acesso às aplicações	DS 5 Assegurar Segurança dos Serviços
9.7 Monitoração do uso e acesso ao sistema	AI 3 Adquire e mantém a infra-estrutura tecnológica
	DS 5 Assegurar Segurança dos Serviços
	DS 13 Gerencia as Operações
	M 1 Monitora os Processos
9.8 Computação móvel e trabalho remoto	DS 9 Gerencia a Configuração
	DS 11 Gerencia os Dados
	DS 12 Gerencia a Infra-Estrutura
	DS 13 Gerencia as Operações
10 Desenvolvimento e manutenção de sistemas	
10.1 Requisitos de segurança de sistemas	PO 11 Gerencia a Qualidade
	DS 5 Assegurar Segurança dos Serviços
10.2 Segurança nos sistemas de aplicação	PO 11 Gerencia a Qualidade
	AI 3 Adquire e mantém a infra-estrutura tecnológica
	DS 5 Assegurar Segurança dos Serviços

QUADRO 38
ISO/IEC 17799 x COBIT
(Continuação – Parte V)

NBR ISO/IEC 17799:2000	COBIT V.3
	DS 11 Gerencia os Dados
10.3 Controle de criptografia	DS 5 Assegurar Segurança dos Serviços
	DS 11 Gerencia os Dados
10.4 Segurança de arquivos do sistema	PO 10 Gerencia de projetos
	AI 5 Instala e Certifica Softwares
	DS 11 Gerencia os Dados
10.5 Segurança nos processos de desenvolvimento e suporte	AI 1 Identifica Soluçoes de Automação
	AI 2 Adquire e Mantém os Softwares
	AI 5 Instala e Certifica Softwares
	AI 6 Gerencia as Mudanças
	DS 5 Assegurar Segurança dos Serviços
11 Gestão da continuidade do negócio	
11.1 Aspectos da gestão da continuidade do negócio	PO 3 Determina a direção tecnológica
	PO 7 Gerencia Recursos Humanos
	DS 2 Gerencia Serviços de Terceiros
	DS 4 Assegura a continuidade dos serviços
	DS 12 Gerencia a Infra-Estrutura
	DS 13 Gerencia as Operações
12 Conformidade	
12.1 Conformidade com requisitos legais	PO 6 Gerencia a Comunicação das Direções de TI
	PO 8 Assegura o alinhamento de TI com os requerimentos externos
	DS 11 Gerencia os Dados
	M1 Monitora os Processos
	M3 Prove Auditorias Independentes

QUADRO 38
ISO/IEC 17799 x COBIT

(Conclusão – Parte VI)

NBR ISO/IEC 17799:2000	**COBIT V.3**
12.2 Análise critica da política de segurança e da conformidade técnica	PO 6 Gerencia a Comunicação das Direções de TI
	PO 11 Gerencia a Qualidade
	AI 2 Adquire e Mantém os Softwares
12.3 Considerações quanto à auditoria de sistemas	AI 1 Identifica Soluções de Automação

Fonte: ALVES, 2006, p. 102-106.