UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM MODELO FASEADO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

LEANDRO RAMALHO FRÓIO

ORIENTADOR: ANDERSON CLAYTON ALVES NASCIMENTO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.DM – 361/08

BRASÍLIA/DF: DEZEMBRO – 2008

FICHA CATALOGRÁFICA

FROIO, LEANDRO RAMALHO
Um Modelo Faseado de Gestão da Segurança da Informação [Distrito Federal] 2008.
xvii, 134p., 210 x 297 mm (ENE/FT/UnB, Mestre, Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia).
Departamento de Engenharia Elétrica
1.Segurança da Informação 2.Gestão da Segurança da Informação
3.Modelo de Gestão 4.Tecnologia da Informação
I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

FROIO, L. R. (2008). Um Modelo Faseado de Gestão da Segurança da Informação. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM-361/08, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 134p.

CESSÃO DE DIREITOS

AUTOR: Leandro Ramalho Fróio.

TÍTULO: Um Modelo Faseado de Gestão da Segurança da Informação.

GRAU: Mestre ANO: 2008

_____

Leandro Ramalho Fróio
Qd. 301, Alameda Gravatá, Conjunto 18, Águas Claras
71904-180 – Brasília – DF – Brasil.

AGRADECIMENTOS

Aos meus pais pelo carinho e ensinamentos, sem os quais, jamais encontraria motivação para conclusão desta obra.

À minha irmã pela paciência e dedicação nos trabalhos de revisão, sem a qual, muitas idéias não teriam tomado forma.

À Carla pela compreensão, carinho e apoio em todos os momentos, sem a qual, muitos desafios não teriam sido superados.

Ao meu Orientador, Anderson Nascimento, que apesar das diferenças acadêmicas, soube respeitá-las, acreditou na idéia desta obra e me incentivou a seguir os meus caminhos.

Aos membros do Núcleo de Segurança da Informação da Agência Nacional de Transportes Terrestres (Jece Janer, Jean-Claude Seillier, Paulo Perez e Juliana Gonçalves) pelos ensinamentos e trabalhos, que contribuíram significativamente para o desenvolvimento desta obra. Em especial à Juliana Gonçalves pela paciência nos trabalhos de revisão desta obra, e por me ensinar que parágrafos devem ser curtos, com começo, meio e fim.

Ao Prof. Ian Webster pelos ensinamentos e amizade, verdadeiro co-orientador desta obra, que apenas por razões de regulamentação não pôde ser registrado formalmente como tal.

Ao Prof. Rafael Timóteo de Sousa Júnior pelos ensinamentos e amizade, que tiveram contribuição única nesta obra.

A todos meus amigos pelo apoio, e em especial ao Marcos Baeta, Rafael Araújo, Silvio Yamanaka e Walter Ferreira, pela atenção dispensada na leitura e debates sobre o tema, que propiciaram o aprimoramento desta obra.

À Universidade de Brasília pela presteza e colaboração.

A Deus pelas oportunidades oferecidas.

A todos, o meu sincero muito obrigado!

Dedico este trabalho aos meus avós
paternos, que deixaram muita saudade.

RESUMO

UM MODELO FASEADO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Autor: Leandro Ramalho Fróio
Orientador: Anderson Clayton Alves Nascimento
Programa de Pós-graduação em Engenharia Elétrica
Brasília, Dezembro de 2008

As práticas de Segurança da Informação não são recentes, no entanto, diversos fatores contribuíram para a necessidade de métodos capazes de planejar, coordenar, integrar e controlar tais práticas, visando alinhá-las aos objetivos do negócio da organização.

Observamos que as práticas de Segurança da Informação tendem a evoluir de atividades pontuais e descoordenadas para uma posição sistemática e estratégica dentro das organizações, exigindo o uso e desenvolvimento de metodologias capazes de lidar com diferentes questões, que não somente aquelas relacionadas à tecnologia.

Diante destes desafios surgem os modelos de Gestão da Segurança da Informação (GSI), que visam sistematizar e organizar a aplicação das práticas de Segurança da Informação para que os negócios das organizações estejam seguros e seus objetivos sejam alcançados com sucesso.

Os Modelos de Gestão da Segurança da Informação foram os objetos de estudo deste trabalho, no qual identificamos as suas diferenças e deficiências que comprometeriam o sucesso da GSI nas organizações.

Além disso, apresentaremos um Modelo Faseado de Gestão da Segurança da Informação capaz de endereçar, de maneira mais ampla, as questões de Segurança da Informação.

ABSTRACT

A PHASED INFORMATION SECURITY MANAGEMENT MODEL

Author: Leandro Ramalho Fróio

Supervisor: Anderson Clayton Alves Nascimento

Programa de Pós-graduação em Engenharia Elétrica

Brasília, December 2008

The Information Security Practices are not recent, however, many factors has contributed to the need of methodologies capable to plan, coordinate, integrate and control those practices, which aim to align them with the business's objectives of the companies.

We notice that those Information Security Practices has being migrating from isolated and uncoordinated practices to a systematic and strategic position inside the companies, demanding the use and the development of methodologies capable to handle with different questions, not only those related to technology.

These challenges motivate the development of Information Security Management Models, which aim to systematic and organize the application of the information security practices to assurance that the companies' business will be safe, and their objectives will be successful achieved.

The Information Security Management Models were the object of study of this work, at which we identified the main differences and deficiencies that compromises the success of the ISM in the companies.

We will present a Phased Information Security Management Model capable to address the questions related to information security.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

CGI	Comitê Gestor da Internet no Brasil
CISM	*Certified Information Security Manager*
CMM	*Capability Maturity Model*
COBIT	*Control Objectives for Information and related Tecnology*
GSI	Gestão da Segurança da Informação
HIPAA	*Health Insurance Portability and Accountability Act*
ISACA	*Information Systems Audit and Control Association*
ISM3	*Information Security Management Maturity Model*
ISMS	*Information Security Management System*
ISO	*International Organization for Standardization*
ISSEA	*International Systems Security Engineering Association*
ITGI	*IT Governance Institute*
ITIL	*Information Tecnology Infrastructure Library*
NIST	*National Institute of Standards and Tecnology*
PDCA	*Plan - Do - Check - Act*
PSI	Política de Segurança da Informação
RFC	*Request For Comments*
SI	Segurança da Informação
SOX	*Sarbanes-Oxley*
SSE-CMM	*Systems Security Engineering - Capability Maturity Model*
TIC	Tecnologia da Informação e Comunicação

1. INTRODUÇÃO

A disseminação do uso de computadores em diversas áreas de negócios, a ampliação da capacidade de comunicação e interação entre os sistemas, a substituição de redes isoladas por redes convergentes, e a evolução de redes fixas para redes móveis, vem proporcionando aos usuários, clientes, investidores, executivos e pesquisadores, comunicação contínua e em qualquer local, possibilitando diversas maneiras de acesso à informação. Como conseqüência, verifica-se que a natureza e a sensibilidade das informações mudaram significativamente, concomitantes com a variedade de vulnerabilidades e riscos a que estão expostas. Neste cenário, soluções para gerenciar, controlar e garantir o acesso à informação são essenciais, juntamente com programas de desenvolvimento da gestão da segurança da informação e meios de avaliar o nível de segurança da organização.

Certamente a prática de proteção da informação é tão antiga quanto a existência das sociedades. Na Grécia antiga, por exemplo, o conhecimento era restrito a grupos, como forma de proteger os valores sociais e culturais, além disso, a proteção de informações servia como estratégia de guerra (MOSSE, 1985). No entanto, a segurança da informação tomou dimensões maiores com o avanço da tecnologia e, em alguns momentos, se confunde com as práticas de segurança de computadores. Entretanto, conforme apresentado por Cheswick e Bellovin (1994, p. 08), “é importante considerar que segurança de computadores não é um objetivo, é um meio de alcançar um objetivo, o qual é a segurança da informação”.

No ano de 1967 o Departamento de Defesa dos Estados Unidos publicava o documento *Security Control for Computer System: Report of Defense Science Board Task Force on computer Security*, como uma iniciativa para controlar o acesso e proteger as informações contidas em sistemas de computadores de múltiplos acessos. Este documento marcou o início dos trabalhos oficiais de padronização da segurança da informação, segundo Gonçalves (2003).

Posteriormente, outras pesquisas sobre o assunto foram publicadas como *Trusted Computer Evaluation Criteria - DoD 5200.28-STD*, conhecido como *The Orange Book*, e *Computer Security Act of 1987*. Este possuía a finalidade de garantir a privacidade das informações nos sistemas de computadores do governo norte americano, conforme segue:

> *(b) SPECIFIC PURPOSES.-The purposes of this Act are--*

> *(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;* (ESTADOS UNIDOS DA AMÉRICA, 1988, Sec. 02)

Seguindo a tendência, o Governo Federal Brasileiro instituiu em 8 de janeiro de 1991 a Lei nº 8.159 que "dispõe sobre a política nacional de arquivos públicos e privados a fim de definir e assegurar o sigilo de documentos" (BRASIL, 1991, p. 01). Posteriormente a esta Lei, o Decreto nº 3.505 de 13 de junho de 2000 institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, cujos pressupostos básicos vão além das práticas de sigilo da informação e dotam a administração federal de instrumentos que permitem a implantação de um modelo de segurança da informação amplo. Os pressupostos básicos do Decreto são:

> I. assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
> II. proteção de assuntos que mereçam tratamento especial;
> III. capacitação dos segmentos das tecnologias sensíveis;
> IV. uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duas;
> V. criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
> VI. capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e
> VII. conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade. (BRASIL, 2002, p. 01)

Incluí-se nas ações do Governo Federal Brasileiro a criação do Comitê Gestor da Internet no Brasil, CGI, instituído por meio da Portaria Interministerial nº 147 de 31 de maio de 1995 e alterada pelo Decreto nº 4.829 de 3 de setembro de 2003, para coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.

Dentre os trabalhos do CGI está a publicação das Práticas de Segurança para Administradores de Redes Internet, que reúne um conjunto de boas práticas em configuração, administração e operação segura de redes conectadas à Internet, mas "é importante frisar que este conjunto representa o mínimo indispensável dentro de um grande universo de boas

práticas de segurança, o que equivale a dizer que a sua adoção é um bom começo, mas não necessariamente o suficiente em todas as situações" (BRASIL, CGI, 2003, p. 01).

Outra ação importante do Governo Federal Brasileiro foi a sansão do Decreto nº 4.553 de 27 de dezembro de 2002, que "dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal" (BRASIL, 2002, p. 01), e fornece diretrizes para implantação de ações de segurança da informação, introduzindo definições de Autenticidade, Disponibilidade e Integridade, um marco importante para a Política de Segurança da Informação nacional.

Trabalhos correntes demonstram que as práticas de Segurança da Informação tendem a evoluir de atividades pontuais e descoordenadas para uma posição sistemática e estratégica dentro das organizações (INSTITUTE OF INTERNAL AUDITORS, 2001) e (VON SOLMS, 2000). Os esforços em Segurança da Informação visam integrar as decisões de negócio e alinhar seus objetivos aos objetivos das organizações. Observa-se ainda que a responsabilidade pelo Gerenciamento da Segurança da Informação extrapola os limites de um único departamento e incorpora a cultura e os objetivos das organizações e governos.

Esta tendência sofre uma acentuada aceleração quando normas e leis são impostas às organizações, exigindo delas transparência no trato dos negócios e atribuindo aos seus executivos as responsabilidades pela segurança da informação. Dentre essas normas, se destacam a Lei norte-americana Sarbanes-Oxley (EUA, SOX, 2002) e o Acordo de Capitais da Basiléia (BASEL II, 2004), ambas originárias após os escândalos fiscais envolvendo gigantes americanas de energia e telecomunicações[1].

A Lei SOX impõe um nível elevado de responsabilidade sobre os executivos das organizações pela veracidade do conteúdo dos relatórios financeiros, exigindo na Sessão 409, por exemplo, informações financeiras de forma rápida e em bases atuais. Apesar de ser uma lei norte-americana, afeta todas as empresas do mundo de capital aberto com negociações no mercado financeiro de ações norte-americano.

O acordo BASILÉIA II foi criado pelo Comitê de Supervisão Bancária de Basiléia, composto por autoridades de supervisão bancária e bancos centrais dos países G-10 (Bélgica,

[1] A Enron, gigante americana do setor de energia, pediu concordata em dezembro de 2001 após ter sido alvo de uma série de denúncias de fraudes contábeis e fiscais, com uma dívida de quase 13 bilhões de dólares. Outras empresas americanas também foram indiciadas em fraudes fiscais, como a Tyco, WorldCom, Qwest Communications e Global Crossing.

Canadá, França, Alemanha, Itália, Japão Luxemburgo, Suécia, Reino Unido, Suíça e Estados Unidos), e visa proteger o sistema financeiro internacional de problemas que o levem ao colapso utilizando para isso, de maneira sucinta, a gestão de capital e de riscos.

Os benefícios de implantar, gerenciar e controlar a segurança da informação nas organizações transpõe as características de privacidade inicialmente pretendidas e agregam propriedades que auxiliam as organizações a alcançarem seus objetivos. Isto possibilita que os serviços e negócios sejam executados em qualquer situação operacional, que as comunicações com fornecedores e clientes sejam eficientes, que as informações sensíveis tenham tratamentos diferenciados, que os investimentos para proteger a informação sejam compatíveis com as necessidades da organização e com o valor da informação. Além disso, permite que a organização se adéqüe às legislações e códigos de ética vigentes, mantendo sua imagem íntegra e transparente para investidores, auditores e sociedade.

Diante destes desafios surgem os modelos de Gestão da Segurança da Informação (GSI), que visam sistematizar e organizar a aplicação das práticas de Segurança da Informação para que os negócios das organizações estejam seguros e seus objetivos sejam alcançados com sucesso. Os modelos de Gestão da Segurança da Informação serão os objetos de estudo deste trabalho.

A motivação, os objetivos e a metodologia deste trabalho serão apresentados no capítulo 2.

No capítulo 3 faremos um estudo das diferentes orientações de Gestão da Segurança da Informação e das suas características marcantes. Ainda no capítulo 3, faremos uma delimitação do que seriam os elementos de Gestão da Segurança da Informação, e criaremos uma base de comparação para análise de modelos de GSI.

No capítulo 4 faremos uma análise crítica dos modelos atuais e mais utilizados de Gestão da Segurança da Informação.

No capítulo 5 apresentaremos a nossa proposta de Modelo de Gestão da Segurança da Informação, e no capítulo 6, realizaremos uma comparação do modelo proposto com os modelos atuais, utilizando a mesma base de comparação definida no capítulo 3.

O capítulo 7 é reservado às conclusões e às apresentações dos trabalhos futuros.

2. APRESENTAÇÃO DO TRABALHO

Neste capítulo apresentaremos os motivadores que levaram ao desenvolvimento deste trabalho, assim como apresentaremos os seus objetivos. Além disso, descreveremos a metodologia utilizada para abordar o problema aqui descrito e como pretendemos atingir nossos objetivos.

2.1. MOTIVAÇÃO

A Gestão da Segurança da Informação deve assessorar e nortear as decisões da organização, além de prover e manter níveis necessários de segurança para que a organização funcione, se desenvolva e alcance seus objetivos. Desta forma, é imprescindível que os objetivos da GSI estejam alinhados aos objetivos do negócio, garantindo que os investimentos em segurança sejam compatíveis com os valores e as necessidades da organização.

Entretanto, determinar as necessidades de segurança da organização e realizar investimentos em soluções não são suficientes para garantir a eficiência ou o sucesso da GSI, é preciso que haja gerenciamento das atividades de segurança. Conforme apresentado por Baker e Wallace (2007, p. 37), "pode-se responder SIM em um questionário que pergunta se são utilizados *softwares* antivírus na organização, quando na realidade o *software* pode estar mal configurado, mantido de forma inadequada e instalado somente em algumas estações".

Análises de pesquisas[2] sobre a natureza dos incidentes em segurança da informação nos permitem observar que as perdas financeiras das organizações resultam tanto de vulnerabilidades técnicas, como de falhas em procedimentos de gestão, falta de conformidade com as leis e despreparo dos profissionais da organização.

Tais análises são ainda mais preocupantes quando observado que quase 99% das organizações utilizam algum tipo de tecnologia ou metodologia de segurança, mas, quase todas elas sofreram algum tipo de perda decorrente de falta de gestão da segurança de informação (MODULO SECURITY, 2006) e (COMPUTER SECURITY INSTITUTE, 2006).

[2] Pesquisas realizadas por MODULO SECURITY (2003), MODULO SECURITY (2006), COMPUTER SECURITY INSTITUTE (2007) e CERT (2007).

Desta forma, é importante entender e conhecer os elementos que compõem a segurança da informação para seja possível endereçar as questões de segurança necessárias ao sucesso do negócio, e evitar o uso descoordenado de práticas ou tecnologias.

Observando o caso do Brasil, por exemplo, de acordo com a Nona Pesquisa Nacional de Segurança da Informação[3], o padrão ISO/IEC 17799:2005 foi o modelo de Gestão da Segurança da Informação mais utilizado no Brasil em 2003, seguido dos decretos federais e do modelo de governança CobiT. No entanto, Sanchéz, ao comentar sobre o padrão ISO/IEC 17799:2005, destaca:

> Apesar da relevância internacional do padrão ISO/IEC 17799:2005, não se pode afirmar que ele provê uma arquitetura de gerenciamento da segurança da informação, mas uma série de controles que podem ser utilizados como guia na condução de uma revisão detalhada da situação de segurança dos sistemas. (2006, p. ?)

Além disso, apesar do padrão ISO/IEC 17799:2005 e dos decretos federais oferecerem diretrizes e estabelecerem controles que agregam segurança, sua aplicação isolada não garante proteção aos negócios das organizações, conforme apresentado pelo padrão ISO/IEC 17799:2005:

> Deve-se ter em mente que nenhum conjunto de controles pode alcançar uma segurança completa, e que ações adicionais de gerenciamento devem ser implementadas para monitorar, desenvolver e melhorar a eficiência e a efetividade dos controles de segurança, visando alcançar os objetivos da organização. (2005, p. 06)

O CobiT apresenta uma abordagem diferente e mais complexa daquela utilizada pelo padrão ISO/IEC. Dentre as principais diferenças estão a utilização de processos para estruturação das atividades e a existência de uma arquitetura de mensuração do nível de alinhamento dos processos com os objetivos do negócio. Ademais, o CobiT é um modelo específico de Governança da Tecnologia da Informação, e por isso, conforme apresentado por Von Solms (2005a, p. 100-101), "há a necessidade de guias mais específicos sobre segurança da informação, principalmente nos níveis operacionais".

Existem outros modelos, como o ISM3 e o SSE-CMM, que não constam na lista de modelos utilizados no Brasil. No entanto, mesmo estes modelos não oferecem um completo

[3] Pesquisa realizada pela empresa Modulo Security entre março e agosto de 2003 no Brasil, publicada em outubro de 2003. Os dados foram coletados por meio de questionários presenciais e on-line, totalizando 682 questionários. Foram ouvidos profissionais das áreas de Tecnologia e Segurança da Informação, distribuídos pelos diferentes setores da economia, correspondendo à metade das mil maiores empresas brasileiras. Disponível em http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf, acesso em 20 nov 2007.

alinhamento dos objetivos da Gestão da Segurança da Informação com os objetivos do negócio. De maneira geral, o ISM3 apresenta uma série de atividades de segurança que devem ser realizadas a fim de que a organização esteja em determinados níveis de maturidade. Assim, o modelo acaba desconsiderando a necessidade de segurança da organização, já que determina quais atividades devem ser realizadas.

O modelo SSE-CMM é específico para o desenvolvimento de sistemas seguros. Sendo assim, desde que o negócio da organização seja serviços de software, o modelo é útil para a Gestão da Segurança a Informação e apresenta um alinhamento com os objetivos do negócio. Do contrário, o modelo não é amplo o suficiente para realizar a Gestão da Segurança da Informação.

Faremos uma apresentação mais detalhada desses modelos no Capítulo 4, no entanto, há um consenso que, isoladamente, eles não proporcionam um completo alinhamento dos objetivos da GSI aos objetivos de negócio.

Para tentar solucionar essa deficiência, diversos estudos sobre a GSI propõem a integração entre diversos modelos. Gustavo Alberto de Oliveira Alves (2006), por exemplo, propõem a integração do modelo CobiT e dos objetivos estratégicos e indicadores do *Balanced Scored Card* com o padrão ISO/IEC 17799:2005 como uma forma de compor um modelo de GSI, cujos objetivos estejam alinhados aos objetivos de negócio.

Sanchéz (2006) propõe o estabelecimento de mecanismos de controle e avaliação das práticas do padrão ISO/IEC 17799:2005 através de metodologia de gerenciamento em aspiral, criando um ciclo de implantação da GSI. Chapin e Akridge (2005), por usa vez, propõem a integração de modelos de maturidades e das práticas do padrão ISO/IEC 17799:2005 como meio de mensurar e avaliar o nível de segurança das organizações.

No entanto, a aplicação de diversas metodologias requer que as organizações já possuam conhecimentos amadurecidos sobre elas, além de esforços e investimentos para manter uma estrutura complexa de gestão.

Não é somente na literatura acadêmica que encontramos esforços para realizar a integração de modelos e metodologias de segurança. Uma pesquisa realizada pelo *Enterprise Strategy Group* (ESG, 2008), demonstrou que setenta e dois por cento das grandes companhias[4] norte-americanas utilizam mais de um modelo de Gestão da Segurança da Informação. Os motivos aparentam ser as necessidades de conformidade com inúmeras

[4] Organizações com mais de 1 mil funcionários.

regulamentações que atingem setores distintos dentro da organização, além de necessidade de cooperação e colaboração entre as áreas de negócio e segurança. Por isso, o uso de diversos modelos permitiria abranger diferentes áreas da segurança da informação e endereçar as questões de conformidade.

Neste cenário, podemos observar que a busca por proteção das informações e conformidade com as regulamentações, entre outros, têm feito com que as organizações adotem diversas ferramentas tecnológicas e metodologias de gestão. No entanto, estas composições tendem a ser complexas e custosas, prejudicando, por exemplo, organizações de pequeno porte ou com limitações orçamentárias, as quais também possuem necessidades de proteção da informação. Por essas razões, talvez o uso de inúmeras ferramentas tecnológicas ou metodologias de gestão não seja a solução mais viável ou exeqüível.

Desta forma, existe a necessidade de identificação e desenvolvimento de modelos de Gestão da Segurança da Informação simples e eficientes, capazes de alinhar as práticas de segurança aos objetivos do negócio, indiferente do porte ou do volume de investimentos das organizações.

2.2. OBJETIVOS

Este trabalho tem como objetivo propor um modelo faseado de Gestão de Segurança da Informação, alinhado aos objetivos do negócio e capaz de integrar e endereçar os Elementos Gerais de GSI.

Este trabalho também pretende analisar e comparar os modelos atuais de Gestão da Segurança da Informação, ISO/IEC 17799:2005, CobiT, ITIL, SSE-CMM, ISM3 e ISO/IEC 27001:2005, buscando identificar as suas diferenças e deficiências que comprometeriam o sucesso da GSI nas organizações.

2.3. METODOLOGIA

Faremos uma pesquisa através da literatura para identificarmos os modelos que são utilizados atualmente para a Gestão da Segurança da Informação, de tal forma que possamos

utilizá-los nas nossas análises e comparações dos modelos atuais de GSI. Consideraremos apenas os modelos amplamente utilizados e listados em pesquisas de mercado, como aquela realizada pela empresa Módulo Security (2006) no Brasil.

Para que seja possível analisar e comparar modelos com abordagens distintas de Segurança da Informação, é importante que seja estabelecido uma base de comparação. Imaginemos, por exemplo, que a característica marcante de dois modelos de GSI distintos seja a listagem de uma série de práticas de segurança, algo como um *checklist*. Desta forma, ao invés de compararmos o conteúdo da lista de cada modelo, basta identificarmos a finalidade da lista e a forma como o modelo realiza a Gestão da Segurança da Informação, que neste caso é por meio de um *checklist* de atividades.

Realizaremos um estudo para identificar as diferentes orientações de Gestão da Segurança da Informação e quais as suas características marcantes. Este estudo permitirá entender a maneira como os modelos abordam a GSI. Além disso, faremos uma delimitação do que seriam os Elementos Gerais de Gestão da Segurança da Informação, e então, com base nesses elementos, criaremos a base de comparação para análise dos modelos atuais de GSI.

De maneira geral, procuraremos identificar quais componentes um modelo de Gestão da Segurança da Informação deve possuir para que consiga abordar as questões que envolvem a Segurança da Informação nas organizações.

Faremos uma proposta de um Modelo Faseado de GSI, buscando abordar os Elementos Gerais de GSI.

3. UMA VISÃO GERAL DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Neste capítulo, faremos uma apresentação geral de Gestão da Segurança da Informação, abordando diversas orientações. O conhecimento sobre as orientações de GSI nos permitirá estabelecer elementos de comparação entre modelos distintos de GSI e identificar suas características marcantes.

Não obstante, faremos um estudo dos Elementos Gerais que devem ser endereçados pela Gestão da Segurança da Informação a fim de que os objetivos da GSI estejam alinhados aos objetivos do negócio e que as necessidades de segurança da organização sejam tratadas.

3.1. TERMINOLOGIA

De acordo com Harris (2004), Gestão da Segurança da Informação é um programa ou uma estrutura composta por procedimentos de segurança, cujo objetivo é proteger a organização e seus ativos[5]. Para o autor, a Gestão da Segurança da Informação deve definir o que é valioso para a organização, o que deve ser protegido e quais as conseqüências pela falta de conformidade com legislações. Além disso, Harris aponta que uma boa Gestão da Segurança da Informação é aquela que é planejada, implantada e mantida de acordo com as necessidades e os objetivos da organização.

De acordo com a Publicação Especial do NIST, SP 800-100 (EUA, NIST, 2006), Gestão da Segurança da Informação é um processo de estabelecimento e manutenção de uma arquitetura de gestão que assegura que as estratégias de proteção da informação estarão alinhadas aos objetivos do negócio e também o suportarão, além de assegurar que tais estratégias estarão em conformidade com lei e regulamentações, por meio de políticas e controles internos, e que garante a existência de responsabilidades.

Para Canal (2007), Gestão da Segurança da Informação são práticas que visam prevenir e mitigar ataques, erros e acidentes que impactam negativamente os sistemas de segurança da informação e os processos organizacionais suportados por eles.

[5] De acordo com o *International Accounting Standards Board*, ativo é tudo aquilo que tem valor para a organização. Disponível em http://www.iasb.org , acesso em 05 nov 2007. Definição similar pode ser encontrada no padrão ISO/IEC 13335-1:2004 (ISO, 2004).

Observa-se nas definições apresentadas sobre Gestão da Segurança da Informação a relação de alinhamento entre as práticas de segurança e as necessidades de proteção da organização, visando alcançar os objetivos do negócio. No entanto, tais definições não demarcaram o que seriam as práticas de gestão de segurança, assim como não definiram o que seriam informações e qual a relação entre estas e o negócio da organização.

Por isso, como uma primeira contribuição, faremos uma análise dos termos *Informação*, *Segurança* e *Gestão*, visando delimitar o conceito e expor nosso entendimento sobre Gestão da Segurança da Informação.

O termo *informação*, conforme apresentado por Mcgarry (1993), é conceituado de modos distintos por diferentes áreas de estudos como biblioteconomia, informática e engenharia, e que, de maneira genérica, remete à noção de comunicação, transmissão de dados, notícias, assuntos contidos em textos ou documentos, conhecimentos, e conteúdo de permuta. Muito embora, é aceito que *dado, informação, conhecimento e sabedoria* são elementos distintos e estão dispostos em uma hierarquia conhecida como DIKW (*Data, Information, Knowledge and Wisdom*), conforme apresentado por Ackoff (1989) e Roberts (1976).

Wurman (1991, p. 42) considera que “dados brutos podem ser informação, mas não são necessariamente. A não ser que sejam usados para informar, não têm valor intrínseco. (...) Assim, o que constitui informação para uma pessoa pode não passar de dados para outra”. Então, uma maneira de diferenciar *dados* de *informação* é por meio do valor e da importância que esses dados representam para alguém. Não obstante, existem diferentes conceitos e métodos de mensuração do valor de uma informação, conforme apresentado por Glazer (2003), Stephens (1989) e Repo (1986).

Diante da diversidade e amplitude de significados para o termo *informação*, há necessidade de definição do escopo da Segurança da Informação, ou melhor, identificar o bem a ser protegido. Portanto, destacamos que nos ateremos aos conceitos operacionais do termo *informação*, visando delimitar, exclusivamente, a questão a ser trabalhada.

Canal (2007), Theoharidou e Gritzalis (2007), e OECD (2002) consideram que tudo aquilo que contém dado ou informação é passível de ser protegido, e neste sentido, documentos impressos, tempo de armazenamento de arquivos, dados em computadores e conhecimentos humanos são alvos de proteção da Segurança da Informação. Van Bon (2002), ISO (2005), ITGI (2005) e SSE-CMM (2007) concentram suas atividades em tecnologia e nas

informações existentes em sistemas de computadores, e desta forma, a Segurança da Informação está associada à Segurança da Tecnologia da Informação e Comunicação (TIC).

Em ambos os enfoques, o bem protegido contém valor para a organização e é um elemento essencial para o sucesso do negócio, por isso, a sua perda, exposição imprópria ou fraudes acarretariam em prejuízos e danos. Desta forma, definimos *informação* como um ativo para a organização, e tudo aquilo que é sensível para os objetivos do negócio é alvo da segurança da informação, seja a imagem da organização, documentos sigilosos, salvaguarda de arquivos ou conhecimentos humanos.

Resta ainda uma definição para o termo *segurança*. Segundo definições encontradas em Howard (1997), Russel e Gangemi (1994), Harris (2004) e Pipkin (2000), Segurança é a preservação da Disponibilidade, Confidencialidade e Integridade da informação, além de outras propriedades citadas no padrão internacional ISO/IEC 17799:2005 (2005), como Autenticidade, Confiabilidade, Não-Repúdio e Responsabilidade sobre a informação. Tais termos são assim definidos:

- Disponibilidade: Garantia da acessibilidade da informação quando solicitada, além de que, os recursos devem ter capacidade de prover informações com níveis aceitáveis de desempenho.
- Confidencialidade: Garantir que a informação seja acessada apenas por pessoas autorizadas e mantida em nível mínimo de privacidade, ou ainda, garantir que a informação seja transmitida sem que seu conteúdo seja exposto às pessoas não autorizadas.
- Integridade: Garantir que a informação esteja íntegra, completa, consistente, na forma original no momento do seu acesso. Garantir ainda que a informação seja transmitida e alcance seu destino sem modificações ou erros.
- Autenticidade: Garantir a autoria da informação e o não-repudio à autoria. Alguns trabalhos em segurança da informação visam garantir que a autoria não seja revelada e não seja rastreada.
- Não-repúdio: Impedir que uma entidade participe de uma dada operação e posteriormente negue esta participação.
- Confiabilidade: É uma relação de confiança que existe entre pessoas ou sistemas, é acreditar em alguma coisa ou alguma informação baseado na essência dessa

informação. É a garantia que aquela informação vai estar segura mesmo em condições adversas.

- Responsabilidade: Remete à obrigação dos membros de uma organização de prestar contas às instâncias controladoras ou perante códigos de éticas ou legais perante ações.

Encontramos On-line (2008) que o termo *gerenciamento* ou *gestão* é originário do latin *manus*, que significa "conduzir com as mãos", remetendo a idéia de que o ato de gerenciar é seguir um caminho e ir na frente, é estar comprometido, e desta forma, o ato de gerenciar é mais forte do que apenas nortear ou apontar uma direção. Não obstante, "*gestão* é a efetiva utilização e coordenação dos recursos a fim de atingir os objetivos definidos com a máxima eficiência" (ON-LINE, 2008, p. 04).

De acordo com Fayol (1990), *gestão* é o conjunto de ações ou processos responsáveis por planejar, organizar, liderar, coordenar e controlar atividades e pessoas a fim de atingir os objetivos pretendidos.

- Planejar: É uma atividade ou processo de criação, desenvolvimento e manutenção de um plano estratégico a ser seguido com o propósito de alcançar os objetivos estabelecidos. Planejar é uma propriedade fundamental do comportamento inteligente. De acordo com Koontz e O'Donnell (1974), a mais fundamental das cinco funções administrativas é o planejamento, visto que envolve seleção entre alternativas de cursos de ação futuros para a organização, além de definir os objetivos e metas da organização e determinar maneiras de alcançá-los.

- Organizar: É a forma de coordenar ou rearranjar os recursos disponíveis, alocando-os da melhor forma segundo o planejamento estabelecido. De acordo com Koontz e O'Donnell (1989), organizar é estabelecer uma estrutura intencional de funções, por meio da identificação e enumeração de atividades necessárias para o cumprimento das finalidades, e pela designação e delegação dessas atividades. É, portanto, um conjunto de relações de atividades e autoridades.

- Liderar: É a habilidade de conduzir, inspirar ou afetar o comportamento humano, de maneira que estimule no liderado a percepção do caminho a ser seguido e atraia seu comprometimento com o sucesso da atividade.

- Coordenar: Significa harmonizar todos os atos e todos os esforços coletivos do negócio, sincronizando ações e adaptando os meios aos fins.
- Controlar: De acordo com Koontz e O'Donnell (1989), controlar é a medição do desempenho contra metas e correção das atividades de modo garantir que os objetivos da organização sejam alcançados. Segundo Fayol (1990), controlar consiste em avaliar e verificar se as atividades estão sendo conduzidas conforme planos previamente definidos, ordens previamente dadas e princípios previamente acordados.

Desta forma, definimos *Gestão da Segurança da Informação* como um conjunto de práticas e métodos de controle, coordenação, liderança, organização e planejamento, que visam prover e manter os elementos essenciais de sucesso da organização em níveis aceitáveis e necessários de disponibilidade, confiabilidade, autenticidade, integridade, confidencialidade, responsabilidade e não-repúdio para que os objetivos do negócio sejam atingidos conforme planejado.

De forma sucinta, desde que saibamos a definição de termos chaves, podemos redefinir a frase acima como: *Gestão da Segurança da Informação* é um conjunto de práticas e métodos de **gestão** que visam prover e manter os **ativos** da organização em níveis aceitáveis e necessários de **segurança** para que os objetivos do negócio sejam atingidos conforme planejado.

3.2. AS ORIENTAÇÕES DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Canal (2007) e Alaboodi (2007) apresentam uma divisão dos modelos de Gestão da Segurança da Informação (GSI) em categorias. Os modelos são classificados conforme a forma de atuação e a orientação dada ao desenvolvimento e à estrutura de gestão. Desta forma, são definidas cinco categorias, conforme segue:

- Orientada a Produtos;
- Orientada a Processos;
- Orientada a Controles;
- Orientada a Melhores Práticas;

- Orientada a Gerenciamento de Riscos.

Alguns modelos de Gestão de Segurança da Informação, como aquele apresentado por Canal (2007), sugerem que os objetivos dos programas de segurança devem estar totalmente ligados aos objetivos de negócio da organização e não somente garantir a Disponibilidade, Confidencialidade, Integridade e Autenticidade das informações. Desta maneira, falha no cumprimento dos objetivos da organização incorre em um incidente de Segurança da Informação, que deve ser tratado pela Gestão da Segurança da Informação.

Tais modelos são originários de modelos de Qualidade Total e do padrão ISO 9001, e definem Segurança da Informação como Segurança Contextualizada, dependente do contexto e baseada nos objetivos da organização. Tal definição está presente no modelo de Gestão da Segurança da Informação ISM3 (*Information Security Management Maturity Model*), "Tradicionalmente, um incidente é qualquer perda de confidencialidade, disponibilidade e integridade. Na segurança contextualizada, um incidente é uma falha em alcançar os objetivos de negócio da organização." (CANAL, 2007, p. 16).

É importante destacar que mesmo os modelos de GSI que definem o escopo da Segurança da Informação baseado na Disponibilidade, Confidencialidade, Integridade e Autenticidade da informação também visam o alinhamento com os objetivos da organização. No entanto, um incidente de segurança decorreria da falha no cumprimento de uma dessas quatro características e não no objetivo de negócio da organização. Adiante apresentaremos as características marcantes e diferenças entre os principais modelos de Gestão da Segurança da Informação.

De maneira geral, "um modelo de Gestão de Segurança da Informação é uma estrutura composta por diversos módulos – de disciplinas distintas" (THEOHARIDOU; GRITZALIS, 2007, p. 64) que interagem entre si para garantir os níveis de segurança exigidos pela organização para que ela alcance os objetivos pretendidos. A maneira como esses módulos interagem entre si, define a estrutura de desenvolvimento e orientação do modelo de gestão.

Desta forma, conforme citado no início do capítulo, interações baseadas em processos, procedimentos, controles, melhores práticas e tecnologia norteiam os modelos de GSI atualmente utilizados, que comumente mesclam essas características para compor um modelo de gestão mais completo e robusto.

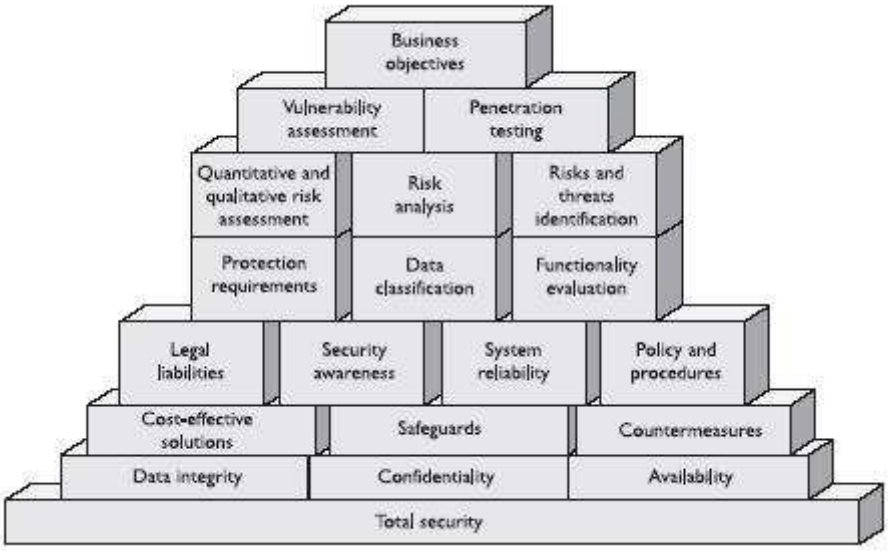

Figura 3.1 - Estrutura genérica de disciplinas que compõem um modelo de Gestão de Segurança da Informação
(Fonte: Harris, Shon. (2004), Editora McGraw Hill, CISSP All-inOne Exam Guide, 3º Edição.)

3.2.1. A orientação a produtos

Modelos de GSI orientados a produtos caracterizam-se por apresentarem uma estrutura de avaliação de especificações e conformidades de produtos de acordo com técnicas e métodos específicos. Desta forma, a orientação a produtos é completamente voltada à tecnologia, e é muito útil em processo de seleção de equipamentos ou tecnologias que satisfaçam ou supram demandas da organização.

Imaginemos, por exemplo, que determinada organização pretende instalar um equipamento de proteção de intruso, visando mitigar vulnerabilidades do seu sítio *web*, no entanto, não sabe qual produto escolher ou qual a melhor tecnologia que endereça seu problema. A orientação a produtos, como o ICSA Labs (2007) e Common Criteria (2007), detalha os requisitos que equipamentos de proteção de intruso devem apresentar para que satisfaçam condições mínimas de segurança. Assim, a organização, durante as tomadas de decisões, pode utilizar os resultados da orientação a produtos para selecionar o equipamento que melhor atende às suas necessidades.

A orientação a produtos certifica as características de segurança esperadas em equipamentos, “define os padrões de segurança da informação para produtos e, atualmente,

certifica mais de 95% da base instalada de produtos de segurança no mundo" (ICSA LABS, 2007, p. ?).

3.2.2. A orientação a processos

Modelos de GSI orientados a processos apresentam atividades estruturadas e organizadas em grupos – conhecidos como processos – que permitem que um objetivo seja traçado e alcançado, possibilitando ainda a interação com outros processos. "Um processo é uma série de atividades logicamente relacionadas e conduzidas para alcançar um objetivo definido" (VAN BON, 2002, p. 25).

De maneira genérica, um processo possui uma entrada – *Input* – que é processada ou executada por uma série de atividades, e o resultado dessa execução é apresentado na saída, conhecido como *Output*. Durante o processo de execução das atividades, mecanismos de mensuração e controle são acionados a fim de garantir que o resultado dessas atividades esteja em conformidade com leis, padrões e objetivos pretendidos.

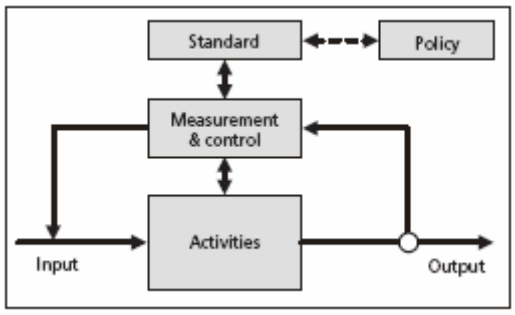

Figura 3.2 - Diagrama de processo
(Fonte:. Van Bon, J. (2002), IT Service Management: An Introduction. 1º Edição)

Visibilidade é um dos benefícios proporcionados pela orientação a processos, pois as atividades são encadeadas, seqüenciadas e co-relacionadas, o que permite que seja criado um mapa de atividades – conhecido como diagrama de processos – e desta forma, pontos de verificação e controle podem ser implantados a fim de assegurar que os objetivos e metas, previamente definidos, sejam alcançados. Esta característica, de acordo com Harris (2002) é definida como visibilidade.

A orientação a processos garante ainda que as atividades e os resultados sejam repetíveis, dado que existe um padrão na forma como são executados e há possibilidade de controlar as etapas do processo. Desta forma, a Gestão da Segurança da Informação baseada em processos agrega confiabilidade ao negócio da organização, pois proporciona um nível estável e contínuo dos resultados de segurança.

3.2.3. A orientação a controles

Modelos de GSI orientados a controle oferecem métodos, indicadores e ferramentas que visam estabelecer uma arquitetura de mensuração da Segurança da Informação. Assim, de acordo com Alger (2001) modelos de GSI orientados a controle podem ser utilizados como indicadores isolados, servindo de bases para métricas e medidas. Além disso, podem ser aplicados de maneira mais ampla, como nos processos de mensuração e controle da arquitetura de processos citada anteriormente, e desta forma, sua principal característica é dotar a GSI de um mecanismo de monitoramento e revisão do processo, também conhecido como melhoria contínua do processo. Para tal, normalmente são utilizadas técnicas de gestão de qualidade, como o ciclo de Deming, exemplificado na figura 3.3.

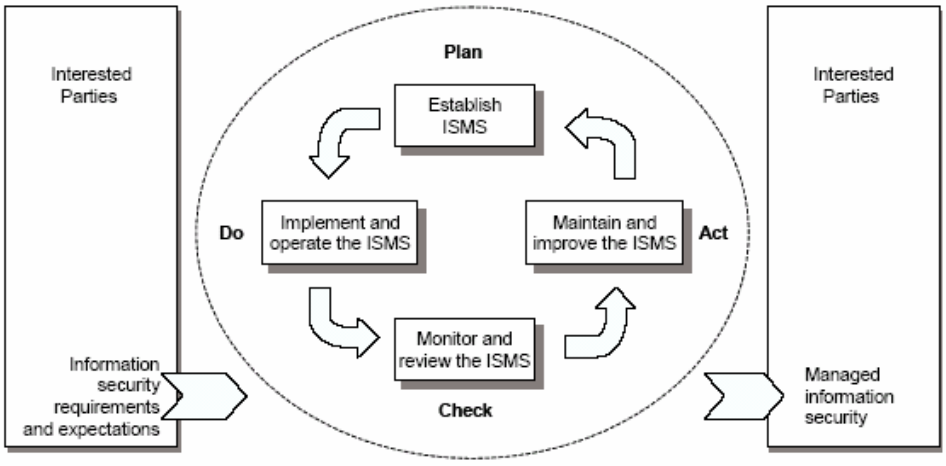

Figura 3.3 - Ciclo de Deming - PDCA (Plan-Do-Check-Act)
(Fonte: ISO/IEC 27001:2005)

É amplamente aceito que uma atividade não pode ser bem gerenciada se não puder ser mensurada. Desta forma, a orientação a controles proporciona um norte para a Gestão da Segurança da Informação, pois permite que a segurança seja mensurada, rastreada, e o mais importante, possibilita a criação de um programa de segurança faseado, equivalente a Modelos de Maturidade e Capacidade, onde é possível canalizar os investimentos em segurança, proporcionando um desenvolvimento orientado e gradual da segurança da informação.

Não obstante, é passível de imaginação que quando são feitos investimentos em qualquer área, espera-se ou cria-se uma expectativa do retorno deste investimento, seja em benefícios, seja em lucros ou em alguma melhoria. Neste sentido, programas de segurança faseados permitem à Gestão da Segurança da Informação demonstrar e mensurar o retorno dos investimentos em segurança, uma vez que as fases do programa indicam propriedades de segurança e revelam a capacidade da gestão de auxiliar a organização a alcançar os objetivos do negócio. Como exemplo, determinada fase ou nível do programa pode indicar que existe um plano de continuidade dos negócios que garante o funcionamento da organização mesmo em situações extremas de adversidade.

Essa característica agrega confiança à Gestão da Segurança da Informação, e conforme apresentado por Ferraiolo, “engenharia de segurança apresenta problemas com respeito à confiança nos modelos de gestão da segurança, e esta questão pode ser trabalhada através da implementação de modelos de maturidade e capacidade (CMM).” (1993, p. 02)

Modelos de Maturidade e Capacidade (CMM) provêm um guia para definição e melhoria contínua dos processos com o passar do tempo, definem níveis de maturidade e capacidade com significados diversos, e podem ser aplicados a qualquer tipo de processo. Os CMMs descrevem O QUÊ deve ser feito para melhorar o controle sobre os processos, a performance, o gerenciamento e o monitoramento de atividades.

> A filosofia básica por trás do CMM é fornecer mecanismos de controle que melhoram e tornam os processos das organizações mais eficientes, aumentando a capacidade dessas organizações de executarem atividades particulares. Ele é baseado na habilidade de documentar, definir, monitorar, gerenciar e padronizar os processos por toda organização. (BEMBERGER, 1997, p. 113)

3.2.4. A orientação a melhores práticas

Modelos de GSI orientados a melhores práticas baseiam-se na elaboração e utilização de listas de padrões e técnicas comumente aceitas, testadas e difundidas nas organizações que utilizam segurança da informação. Normalmente estas melhores práticas derivam de um processo contínuo de evolução do estudo da segurança da informação dentro das organizações, e são coletadas e analisadas por instituições normativas.

Desta forma, modelos de GSI orientados às melhores práticas apresentam uma lista de atividades – conhecidas como melhores praticas – que agregam segurança à organização. As melhores práticas não são verdades absolutas e a simples aplicação delas não garante que a organização estará livre de incidentes de segurança, no entanto, "servem como ponto de partida para implementação de uma Gestão de Segurança da Informação" (PELTIER, 2003, p. 25), assim como podem ser utilizadas como guias em processos de auditoria e conformidade.

3.2.5. A orientação a gestão de riscos

A Gestão de Riscos[6] deve ser interpretada muito mais como um processo do que como um modelo de Gestão de Segurança da Informação, dado que ela fornece ferramentas e metodologias para identificar, quantificar, qualificar e auditar as vulnerabilidades e ameaças[7] presentes nos ativos da organização. O termo *modelo* é definido como "uma construção abstrata e conceitual que representa a relação entre variáveis, sem o provimento de guias específicos de como implementar" (TOMHAVE, 2007, p. 09).

Por tal motivo, a Gestão de Riscos é encontrada em modelos com diferentes orientações, como exemplo no padrão ISO/IEC 17799:2005, cuja orientação é voltada às Melhores Práticas e inclui atividades de análise e avaliação de riscos. Os resultados da Gestão de Riscos norteiam a Gestão da Segurança da Informação nas atividades de seleção de

[6] Segundo Holton (2004), o termo risco é definido como incerteza e probabilidade de erro ou de impacto negativo que um evento pode provocar sobre os objetivos da organização, caso venha a ocorrer.
[7] Segundo Harris (2004), vulnerabilidade é a existência conhecida de uma fraqueza ou falta de proteção que possa ocasionar uma falha ou erro de operação, enquanto que ameaça é o perigo potencial à segurança da informação e/ou a sistemas, ou então é alguém ou alguma coisa que utiliza das vulnerabilidades do sistema para atacá-lo. Conceito similar é encontrado no padrão ISO/IEC 13335-1:2004 (ISO, 2004).

controles para reduzir e manter os riscos em níveis aceitáveis pela organização, assegurando os objetivos do negócio.

De acordo com o *National Institute of Standards and Technology* (EUA, NIST, 2003), a gestão de riscos é composta por 3 processos básicos – Análise e Avaliação de Riscos, Mitigação de Riscos, e Auditoria. “A profundidade dos processos de Avaliação e Análise de riscos pode variar significativamente, e é determinada pela criticidade e sensibilidade dos sistemas.” (EUA, NIST, 2006, p. 08).

No entanto, a principal característica da Gestão de Riscos é a sua natureza contínua e periódica, na qual, os riscos, vulnerabilidades e ameaças não precisam ser completamente eliminados, e provavelmente o custo de eliminar os riscos por completo é impraticável, mas, devem sempre ser controlados e mantidos em níveis aceitáveis pela organização.

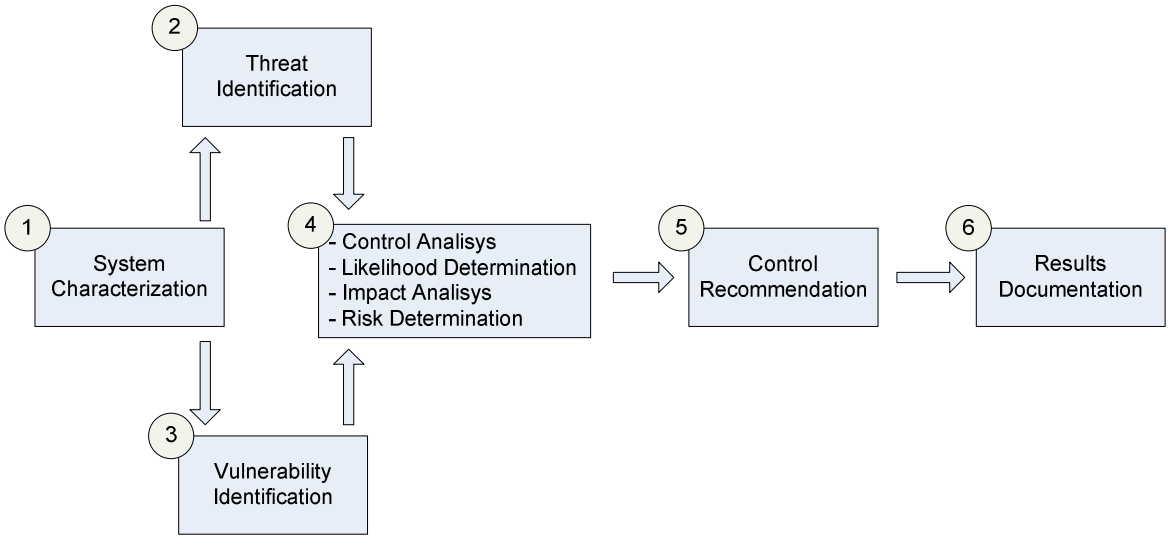

Figura 3.4 - Processo de avaliaçao de riscos
(Fonte: NIST, Special Publication 800-100, Information Security Handbook: A Guide for Managers)

Para NIST (EUA, NIST, 2006), Chapin e Akridge (2005) e ISO (2005), as práticas de gestão de riscos são, certamente, elementos essenciais de um modelo de GSI, pois oferecem métodos eficientes para identificar vulnerabilidades e selecionar controles para manter as atividades de segurança alinhadas aos objetivos do negócio. Além disso, a Gestão de Riscos fornece informações para balancear os custos dos benefícios da segurança, que de maneira geral, é uma forma de avaliar o valor da informação.

3.3. OS ELEMENTOS DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Indiferente dessas características e da orientação dada aos modelos, os seus objetivos são muito similares, visam reduzir os riscos, canalizar os investimentos e promover um alinhamento dos objetivos da Gestão da Segurança da Informação com os objetivos de negócio da organização. Os modelos de GSI estão fundamentados em conhecimentos adquiridos sobre processos, gerenciamento, qualidade, negócios, tecnologia, controles e melhores práticas, e certamente não são um manual de COMO FAZER[8] (*how to*), por isso, os modelos de GSI devem ser analisados e integrados às decisões estratégicas de qualquer organização, pois, absolutamente não há um modelo melhor que o outro.

Estar alinhado aos objetivos da organização significa conhecer e trabalhar pelo negócio da organização, ou seja, em segurança da informação significa garantir que o nível de segurança fornecido para os ativos da organização são compatíveis com seus valores e necessidades. Como exemplo, imaginemos que uma organização instalou um sistema de *firewalls* redundante e com isso elevou a disponibilidade de acesso ao seu sítio web de 99,0% para 99,99%, ou seja, elevou o nível de segurança daquele sítio web, afinal, elevou uma métrica da disponibilidade. Mas naquele momento a organização precisava aumentar a disponibilidade através desta métrica ou aumentar a capacidade de oferecer serviços no seu sítio web, e para isso, talvez ferramentas criptográficas fossem mais eficazes do que o sistema de *firewalls* redundantes?

Essas questões devem ser tratadas pela Gestão de Segurança da Informação, que não deve se preocupar somente em atingir níveis máximos absolutos de segurança ou implantar o estado da arte em tecnologia, pois, segurança não é alcançada apenas com aplicação de tecnologia, mas com metodologias de gerenciamento e conhecimento do negócio, afinal, “Segurança da Informação não é meramente um problema técnico, é também um problema organizacional e social”(DHILLON; BACKHOUSE, 2000, p. 126).

Os modelos de GSI devem assessorar, nortear, prover e manter níveis de segurança necessários para que a organização funcione, se desenvolva e alcance seus objetivos. Estudos

[8] Manuais de COMO FAZER normalmente instruem passo a passo como executar e alcançar os objetivos propostos naquele manual. No caso de Gestão de Segurança da Informação, um modelo COMO FAZER seria aquele que instrui como executar as ações de segurança para que a organização esteja segura, ou seja, quais configurações, equipamentos, treinamentos, entre outros, devem ser feitos, e por isso, normalmente são utilizados pelos Níveis Operacionais das organizações. Modelos COMO FAZER tendem a ser específicos, e apresentam pouca flexibilidade de adequação às necessidades estratégicas das organizações.

que descrevem as vantagens de se investir em Gestão da Segurança da Informação, e uma delas é “garantir que os investimentos não excederão os benefícios esperados, que serão compatíveis com as necessidades de segurança e com o valor da informação” (EUA, NIST, 2006, p. 2).

De acordo com Gaunt (2000), Andress (2000) e Von Solms (2000), o sucesso da implantação de modelos de GSI depende muito mais da inseminação dos conceitos de segurança dentro da cultura da organização do que de configuração de equipamento, implantação de tecnologia, normas e decretos. OECD (2002) defende ainda que todos participantes da organização são peças importantes para o sucesso do programa de Segurança da Informação, e que a cultura é expressa em valores coletivos e costumes, que normalmente resulta em ações, comportamentos e maneiras de interagir dentro de um ambiente.

De acordo com Von Solms e Von Solms (2004), programas de treinamento e educação desempenham um papel importante na disseminação dos conceitos de segurança da informação. No entanto, para que a segurança incorpore a cultura da organização é preciso algo mais. Segundo Martins (2003) a cultura organizacional de segurança é composta por confiança, condutas éticas, políticas e procedimentos, treinamento e educação. Para este autor, é necessário que seja dada devida importância e incentivo ao comportamento de segurança da informação dentro das organizações. Além disso, devem existir políticas para nortear o comportamento humano e descrever as expectativas de segurança da organização. Não obstante, a liderança e a participação intensa dos executivos da organização são peças chaves para o sucesso da inseminação da cultura da Segurança da Informação na organização.

Segundo Eloff e Eloff, um ambiente de Gestão da Segurança da Informação deve ser composto por “uma mescla inteligente de aspectos como políticas, padrões, guias, melhores práticas, tecnologia, recursos humanos e requisitos legais e éticos” (2003, p. 01). Além desses aspectos, acrescenta-se que os aspectos relacionados ao negócio da organização devem ser compreendidos pelos domínios da Gestão da Segurança da Informação, conforme citado por Theoharidou e Gritzalis (2007).

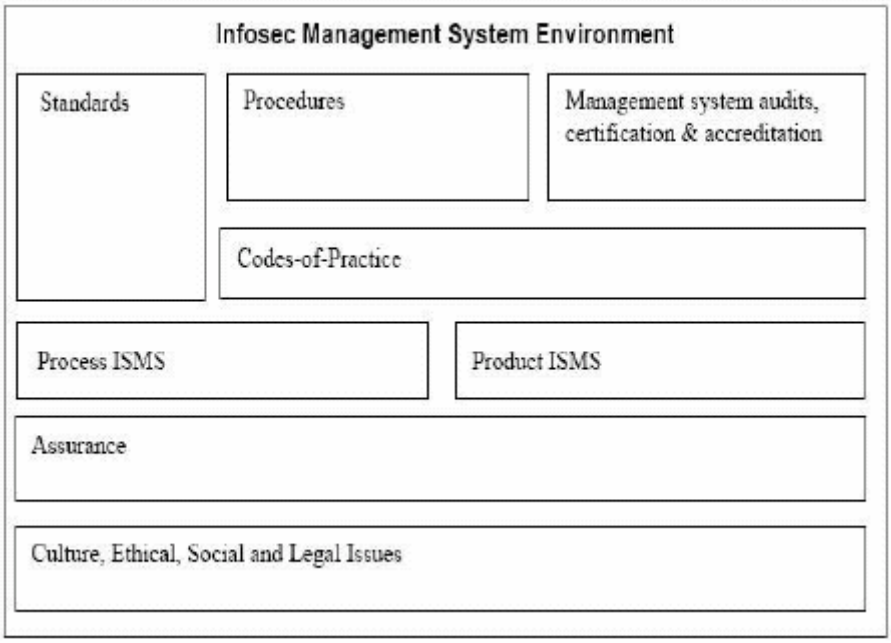

Figura 3.5 - Ambiente de Gestão da Segurança da Informação
(Fonte: Eloff, J., Eloff, M., Information Security Management - A New Paradigm, SAICSIT, 2003.)

Segundo Harris (2004), a Gestão da Segurança da Informação deve servir como um programa de segurança corporativo composto por gestão de riscos, políticas de segurança da informação, procedimentos, padrões, guias e bases de execução, classificação da informação, segurança organizacional e educação em segurança. Além disso, são funções da GSI determinar objetivos, escopo, políticas, prioridades, padrões e estratégias a serem cumpridas pelo programa de segurança.

Baseados nas definições de Harris (2004), Eloff e Eloff (2003), Theoharidou e Gritzalis (2007), nos estudos sobre cultura de segurança realizados por Martins (2003), Gaunt (2000), Andress (2000) e Von Solms (2000), e nas considerações feitas neste Capítulo, podemos definir que os **Elementos Gerais da Gestão da Segurança da Informação** abrangem aspectos relacionados à:

- **PROCESSOS E GESTÃO;**
    - Apresentação de atividades estruturadas, co-relacionadas e organizadas em grupos, formando uma cadeia de resultados previsíveis que agregam visibilidade ao modelo de GSI e permitem que os objetivos sejam traçados e rastreados;

- Desenvolvimento de ações de planejamento, visando determinar os cursos da organização por meio de definição de objetivos e escopo;
- Organização dos recursos disponíveis, estabelecendo uma estrutura intencional de funções que permitem identificar e enumerar as atividades necessárias para o cumprimento das finalidades;

- **CONTROLES DE SEGURANÇA;**
  - Apresentação de métodos, indicadores e ferramentas de segurança que visam mensurar e manter o curso das atividades e evitar desvios nos resultados;
  - Estabelecimento de métricas e medidas de segurança, a fim de determinar o nível de segurança da organização;

- **ARQUITETURA DE MENSURAÇÃO E AUDITORIA;**
  - Estabelecimento de guias para o desenvolvimento orientado e gradual das práticas e processos de segurança, permitindo canalizar os investimentos e identificar o grau de eficiência ou alinhamento dos objetivos da GSI com os objetivos do negócio;
  - Estabelecimento de um Programa de Segurança que permite ao Modelo de GSI demonstrar a evolução dos benefícios de segurança e assegurar o retorno dos investimentos.

- **TECNOLOGIA;**
  - Apresentação de técnicas e tecnologias que possibilitam que os serviços e negócios da organização sejam realizados de maneira mais segura;
  - Apresentação de requisitos, referências e características de segurança para equipamentos, produtos e operações da organização.

- **PRÁTICAS BASES E PADRÕES;**

- Apresentação de ampla lista de atividades, procedimentos e práticas eficientes para minimizar os riscos e proteger o negócio da organização;
- Estabelecimento de práticas comumente aceitas e aplicadas em todo mundo, possibilitando uma linguagem universal e facilitando a troca de informações entre as organizações.

- **ASPECTOS LEGAIS, CULTURAIS, SOCIAIS E ÉTICOS;**
  - Estabelecimento de processos ou meios que permitam ao modelo de GSI endereçar questões legais e éticas, garantindo que a organização esteja em conformidade com leis e códigos de ética, e utilizando dos mecanismos legais para proteger os negócios da organização;
  - Estabelecimento de processos ou meios que permitam ao modelo de GSI lidar com as diferentes culturas organizacionais, e garantir o sucesso das ações de segurança por meio do comportamento de todos os membros da organização.

- **NEGÓCIO;**
  - Estabelecimento de processos ou meios que permitam ao modelo de GSI identificar, endereçar e acompanhar as necessidades de segurança e expectativas do negócio;
  - Estabelecimento de processos ou meios que permitam ao modelo de GSI alinhar, manter e revisar os seus objetivos aos objetivos do negócio.

As orientações da Gestão da Segurança da Informação, apresentadas neste Capítulo, demonstram características complementares que, se forem passíveis de integração em um modelo único de gestão, conseguiriam endereçar parte dos Elementos Gerais da GSI. Não obstante, “os problemas da segurança da informação devem ser solucionados através de ações coordenadas entre as áreas da tecnologia, da administração e métodos de gestão, dos sistemas de auditorias, das leis para segurança da informação e da ética.” (TSUJII, 2004, p. 03).

Apesar da característica genérica e ampla dos Elementos Gerais de GSI, devem ser identificados meios de realizar a integração desses diversos componentes, de forma que garanta a continuidade e a viabilidade de um Modelo de Gestão.

Além disso, é imprescindível que sejam feitas análises dos modelos de GSI atuais visando identificar suas vantagens, desvantagens e composições, confrontando-os com os Elementos Gerais da GSI. Esta análise permitiria, por exemplo, identificar possíveis deficiências que motivariam o desenvolvimento de um novo modelo de GSI. Faremos esta análise no capítulo seguinte.

4. REVISÃO E ANÁLISE DOS MODELOS ATUAIS DE GSI

Neste Capítulo faremos uma apresentação e uma análise crítica dos principais modelos de Gestão da Segurança da Informação encontrados na literatura[9] e pesquisas de mercado[10].

Os modelos analisados serão os seguintes:

- ISO/IEC 17799:2005;
- CobiT 4.0;
- ITIL;
- SSE-CMM;
- ISM3;
- ISO/IEC 27001:2005.

4.1. ISO/IEC 17799:2005

O padrão britânico BS7799 foi publicado em 1995 pelo *British Standards Institute*[11], e em 2000, após inúmeras revisões, foi adotado como padrão internacional ISO/IEC 17799:2000 que define as melhores práticas para gestão da segurança da informação.

O seu conteúdo sofreu uma revisão em junho de 2005, e a partir daí, o padrão ficou conhecido como **ISO/IEC 17799:2005**. Em julho de 2007 o padrão foi renumerado para ISO/IEC 27002:2005, para que fizesse parte da nova série de certificações ISO/IEC 27000, no entanto, seu conteúdo permaneceu o mesmo.

O padrão é orientado a melhores práticas e a versão de 2005 está composta por onze cláusulas e trinta e nove categorias principais de segurança, conforme tabela abaixo:

[9] Modelos citados por estudos de Canal (2007), Aloboodi (2007), Sanchéz (2006), Von Solms e Von Solms (2004), Chapin e Akridge (2005), de Oliveira Alves et al. (2006), Kajava e Savola (2005) e Tomhave (2007).
[10] Modelos citados em pesquisas de Modulo Security (2003), Modulo Security (2006) e Tuner, Oltisk e McKinght (2008).
[11] British Standards Institute é a organização nacional de padrões do Reino Unido sem fins lucrativos.

Tabela 4-1 - Estrutura do padrão ISO/IEC 17799:2005

CLAUSULAS	PRINCIPAIS CATEGORIAS DE SEGURANÇA
Security Policy	INFORMATION SECURITY POLICY
Organizing Information Security	INTERNAL ORGANIZATION
	EXTERNAL PARTIES
Asset Management	RESPONSIBILITY FOR ASSETS
	INFORMATION CLASSIFICATION
Human Resources Security	PRIOR TO EMPLOYMENT
	DURING EMPLOYMENT
	TERMINATION OR CHANGE OF EMPLOYMENT
Physical and Environmental Security	SECURE AREAS
	EQUIPMENT SECURITY
Communications and Operations Management	OPERATIONAL PROCEDURES AND RESPONSIBILITIES
	THIRD PARTY SERVICE DELIVERY MANAGEMENT
	SYSTEM PLANNING AND ACCEPTANCE
	PROTECTION AGAINST MALICIOUS AND MOBILE CODE
	BACK-UP
	NETWORK SECURITY MANAGEMENT
	MEDIA HANDLING
	EXCHANGE OF INFORMATION
	ELECTRONIC COMMERCE SERVICES
	MONITORING
Access Control	BUSINESS REQUIREMENT FOR ACCESS CONTROL
	USER ACCESS MANAGEMENT
	USER RESPONSIBILITIES
	NETWORK ACCESS CONTROL
	OPERATING SYSTEM ACCESS CONTROL
	APPLICATION AND INFORMATION ACCESS CONTROL
	MOBILE COMPUTING AND TELEWORKING
Information Systems Acquisition, Development and Maintenance	SECURITY REQUIREMENTS OF INFORMATION SYSTEMS
	CORRECT PROCESSING IN APPLICATIONS
	CRYPTOGRAPHIC CONTROLS
	SECURITY OF SYSTEM FILES
	SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES
	TECHNICAL VULNERABILITY MANAGEMENT
Information Security Incident Management	REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES
	MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS
Business Continuity Management	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
Compliance	COMPLIANCE WITH LEGAL REQUIREMENTS
	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS AND TECHNICAL COMPLIANCE
	INFORMATION SYSTEMS AUDIT CONSIDERATIONS

Fonte: International Organization for Standardization, ISO/IEC 17799:2005, Information technology - Security techniques - Code of practice for information security management.

Cada categoria principal de segurança contém um objetivo de controle, que determina o que deve ser alcançado naquele item, e um ou mais controles que podem ser aplicados a fim de atingir os objetivos das categorias.

Por ser um padrão aceito internacionalmente, a ISO/IEC 17799:2005 oferece uma linguagem universal para segurança da informação, além de definir conceitos, princípios básicos e oferecer um guia detalhado de melhores práticas e controles que norteiam processos de implantação e auditoria de segurança da informação nas organizações.

De acordo com a Nona Pesquisa Nacional de Segurança da Informação [12], é o modelo de Gestão da Segurança da Informação mais utilizado atualmente no Brasil, seguido dos decretos federais e do modelo de governança CobiT.

Figura 4.1 - Normas e Regulamentações que norteiam a Gestão da Segurança da Informação no Brasil
(Fonte: 9º Pesquisa Nacional de Segurança da Informação - Modulo Security)

Sanchéz, ao comentar sobre o padrão ISO/IEC 17799:2005, destaca:

> Apesar da relevância internacional do padrão ISO/IEC 17799:2005, não se pode afirmar que ele provê uma arquitetura de gerenciamento da segurança da informação, mas uma série de controles que podem ser utilizados como guia na condução de uma revisão detalhada da situação de segurança dos sistemas. (2006, p. ?)

[12] Pesquisa realizada pela empresa Modulo Security entre março e agosto de 2003 no Brasil, publicada em outubro de 2003. Os dados foram coletados por meio de questionários presenciais e on-line, totalizando 682 questionários. Foram ouvidos profissionais das áreas de Tecnologia e Segurança da Informação, distribuídos pelos diferentes setores da economia, correspondendo à metade das mil maiores empresas brasileiras. Disponível em http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf, acesso em 20 nov 2007.

Além disso, o padrão não apresenta uma ordem para execução dos controles, não estrutura ou co-relaciona as atividades, não estabelece guias para acompanhamento e orientação das atividades, não determina quais controles são essenciais e defende que nem todos eles precisam ser executados.

Apesar do padrão ISO/IEC 17799:2005 oferecer diretrizes e estabelecer controles que agregam segurança, sua aplicação isolada não garante proteção aos negócios das organizações, conforme apresentado pelo próprio padrão ISO/IEC 17799:2005:

> Deve-se ter em mente que nenhum conjunto de controles pode alcançar uma segurança completa, e que ações adicionais de gerenciamento devem ser implementadas para monitorar, desenvolver e melhorar a eficiência e a efetividade dos controles de segurança, visando alcançar os objetivos da organização. (2005, p. 06)

O padrão ISO/IEC 17799:2005 recomenda atividades de análise e avaliação de riscos como métodos de seleção dos controles e das práticas, no entanto, não apresenta metodologia para implantação e avaliação do cumprimento desses controles. Por isso, a utilização do padrão deve ser acompanhada de meios para planejar a implantação dos controles, mecanismos para assegurar que eles estão sendo aplicados corretamente e processos para agregar visibilidade e garantir que os resultados serão contínuos e repetíveis.

O padrão reconhece a importância de estudos prévios sobre as necessidades de segurança do negócio, além disso, define que o comprometimento dos executivos da organização é um fator crítico de sucesso da GSI, e que questões legais e éticas devem ser identificadas e levadas em consideração.

As necessidades de treinamento e educação em segurança da informação para todos participantes da organização são outros elementos que têm a atenção do padrão, o qual destaca ainda a necessidade de definição de responsabilidades sobre as ações de segurança. Apesar de listar práticas que, de certa forma, atingem a cultura organizacional, o padrão ISO/IEC 17799 não fornece ferramentas para abordar o assunto de maneira clara e explícita. Portanto, o uso do padrão como elemento de modelagem da cultura de segurança está condicionado ao estabelecimento de meios para identificar e avaliar a cultura da organização.

No entanto, em comparação aos Elementos Gerais de GSI, o padrão ISO/IEC 17799:2005 não estabelece meios para identificar as expectativas de segurança da organização e nem meios para alinhar os objetivos da GSI aos objetivos do negócio.

Assim, apesar de a Cláusula Décima dispor sobre o Gerenciamento da Continuidade do Negócio e apresentar práticas para garantir que as operações críticas da organização funcionem em situações adversas, não podemos afirmar que o padrão endereça os domínios de negócio da organização nos moldes estabelecidos nos Elementos Gerais de GSI. Pois, não existem processos ou meios que permitam ao padrão acompanhar, de maneira contínua, as necessidades de segurança e expectativas do negócio.

De fato, o padrão ISO/IEC 17799:2005 não se propõe a estabelecer práticas para o sucesso do negócio ou estratégias de gestão, mas sim, práticas para o estabelecimento de segurança da informação. Com este entendimento, percebemos que o padrão é uma lista de práticas e sugestões de ações que agregam segurança, sem detalhamentos técnicos ou descrição de ferramentas tecnológicas[13]. Portanto, quando se procura um guia inicial ou uma base de referência DO QUE fazer, o padrão demonstra ser uma ótima opção.

Em virtude da sua amplitude internacional, o padrão é utilizado na sustentação do desenvolvimento de vários estudos, como aquele indicado por Eloff e Eloff (2003) que sugere uma aplicação progressiva dos seus controles, permitindo que a organização adapte-se à evolução da segurança de forma não traumática. Endorf (2004) e Masacci e Zannone (2005) sugerem um complemento ao padrão por meio de controles que fazem conformidade com requisitos legais de proteção de informações e privacidade.

Assim, apesar das deficiências gerenciais do padrão ISO/IEC 17799:2005, ele apresenta práticas essenciais e controles básicos para a manutenção de um modelo de Gestão da Segurança da Informação, além de fornecer uma linguagem universal, permitindo que organizações troquem experiências e contribuam para o processo de aprimoramento das práticas de segurança.

[13] Apesar de não fazer referências a tecnologias, como desenho mais eficiente e seguro de uma rede de acesso remoto, ou maneiras seguras de implementar servidores de domínio, o padrão apresenta a necessidade do uso de criptografia, recomendando ainda, na categoria de Controles Criptográficos, o uso de chaves simétricas e assimétricas.

4.2. COBIT 4.0

O CobiT 4.0 (*Control Objectives for Information and related Technology*) é um modelo de governança da tecnologia da informação, desenvolvido pelo ISACA (*Information Systems Audit and Control Association*), e mantido pelo ITGI (*IT Governance Institute*).

O modelo CobiT está fortemente focado em controles, e com menos foco em execução. Além disso, entende que:

> Governança de tecnologia da informação é uma responsabilidade dos executivos e do conselho de administração, e consiste em liderança, estrutura organizacional e processos que asseguram que a TI da companhia sustentará e estenderá as estratégias e objetivos da organização" (ITGI, 2005, p. 05)

O CobiT 4.0 está composto por seis elementos, conforme ilustrado abaixo, e a sua principal finalidade é alinhar os objetivos da TI aos objetivos do negócio.

- Sumário Executivo (*Executive Summary*);
- Arquitetura (*Framework*);
- Controles Objetivos (*Control Objectives*);
- Guias de Gerenciamento (*Management Guidelines*);
- Práticas de Controles (*Control Practices*);
- Guias de Auditoria (*Audit Guidelines*).

4.2.1. Sumário Executivo (*Executive Summary*)

O Sumário Executivo, elaborado por ITGI (2003), consiste de um documento de apresentação dos princípios e conceitos chaves do modelo, destacando os benefícios da governança da tecnologia da informação e as conseqüências da sua inexistência.

O documento, de maneira geral, visa esclarecer questões do tipo: O que é Governança da Tecnologia da Informação? O que a Governança de TI abrange? Porque Governança da TI é importante e a quem ela diz respeito? O que os diretores podem fazer pela Governança de TI e como alcançá-la?

4.2.2. Arquitetura (*Framework*)

A Arquitetura do CobiT é orientada a processos e baseada em controles, além disso, é o principal elemento do modelo, pois estabelece os meios para alinhar os objetivos da TI aos objetivos do negócio.

A Arquitetura é composta por quatro domínios, e, conforme definição do ITGI (2005), endereça as tradicionais responsabilidades da TI de planejar, construir, executar e monitorar, sendo assim definida:

- ***PLAN AND ORGANIZE:***
    - Domínio responsável pelas ações estratégicas e táticas, que visam identificar as formas de contribuição da TI aos objetivos do negócio;
    - Domínio que endereça questões do tipo: Os objetivos da TI estão alinhados aos objetivos do negócio? A organização está utilizando seus recursos de maneira eficiente? Todos da organização entendem os objetivos da TI? Os riscos são conhecidos e gerenciados? A qualidade dos sistemas de TI é apropriada para as necessidades do negócio?
    - Composto por dez Controles Objetivos de Alto-Nível.
- ***ACQUIRE AND IMPLEMENT:***
    - Domínio responsável por identificar, desenvolver ou adquirir, implementar e integrar as soluções de TI aos processos de negócio da organização;
    - Responsável por gerenciar e controlas as mudanças e manutenções dos sistemas de TI, assegurando que as soluções continuarão atendendo às necessidades do negócio;
    - Domínio que endereça questões do tipo: Os novos projetos entregam soluções que atendem às necessidades do negócio? Os novos projetos serão entregues no prazo e de acordo com o orçamento? Os novos sistemas funcionarão corretamente quando implementados?
    - Composto por sete Controles Objetivos de Alto-Nível.

- ***DELIVER AND SUPPORT:***
    - Domínio responsável pela entrega dos serviços de TI, incluindo o gerenciamento da segurança e continuidade, o suporte ao usuário, e o gerenciamento de dados e das facilidades operacionais;
    - Domínio que endereça questões do tipo: Os serviços de TI estão sendo entregues em conformidade com as prioridades do negócio? A TI apresenta eficiência nos custos? A organização é capaz de utilizar os recursos de TI de maneira produtiva e segura? A confidencialidade, integridade e disponibilidade estão sendo atingidas?
    - Composto por treze Controles Objetivos de Alto-Nível.

- ***MONITOR AND EVALUATE:***
    - Domínio responsável por avaliar, com regularidade, a qualidade e a conformidade dos processos de TI de acordo com controles e requisitos;
    - Domínio responsável por gerenciar o desempenho dos processos da TI, monitorar os controles internos, verificar a conformidade com aspectos legais e prover governança;
    - Domínio que endereça questões do tipo: A performance da TI está sendo mensurada, de tal forma que os problemas sejam antecipados? O gerenciamento está garantindo que os controles internos são eficientes e eficazes? A performance da TI pode ser alinhada e correlacionada aos objetivos do negócio? Os riscos e os controles medidos estão sendo reportados?
    - Composto por quatro Controles Objetivos de Alto-Nível.

"A Arquitetura do CobiT é baseada no princípio de que para prover uma informação necessária aos objetivos do negócio, a organização deve gerenciar e controlar os recursos de TI por meio de processos estruturados" (ITGI, 2005, p. 11).

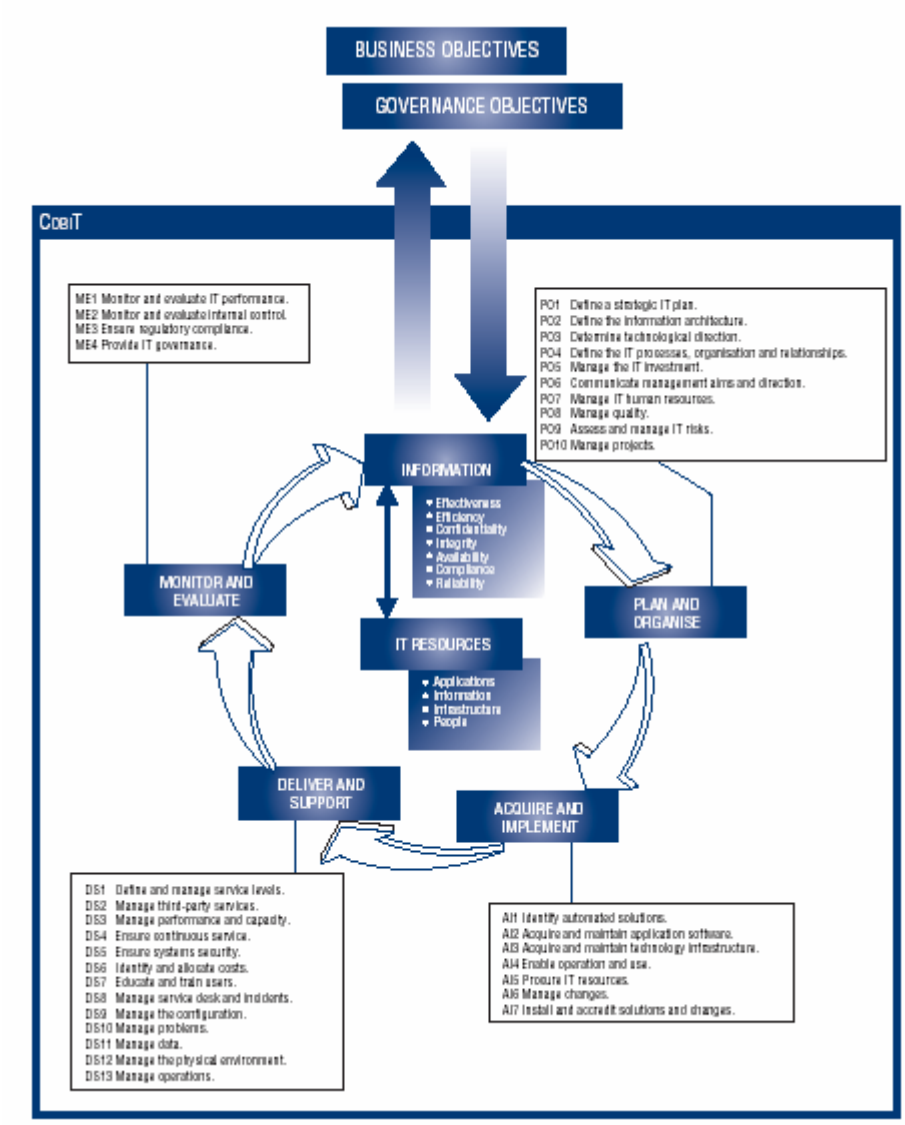

Figura 4.2 - Arquitetura (Framework) do modelo CobiT
(Fonte: IT Governance Institute, Control Objectives for Information and related Technology (COBIT), Version 4)

4.2.3. Controles Objetivos (*Control Objectives*)

Os Controles Objetivos do modelo definem as necessidades que precisam ser gerenciadas em cada processo de TI, a fim de atingir os requisitos do negócio.

O CobiT 4.0 possui trinta e quatro Controles Objetivos de Alto-Nível (*high-level IT Control Objectives*) orientados a processos e distribuídos entre os quatro domínios da Arquitetura do modelo. Cada um desses controles é composto por Controles Objetivos Detalhados (*Detailed Control Objectives*), totalizando 215 controles.

Apesar de não ser um modelo exclusivo de Gestão da Segurança da Informação, o CobiT 4.0 consegue endereçar questões relacionadas ao assunto. Dentre os principais Controles Objetivos de Alto-Nível que tratam da segurança da informação está o DS5 (*Deliver and Support 5 –* ***Ensure System Security***), composto por onze Controles Objetivos Detalhados. É importante destacar que este não é o único Controle Objetivo que aborda segurança, no entanto, certamente é o que faz de forma mais explícita.

Segundo o ITGI (2005), os objetivos do DS5 são estabelecer e manter funções, responsabilidades, políticas, padrões e procedimentos de segurança da tecnologia da informação, incluindo o monitoramento da segurança, testes periódicos e ações corretivas para incidentes e vulnerabilidades de segurança.

Os onze Controles Objetivos Detalhados do processo DS5 são:

- DS5.1 – Gerenciamento da Segurança da TI;
- DS5.2 – Plano de segurança;
- DS5.3 – Gerenciamento de Identidades;
- DS5.4 – Gerenciamento das Contas de Usuários;
- DS5.5 – Testes de Segurança, Fiscalização e Monitoramento;
- DS5.6 – Definição dos Incidentes de Segurança;
- DS5.7 – Proteção das Tecnologias de Segurança;
- DS5.8 – Gerenciamento de Chaves Criptográficas;
- DS5.9 – Prevenção, Detecção e Correção de Softwares Maliciosos;
- DS5.10 – Segurança de Rede;
- DS5.11 – Transferência de Dados Sensíveis.

4.2.4. Guias de Gerenciamento (*Management Guidelines*)

Os Guias de Gerenciamento do Modelo são responsáveis por prover ferramentas e metodologias de assessoramento à gestão da tecnologia da informação. Existe um Guia de

Gerenciamento para cada um dos trinta e quatro Controles Objetivos de Alto-Nível, e são compostos por quatro elementos:

- Uma arquitetura de mensuração e avaliação baseada em um Modelo de Maturidade e Capacidade (CMM), composta por cinco níveis;
- Uma tabela de responsabilidades, denominada *RACI* (*Responsible, Accountable, Consulted, and Informed*), que define as atividades e as responsabilidades dos envolvidos no processo;
- Uma tabela de *inputs* e *outputs* do processo, que encadeia os resultados e estabelece pontos de controle;
- Lista de métricas e objetivos do processo, que define os resultados que a TI deve atingir e estabelece os valores aceitáveis de desempenho.

Tabela 4-2 - Tabela *RACI* do processo DS5 do modelo CobiT 4.0

Functions / ***Activities***	**Chief Executive Office**	**Chief Financial Office**	**Bussiness Executive**	**Chief Information Office**	**Business Process Owner**	**Head Operations**	**Chief Architect**	**Head Development**	**Head IT Administration**	**Project Manager Office**	**Compliance, Audit, Risk and Security**
Define and maintain an IT security plan	I	C	C	A	C	C	C	C	I	I	R
Define, establish and operate an identity (account) management process			I	A	C	R	R	I			C
Monitor potential and actual security incidents				A	I	R	C	C			R
Periodically review and validate user access rights and privileges				I	A	C					R
Establish and maintain procedures for maintaing and safeguarding cryptographic keys				A		R			I		C
Implement and maintain technical and procedural controls to protect information flows across networks				A	C	C	R	R			C
Conduct regular vulnerability assessments		I		A	I	C	C	C			R

Fonte: IT Governance Institute, Control Objectives for Information and related Technology (COBIT), Version 4

A arquitetura de mensuração e avaliação do modelo CobiT mede o nível de alinhamento de cada processo de TI com os objetivos do negócio. Como exemplo, os primeiros níveis do modelo de maturidade do Controle Objetivo DS5 refletem um processo descoordenado e reativo (nível 1), autoridades de gerenciamento limitadas (nível 2), e existência de práticas de segurança mas sem foco claro nos objetivos do negócio.

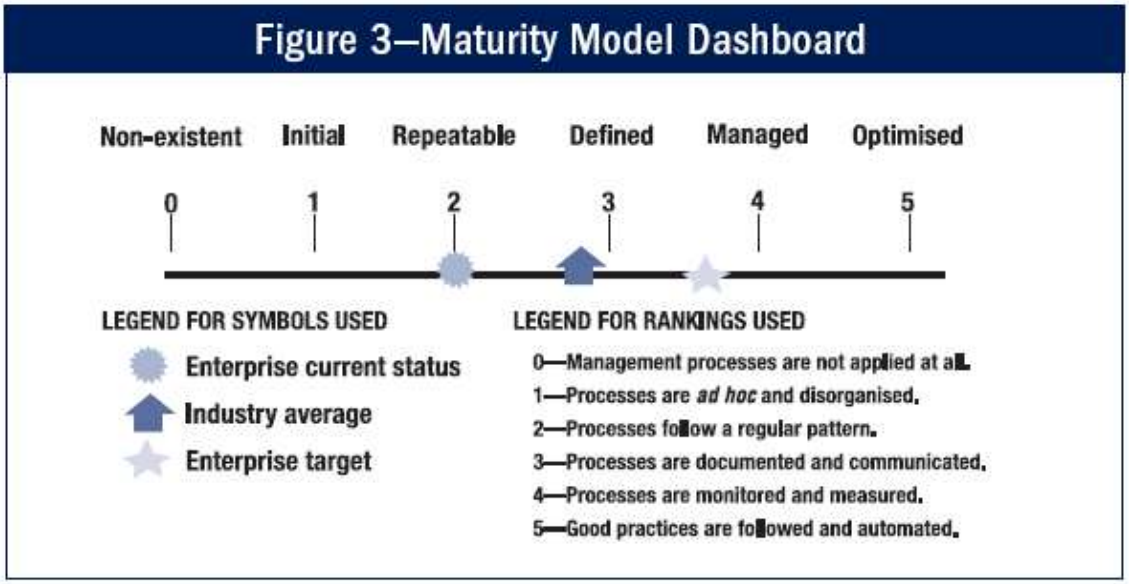

Figura 4.3 - Arquitetura de mensuração e avaliação do CobiT
(Fonte: IT Governance Institute, Board Briefing on IT Governance, 2nd edition, ISBN 1-893209-64-4, USA)

Quando aplicado à Gestão da Segurança da Informação, é imprescindível que os processos estejam posicionados no nível cinco, demonstrando que as atividades estão suportando e contribuindo para o sucesso da organização. Manter um processo de Segurança da Informação de maneira descoordenada e em desconformidade com os objetivos do negócio pode ser danoso para a organização, uma vez que os investimentos não estão sendo canalizados para a redução efetiva dos riscos e para o estabelecimento dos níveis de proteção necessários à organização.

Simonsson, Jonhson e Wijkström (2003), descrevem que a arquitetura de mensuração dos processos do CobiT oferece uma análise vaga e isolada do ambiente, e além disso, somente pessoas experientes no modelo são capazes de avaliar a maturidade da organização. Não obstante, não há garantias que duas análises distintas resultarão nas mesmas conclusões.

Tabela 4-3 - Níveis de Maturidade do Processo DS5 – CobiT

0 – NÃO EXISTENTE
• A organização não reconhece a necessidade de segurança da tecnologia da informação, e não há responsabilidades delegadas para tratar da segurança da TI.
1 - INICIAL / AD HOC
• A organização reconhece a necessidade de segurança da tecnologia da informação; • A segurança da tecnologia da informação é tratada de maneira reativa, e não é mensurada.
2 - REPETÍVEL MAS INTUITIVO
• As responsabilidades pela segurança da tecnologia da informação são delegadas a um coordenador de segurança, no entanto, sua autoridade para gerenciamento é limitada; • Apesar de existir coleta de informações de segurança, elas não são analisadas; • Os serviços de terceiros podem não endereçar necessidades específicas de segurança da organização.
3 - PROCESSO DEFINIDO
• Os processos de segurança da tecnologia da informação são definidos e alinhados com a política de segurança de TI; • Existe um plano de segurança da tecnologia da informação guiado por análises de riscos; • As informações de segurança não apresentam, claramente, foco nos objetivos do negócio.
4 – GERENCIADO E MENSURADO
• As responsabilidades pela segurança da tecnologia da informação são claramente definidas, gerenciadas e implantadas; • Análise de riscos de segurança e análises de impacto são executadas de maneira consistente; • Políticas e práticas de segurança estão completamente alinhadas com bases de segurança específicas; • Identificação, autenticação e autorização de usuários são padronizadas; • Informações de segurança são alinhadas aos objetivos do negócio.
5 – OTIMIZADO
• A segurança da tecnologia da informação é responsabilidade conjunta do gerenciamento do negócio e da TI, e está integrada com os objetivos de segurança do negócio. • Os requisitos de segurança de TI são claramente definidos, otimizados e estão inclusos em um plano de segurança.

Fonte: IT Governance Institute, Control Objectives for Information and related Technology (COBIT), Version 4

4.2.5. Práticas de Controles (*Control Practices*)

As Práticas de Controles do modelo CobiT compreendem uma lista genérica de melhores práticas para cada um dos Controles Objetivos, e descrevem as atividades necessárias para alcançar os objetivos de TI.

As Práticas auxiliam a gestão da TI na identificação de técnicas de implantação dos controles do CobiT, assim como apresentam meios de avaliação da maturidade de um processo. Existem, aproximadamente, 1600 Práticas de Controle no modelo CobiT.

De maneira geral, enquanto os Controles Objetivos estão focados NO QUE precisa ser feito, as Práticas de Controle descrevem orientações de COMO fazer. No entanto, conforme apresentado por ITGI, “as Práticas de Controle não descrevem soluções específicas, portanto, podem ser necessários guias adicionais mais detalhados, que podem ser encontramos em padrões, melhores práticas ITIL ou PRINCE 2.”(2007, p. 13)

Von Solms (2005) apresenta que devido ao CobiT ser um modelo de Governança de TI, o seu uso para a Gestão da Segurança da Informação apresenta a desvantagem de não oferecer guias detalhados e específicos de COMO fazer segurança, e por isso, em alguns casos, será necessário buscar outros guias. Ele apresenta ainda que a integração entre o CobiT e o padrão ISO/IEC 17799 resultaria em benefícios, visto a combinação das estruturas de governança de um modelo e o detalhamento de segurança do outro. Além disso, departamentos distintos poderiam utilizar modelos diferentes e, ainda assim, existir o alinhamento entre eles.

4.2.6. Guias de Auditoria (*Audit Guidelines*)

O documento de Guia de Auditoria apresenta ferramentas e atividades para avaliação da performance e verificação da conformidade dos processos de TI com os objetivos do negócio.

O documento é voltado para auditores internos e externos da organização, e é composto por três fases:

- Planejamento;

- Escopo;
- Execução.

Um dos benefícios do Guia é a padronização dos mecanismos de avaliação, permitindo a troca rápida de informações entre avaliadores e avaliados, e o estabelecimento de objetividade nas atividades de implantação e avaliação dos processos CobiT.

Apesar de ser um modelo orientado à tecnologia da informação, uma análise geral do CobiT 4.0 nos permite concluir que ele compreende quase todos os Elementos Gerias da Gestão da Segurança da Informação. Devido à sua Arquitetura, Controles Objetivos e Práticas de Controle, fica evidente que aspectos relacionados a processos e gestão, controles de segurança, arquitetura de mensuração e auditoria, práticas bases e padrões, e aspectos legais e éticos são compreendidos pelo CobiT.

O Controle Objetivo de Alto-Nível ME3 (*Monitor and Evaluate 3 –* ***Ensure Regulatory Compliance***) é responsável por identificar, acompanhar e integrar questões legais e éticas que impactam nos negócios e na TI.

O modelo CobiT não endereça aspectos culturais de segurança, apesar de abordar questões de treinamento por meio do Controle Objetivo de Alto-Nível DS7 (*Deliver and Support 7 –* ***Educate and Train Users***), seu objetivo é apenas capacitar os usuários ao uso de novas tecnologias.

De acordo com Von Solms e Von Solms (2004), programas de treinamento e educação desempenham um papel importante na disseminação dos conceitos de segurança da informação.No entanto, segundo Martins (2003), para que a segurança incorpore a cultura da organização é preciso que seja dada devida importância e incentivo ao comportamento de segurança da informação dentro das organizações. Além disso, devem existir políticas para nortear o comportamento humano e descrever as expectativas de segurança da organização.

> Uma das maiores desvantagens do modelo CobiT, e talvez um dos motivos pelo qual o modelo não é utilizado com mais freqüência, é a quantidade de conhecimento necessária sobre o modelo a fim de aplicá-lo no suporte à governança de TI ou como método de avaliação do desempenho da TI. (SIMONSSON; JONHSON; WIJKSTRÖM; 2007, p. 04).

4.3. ITIL

> Nos anos de 1980, a qualidade dos serviços de TI providos ao governo Britânico era tal, que o CCTA (*Central Computer and Telecommunications Agency*, hoje *Office of Government Commerce, OGC*) foi instruído a desenvolver uma abordagem para o uso eficiente dos recursos de TI. O objetivo era desenvolver uma abordagem independente de fornecedor. O resultado foi o ITIL (*Information Technology Infrastructure Library*), que cresceu de uma coleção de melhores práticas observadas na indústria de serviços de TI. (VAN BON, 2002, p. 11).

O ITIL é, portanto, um modelo orientado a processos e baseado em melhores práticas de gerenciamento dos serviços de TI. Ele é composto por dois elementos básicos e uma função, conforme descrito abaixo:

- Entrega de Serviços;
- Suporte a Serviços;
- *Service Desk* (função).

Cada um dos dois elementos básicos do modelo é composto por cinco processos, que fazem interações entre eles por meio de *inputs* e *outputs*. Apesar de todos esses dez processos endereçarem assuntos relacionados ao suporte e à entrega de serviços de TI, a maioria deles pode ser aplicada na manutenção da Segurança da Informação.

Os processos do ITIL objetivam manter o ambiente de TI, observando os acordos de níveis de serviço[14], e por isso, questões relacionadas à disponibilidade, integridade e continuidade dos serviços são abordadas pelo modelo. Alem disso, existem processos que abordam as ações reativas e pró-ativas de correção de incidentes e problemas, que podem, perfeitamente, ser aplicados nas práticas de manutenção da Segurança da Informação.

[14] Acordos de Níveis de Serviços (ANS) normalmente descrevem os serviços que devem prestados e detalham a qualidade desse serviço. Muitas vezes, são apresentados os indicadores e as métricas esperadas para os serviços.

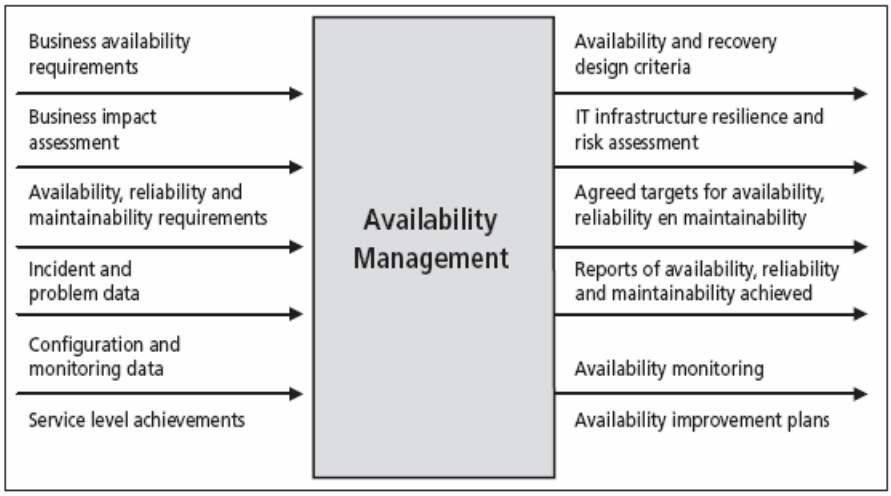

Figura 4.4 - Exemplo de inputs e outputs do modelo ITIL - Processo de Gestão da Disponibilidade
(Fonte: Van Bon, J., IT Service Management: An Introduction. IT Service Management Forum (2002). Van Haren Publishing. ISBN 90-806713-4-7.)

Não obstante, existe um processo de Gestão da Segurança que não faz parte dos elementos básicos do ITIL, mas é referenciado no estudo de Van Bon (2002) sobre o modelo e deve ser lançado em versões futuras, cujos objetivos são:

- Cumprir os requisitos de segurança definidos no Acordo de Nível de Serviço (ANS) e outros requisitos externos relativos a contratos, legislação a políticas externas;
- Prover um nível básico de segurança, independente dos requisitos externos, para impedir o acesso indevido às informações.

Desta forma, observamos que as abordagens de segurança providas pelo modelo ITIL objetivam atender aos níveis de segurança exigidos no ANS, sendo útil para organizações cujo negócio é a entrega e o suporte de serviços de TIC. Portanto, podemos afirmar que o ITIL endereça aspectos de negócio, somente se a organização prover serviços de TI, do contrário, inexiste, no modelo, processos de análises das necessidades de segurança da organização.

Análise similar pode ser feita em relação aos aspectos legais e éticos exigidos, uma vez que, se as necessidades de conformidade com leis, normas e códigos de ética forem restritas ao estipulado no ANS, o ITIL compreende perfeitamente os aspectos legais, do

contrário, inexistem processos que identificam os aspectos legais e éticos pertinentes ao negócio da organização.

No entanto, o modelo ITIL não endereça diversos outros aspectos dos Elementos Gerais de Gestão da Segurança da Informação, como por exemplo, os aspectos culturais e sociais.

Inexiste no modelo uma Arquitetura de Mensuração e Auditoria, que permita orientar e acompanhar o desenvolvimento das práticas de segurança, além de proporcionar o estabelecimento de critérios para a avaliação e comprovação do desempenho da GSI.

Apesar de o ITIL conter uma lista de atividades que endereçam os objetivos básicos de cada processo, não podemos afirmar que se tratam de práticas bases de segurança, uma vez que são restritas e direcionadas às necessidades específicas do processo ITIL.

Justamente por causa dessa especificidade do modelo, e por ser mais detalhado naquilo que se presta, o ITIL, muitas vezes, é utilizado como modelo de suporte para outros modelos, como o CobiT.

4.4. SSE-CMM

> A *International Systems Security Engineering Association* (*ISSEA*), é uma organização sem fins lucrativos dedicada à promoção do *Systems Security Engineering* como uma disciplina definida e mensurável. Fundada em 1999, ISSEA e seus membros têm a incumbência de manter o SSE-CMM – *Systems Security Engineering Capability Maturity Model* (ISSEA, 2007).

O modelo SSE-CMM é orientado a processos, focado nos requisitos necessários para a implantação de segurança em sistemas do domínio da tecnologia da informação. O modelo foi adotado como norma internacional ISO/IEC 21827, e apresenta conceitos e abordagens similares à norma ISO/IEC CD 15288.

O modelo SSE-CMM é composto por 22 áreas de processos (*process areas*), das quais 11 áreas são de segurança e 11 são de projetos e organização, e compreende 129 práticas bases (*base practices*).

As atividades do modelo englobam o ciclo completo do desenvolvimento de sistemas: Definição de conceitos, análise de requisitos, desenvolvimento, desenho, integração, instalação, operação e manutenção. Além disso, “o modelo fornece requisitos e métodos

apropriados de segurança para os desenvolvedores, integradores e organizações que provêm e adquirem serviços de engenharia de software" (SSE-CMM, 2007, p. 03).

A característica principal do modelo é o processo de mensuração baseado em modelos de maturidade e capacidade (CMM), que é composto por 5 níveis de maturidade e compreendido por 12 funcionalidades comuns (*common features*). As funcionalidades comuns, por sua vez, são compostas por 28 práticas genéricas (*generic pratices*) que definem o nível de maturidade da organização. Desta forma, à medida que as práticas genéricas são cumpridas, o nível de maturidade do processo de desenvolvimento de software aumenta, e por meio dessa análise, é possível, por exemplo, determinar qual processo requer mais investimentos e fixar metas.

O modelo SSE-CMM não abrange todos os Elementos Gerais de Gestão da Segurança da Informação, e não aborda assuntos como normas e políticas de segurança – considerado por Von Solms e Von Solms (2004) e ISO (2005) como requisitos mínimos e essenciais para o sucesso da Gestão da Segurança da Informação. Sem uma política de segurança "os esforços de segurança da informação não terão nenhuma referência ou suporte base para decisões, além de não demonstrar comprometimento dos executivos da organização." (VON SOLMS; VON SOLMS, 2004, p. 374).

Assim, o SSE-CMM representa apenas uma parte na Gestão da Segurança da Informação, que é o processo de desenvolvimento de sistemas. Desta forma, observamos que o modelo SSE-CMM é útil para organizações cujo negócio é o desenvolvimento e a avaliação de sistemas, do contrário, inexiste, no modelo, processos de análises mais amplo das outras necessidades de segurança da organização.

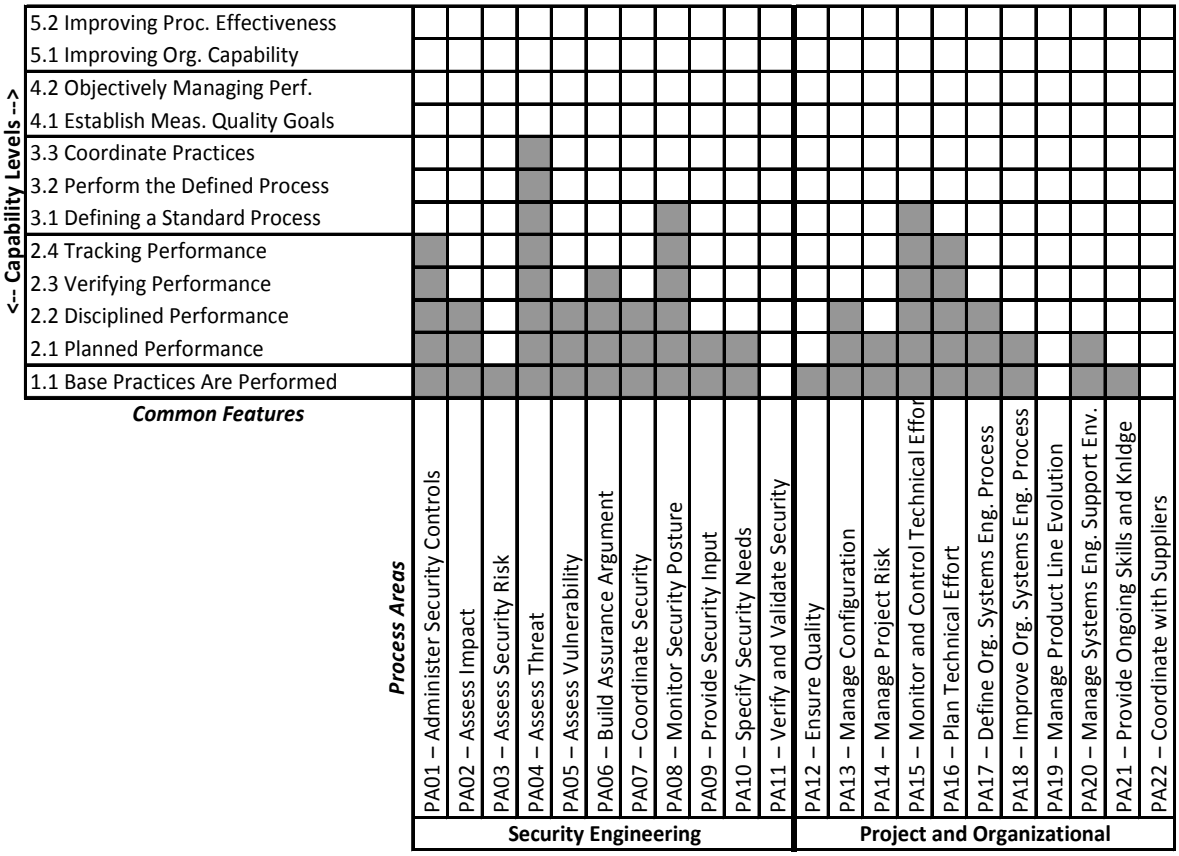

Figura 4.5 - Modelo de Mensuração do SSE-CMM
(Fonte: SSE-CMM, Systems Security Engineering – Capability Maturity Model.)

4.5. ISM3 (*INFORMATION SECURITY MANAGEMENT MATURITY MODEL*)

O ISM3, conforme definido por Canal (2007), é uma arquitetura de gestão da segurança da informação orientada a processos, independente de tecnologia e utiliza modelos de maturidade como método de avaliação, mensuração e controle dos processos. O modelo é baseado nos conceitos de qualidade definidos no padrão ISO 9001.

O objetivo do modelo ISM3 é prevenir incidentes que comprometam os objetivos do negócio, e por isso, a Segurança da Informação é definida como segurança contextualizada, dependente dos objetivos da organização.

Conforme definição dos autores do ISM3, “tradicionalmente, um incidente é qualquer perda de confidencialidade, disponibilidade e integridade. Na segurança contextualizada, um incidente é uma falha em alcançar os objetivos de negócio da organização.” (CANAL, 2007, p. 16).

O modelo ISM3 é composto por quatro processos bases – um genérico e três específicos – que por usa vez, são compostos por práticas. O processo genérico é conhecido como Gerenciamento da Documentação (*Document Management*), e sua finalidade é garantir a escolha dos processos mais adequados para a organização, assim como garantir que processos de revisão da documentação sejam aplicados. O modelo defende ainda que os processos de segurança somente são implantados de maneira robusta e tornam-se repetíveis por meio de processos de documentação.

Os processos específicos do modelo são: Gerenciamento Estratégico (*Strategic Management*), Gerenciamento Tático (*Tatical Management*) e Gerenciamento Operacional (*Operational Management*). Divididos desta maneira, as práticas que compõem os processos são executadas por grupos funcionais, criando uma hierarquia de decisões e atividades, fazendo conformidade com a teoria neoclássica do planejamento administrativo[15].

O modelo ISM3 apresenta uma arquitetura de mensuração dos processos baseada em CMM, composta por cinco níveis de maturidade. Os níveis de maturidade representam a redução dos riscos e o valor dos investimentos em segurança. Assim, níveis mais elevados de maturidade requerem alto investimento em segurança e resultam em baixo nível de riscos. Esta relação é originária do paradoxo de Mayfield, que estabelece uma relação que "para manter toda humanidade dentro de um sistema há necessidade de investimentos infinitos, e para manter toda humanidade fora de um sistema, também há necessidade de investimentos infinitos, no entanto, o custo entre estes dois extremos é muito baixo". (UNIVERSITY OF NEW HAVEN ..., 2001, p. 02).

A figura 4.6 ilustra o paradoxo de Mayfiled.

[15] De acordo com Koontz e O'Donnell (1974), o planejamento administrativo deve ser hierarquizado e constituído de três níveis: Estratégico (planejamento que envolve toda organização), Tático (planejamento que envolve setores da organização) e Operacional (planejamento que envolve atividades pontuais).

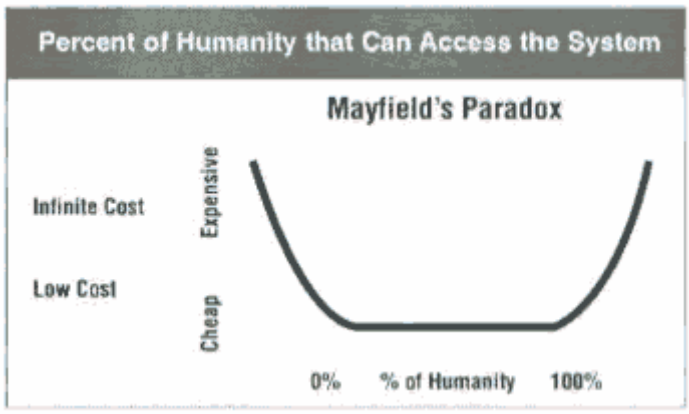

Figura 4.6 - Paradoxo de Mayfield
(Fonte: Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information, Information Systems Control Journal, ISACA, Volume 2, 2001.)

Os níveis de maturidade do modelo são assim classificados e definidos por Canal (2007):

- **Nível 1**: Resulta em uma redução considerável dos riscos de ameaças técnicas, com um baixo investimento em processos de segurança. Este nível é recomendado para organizações com poucos alvos de segurança da informação e recursos limitados. Métricas não são obrigatórias neste nível.
- **Nível 2**: Resulta em uma redução considerável dos riscos de ameaças técnicas, com um investimento moderado em processos de segurança. Este nível é recomendado para organizações com alvos normais de segurança da informação, que precisam demonstrar boas práticas de segurança para parceiros e que se preocupam em reduzir os incidentes de segurança. Métricas não são obrigatórias neste nível.
- **Nível 3**: Resulta em uma alta redução dos riscos de ameaças técnicas, com um investimento significante em processos de segurança. Este nível é recomendado para organizações com muitos alvos de segurança da informação e que dependem de serviços de informação, como exemplo o comércio eletrônico. Métricas não são obrigatórias neste nível.
- **Nível 4**: Resulta na maior redução de riscos de ameaças técnicas e internas, com um máximo de investimento em processos de segurança. Este nível é recomendado

para organizações complexas, com regulamentações específicas, tais como instituições financeiras. Métricas não são obrigatórias neste nível.

- **Nível 5**: Todas as características do nível 4, mas com métricas obrigatórias.

Os níveis de maturidade são atingidos conforme as práticas que compõem os quatro processos básicos do modelo são cumpridas. O modelo ISM3 relaciona quais práticas devem ser cumpridas para cada nível de maturidade, e talvez isso seja uma falha do modelo, dado que, por exemplo, apenas no quarto nível são definidas as regras de delegação de autoridade, no entanto, se isto for um fator de sucesso para a organização, deveria ser feito de imediato.

Na tabela abaixo estão relacionadas as práticas do processo de Gerenciamento Operacional necessárias para cada nível de maturidade:

Tabela 4-4 - Práticas necessárias para alcançar os níveis de maturidade - IMS3

Operational Management		***Maturity Levels***				
		1	2	3	4	5
OSP-1	Report to tactical management	x	x	x	x	x
OSP-2	Select tools for implementing security measures		x	x	x	x
OSP-3	Inventory management			x	x	x
OSP-4	Information Systems Environment Change Control		x	x	x	x
OSP-5	Environment Patching	x	x	x	x	x
OSP-6	Environment Clearing		x	x	x	x
OSP-7	Environment Hardening		x	x	x	x
OSP-8	Software Development Life-cycle control			x	x	x
OSP-9	Security Measures Change Control		x	x	x	x
OSP-10	Backup Management	x	x	x	x	x
OSP-11	Access Control		x	x	x	x
OSP-12	User Registration		x	x	x	x
OSP-14	Physical Environment Protection Management		x	x	x	x
OSP-15	Operations Continuity Management			x	x	x
OSP-16	Segmentation and Filtering Management	x	x	x	x	x
OSP-17	Malware protection management	x	x	x	x	x
OSP-19	Internal Technical Audit		x	x	x	x
OSP-20	Incident Emulation			x	x	x
OSP-21	Information Quality and Compliance Probing			x	x	x
OSP-22	Alerts Monitoring		x	x	x	x
OSP-23	Events Detection and Analysis			x	x	x
OSP-24	Handling of incidents and near-incidents			x	x	x
OSP-25	Forensics			x	x	x
OSP-26	Enhanced Reliabilty and Availability				x	x
OSP-27	Archiving Management				x	x

Fonte: ISM3 Consortium, Information Security Management Maturity Model, Version 2.0

Classificar o nível de maturidade de uma organização de acordo com o volume de investimentos em segurança para reduzir os riscos é uma maneira falha de mensurar um processo de Gestão da Segurança da Informação, considerando que nem sempre os riscos precisam ser eliminados, mas, precisam ser controlados e mantidos em níveis aceitáveis pela organização, e dado que existem N maneiras de reduzir os riscos, e cada uma delas com custos diferentes.

Conforme definido por NIST (2007), Chapin e Akridge (2005), e Baker e Wallace (2007), uma arquitetura de mensuração deve prover orientação, integração e visão dos processos da organização, de maneira torná-los mais eficientes, controlados e alinhados aos objetivos do negócio. Além disso, conforme apresentado por Baker e Wallace (2007, p. 37), "pode-se responder SIM em um questionário que pergunta se são utilizados *softwares* antivírus na organização, quando na realidade o *software* pode estar mal configurado, mantido de forma inadequada e instalado somente em algumas estações". Por isso, a arquitetura de mensuração e auditoria deve fornecer de maneira clara a situação da Gestão da Segurança da Informação.

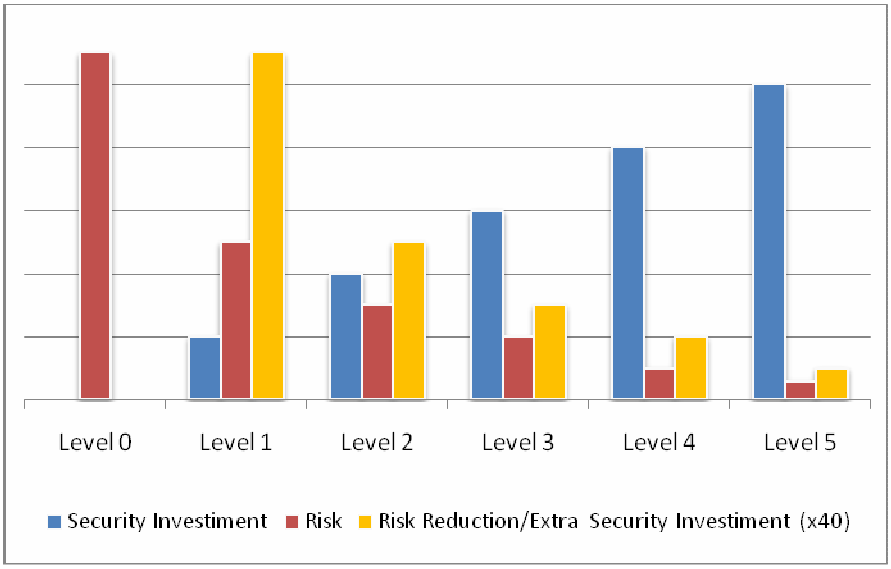

Figura 4.7 - Relação Risco x Investimento do modelo ISM3
(Fonte: ISM3 Consortium, Information Security Management Maturity Model, Version 2.0)

Desta forma, os níveis de maturidade do modelo ISM3 fornecem orientações imprecisas e ineficientes para o processo de gestão da segurança da informação, além de não garantir que as implementações de segurança estarão alinhadas aos objetivos do negócio da

organização, dado que o modelo determina quais atividades devem ser praticadas em cada nível de maturidade, o que pode conflitar com a necessidade e realidade da organização.

Uma análise sucinta permite definir que os níveis de maturidade propostos pela arquitetura de mensuração do modelo ISM3 dependem do tamanho da organização, e a interpretação disso é que: Organizações de pequeno porte não têm a mesma capacidade de organizar os processos de segurança como empresas de grande porte e, por isso, são menos seguras.

Uma análise superficial do paradoxo de Mayfield permitiria validar esta definição gerada pelo modelo ISM3. No entanto, a curva "U" do Paradoxo não determina exatamente em que momento o custo de permitir ou negar o acesso a toda humanidade começa a aumentar. Sendo assim, não é difícil perceber que processos mais eficientes, gerenciados, controlados, mensurados e integrados conseguem manter um baixo custo de implementação e operacionalização para certo percentual da humanidade do que processos menos eficientes.

A máxima eficiência poderia ser definida como um processo que apresenta um custo muito baixo ou mínimo entre o limite dos dois extremos, e somente nos extremos seu custo é máximo ou infinito.

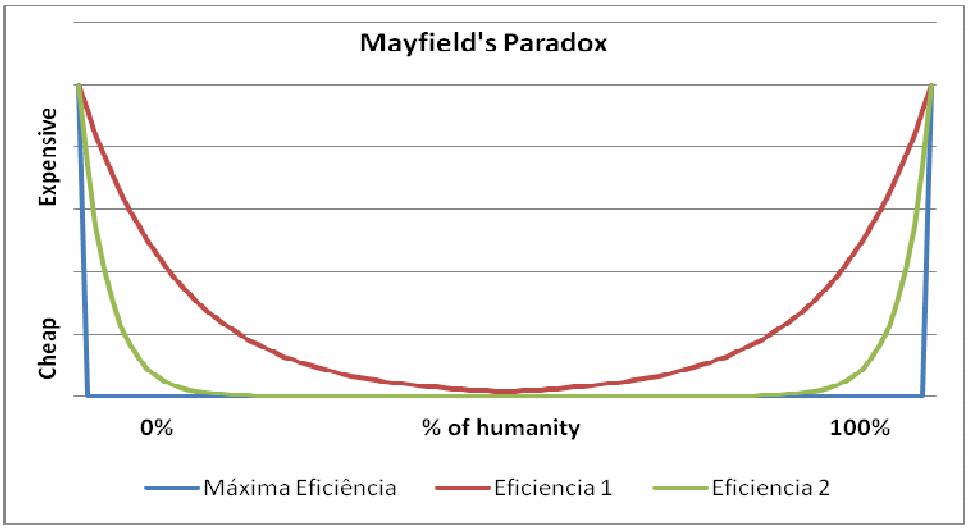

Figura 4.8 - Eficiência na gestão de processos otimiza a curva do Paradoxo de Mayfield

Por meio desta análise é possível vislumbrar que organizações podem atingir níveis superiores de segurança independente do seu tamanho e do volume de investimentos em segurança. Para isso, é importante desenvolver e utilizar modelos de Gestão da Segurança da Informação que ofereçam métodos de gestão e controles eficientes.

4.6. ISO/IEC 27001:2005

> O padrão internacional ISO/IEC 27001:2005 foi desenvolvido para prover um modelo que norteie a implantação, implementação, operacionalização, monitoramento, revisão, manutenção e melhoria dos Sistemas de Gerenciamento da Segurança da Informação (*Information Security Management Systems – ISMS*). (ISO, 2005b, p. v).

O padrão ISO/IEC 27001:2005 apresenta requisitos e controles gerais para o estabelecimento e gerenciamento de sistemas de segurança da informação, que pretendem ser aplicáveis a todo tipo de organização, independente do tipo e tamanho.

O padrão é composto por cinco cláusulas:

- *Information Security Management System;*
- *Management Responsability;*
- *Internal ISMS audit;*
- *Management review of the ISMS;*
- *ISMS improvement*.

O padrão utiliza o ciclo de Deming (*Plan – Do – Check – Act*) como modelo de referência para estruturar e coordenar a aplicação e a interação entre os controles de segurança da informação, conforme figura 3.3. No entanto, não estabelece atividades estruturadas e co-relacionadas, permitindo a formação de cadeias de resultados por meio de *inputs* e *outputs*.

Podemos afirmar que o padrão abrange os aspectos relacionados ao negócio da organização, dado que existem práticas e controles que estabelecem a identificação e a avaliação das necessidades de negócio. Além disso, existem controles responsáveis pela verificação periódica da conformidade e adequação dos sistemas, assegurando a continuidade e eficiência do gerenciamento da segurança.

O padrão destaca que durante as etapas de planejamento e identificação das necessidades do negócio devem ser levados em consideração os requisitos regulatórios, legais e contratuais.

Apesar de conter práticas básicas para o estabelecimento de Sistemas de Gestão da Segurança da Informação, o padrão sugere a utilização das práticas indicadas no ISO/IEC 17799:2005 como mecanismos de controle para o tratamento dos riscos.

Apesar dessas características, o padrão não abrange todos os Elementos Gerais de Gestão da Segurança da Informação. Por exemplo, inexiste no padrão uma arquitetura para mensuração e auditoria dos processos de gestão - existentes em modelos como o CobiT e o SSE-CMM.

No entanto, por ser um padrão internacional, o seu uso trás benefícios conhecidos, como a definição de termos e conceitos, linguagem universal da segurança da informação, permitindo a troca de experiências entre organizações.

Enquanto o padrão ISO/IEC 17799:2005 provê práticas bases de segurança da informação, o padrão ISO/IEC 27001 descreve os requisitos para implementar, manter, revisar e auditar um sistema de gestão da segurança da informação. Desta forma, a aplicação conjunta das normas provê uma base sólida para o desenvolvimento de modelos de Gestão da Segurança da Informação.

4.7. RESUMO DA ANALISE DOS MODELOS

A análise dos modelos de Gestão de Segurança da Informação nos permite validar a afirmação que, isoladamente, os modelos atuais não oferecem a melhor solução absoluta para a gestão da segurança da informação, visto que nenhum deles endereça completamente os domínios da GSI e muitos são para finalidades específicas.

Observamos ainda que os modelos orientados a gestão de TIC apresentam um conjunto de processos, procedimentos e mecanismos de controle para gerir a Tecnologia da Informação e Comunicações das organizações, e apesar de não serem exclusivos para gestão da Segurança da Informação, apresentam módulos que tratam deste assunto. Provavelmente esta prática deve-se ao histórico da Segurança da Informação que está associado à segurança de computadores. No entanto, “segurança de computadores não é um objetivo, é um meio de alcançar um objetivo, o qual é a segurança da informação” (CHESWICK; BELLOVIN; 1994, p. 08).

Alguns desses modelos não específicos de Segurança da Informação, como o CobiT, são orientados aos níveis hierárquicos estratégicos das organizações e, por isso, abordam a segurança da informação de maneira geral, como um processo único e repleto de indicadores, necessitando do auxílio de modelos mais específicos para as etapas de execução. Além disso,

o excesso de detalhes e controles do modelo torna-o complexo e marginaliza os níveis operacionais da organização.

Outros modelos, como o ITIL e o SSE-CMM, são específicos para certas atividades e, por isso, suas práticas de segurança não endereçam todas as possíveis questões de segurança da informação. No entanto, são modelos eficientes de segurança naquilo que se prestam.

Os padrões ISO/IEC 17799:2005 e 27001:2005 oferecem uma lista de controles e práticas mundialmente aceitas e testadas, que visam estabelecer segurança. Por isso, são excelentes guias de referência e úteis em processos de auditoria. No entanto, não se propõem a realizar o gerenciamento da segurança nas organizações e, por isso, devem ser realizadas ações adicionais em conjunto com mecanismos que permitam o planejamento, a coordenação e o acompanhamento das atividades e dos controles.

Na tabela abaixo, encontramos um mapeamento dos Elementos Gerais da GSI compreendidos pelos modelos atuais.

Tabela 4-5 - Modelos atuais da GSI e domínios compreendidos

	Controles de Segurança	Práticas Bases e Padrões	Processos e Gestão	Arquitetura de Mensuração e auditoria	Tecnologia	Aspectos Legais e Eticos	Aspectos Culturais e Sociais	Negócio	Escopo do modelo
ISO/IEC 17799	sim	sim	-	-	sim	sim	-	-	Segurança de TIC
CobiT	sim	sim	sim	sim	sim	sim	-	sim	Governança de TIC
ITIL	sim	sim	sim	-	sim	sim	-	sim	Gestão de TIC
SSE-CMM	sim	sim	sim	sim	sim	sim	-	sim	Des. Software
ISM3	sim	sim	sim	sim	sim	sim	-	sim	Segurança e Qualidade
ISO/IEC 27001	sim	sim	-	-	-	sim	-	sim	Sistemas de Segurança

Conforme consta na tabela acima, nenhum dos modelos analisados endereça os aspectos culturais e sociais da segurança da informação. Isto se deve, principalmente, ao fato

que os aspectos culturais de segurança são compostos por diversos elementos, conforme citado no estudo de Martins (2003) e resumido na tabela abaixo. No entanto, observamos que os modelos não são completamente deficientes neste quesito, afinal, a maioria deles aborda práticas e processos de treinamento, educação e responsabilidades.

Tabela 4-6 - Comparativo dos elementos da cultura de segurança

Componentes da cultura de segurança	ISO 17799	CobiT	ITIL	SSE-CMM	ISM3	27001
confiança entre pessoas	-	-	-	-	-	-
condutas éticas	sim	sim	sim	sim	sim	sim
políticas e procedimentos	sim	sim	sim	-	sim	sim
treinamento e educação	sim	sim	-	sim	sim	sim
política de segurança da informação	sim	sim	-	-	sim	-
responsabilidades e autoridades	sim	sim	sim	sim	sim	sim
incentivos e motivadores	-	-	-	-	-	-
reconhecimento e valorização	-	-	-	-	-	-

Dentre os modelos analisados, o ISM3 é o único com orientação a processos, voltado exclusivamente para a Gestão da Segurança da Informação. Talvez a principal falha do modelo seja a sua arquitetura de mensuração e auditoria, que determina o que deve ser implantado em cada nível de maturidade e tem como referência o volume de investimentos. Além disso, apenas no último nível de maturidade que o ISM3 estabelece controles para mensurar a eficiência dos processos de gestão.

Análise similar pode ser feita com o modelo CobiT, dado que somente no último nível de maturidade as práticas e os processos de segurança do modelo estão totalmente alinhados ao negócio da organização.

Apesar das deficiências isoladas, observam-se esforços para realizar a integração entre alguns modelos, como aquele feito por Von Solms (2005) que propõe o alinhamento dos

processos do CobiT às práticas do padrão ISO/IEC 17799:2005, visando estreitar as atividades de auditoria e operação. Sanchéz (2006) pretende criar uma arquitetura de mensuração, baseada em CMM, para as melhores práticas do ISO/IEC 17799:2005.

Em ambos os estudos, buscam-se métodos para suprimir as deficiências dos modelos atuais, o que converge para o endereçamento dos Elementos Gerais da GSI.

As características e os benefícios dos Elementos Gerais da GSI foram apresentados no Capítulo 3, e o seu resumo pode ser encontrado na tabela abaixo. Implicitamente, a inexistência de um desses componentes resulta em uma vulnerabilidade para a GSI e, por conseqüência, para o sucesso do negócio da organização.

Tabela 4-7 - Características e Benefícios dos Componentes da GSI

Componentes da GSI	Características e Benefícios
Controles de Segurança	• Mensuração das atividades e dos processos, permitindo acompanhar e alinhar os resultados da GSI aos objetivos do negócio.
Práticas Bases e Padrões	• Práticas eficientes de segurança, testadas e utilizadas em todo mundo.
Processos e Gestão	• Visibilidade das atividades de segurança; • Processos são repetíveis e isso agrega confiabilidade nos resultados da GSI. • Existência de uma cadeia de responsabilidade com os objetivos dos negócios, proporcionando liderança e organização à GSI.
Arquitetura de Mensuração e Auditoria	• Desenvolvimento orientado e gradual da GSI, permitindo canalizar os investimentos e identificar níveis de segurança e eficiência da GSI.
Tecnologia	• Aplicação de tecnologias na medida certa para o negócio da organização, agregando eficiência à GSI e assegurando os investimentos
Aspectos Legais, Culturais, Sociais e Éticos	• Comprometimento de toda organização com a GSI; • Comportamentos seguros são valorizados; • Conformidade com leis e aspectos éticos, garantindo a integridade da imagem da organização no mundo externo e assegurando o sucesso das suas negociações e investimentos.
Negócio	• Informações do negócio inseridas no escopo da GSI, permitindo que os objetivos da GSI estejam alinhados aos objetivos do negócio.

Desta forma, há necessidade de desenvolver um novo modelo de Gestão de Segurança da Informação, capaz de endereçar todos os componentes necessários para o sucesso da segurança da informação dentro das organizações. Sendo assim, possa garantir que os negócios sejam executados em qualquer situação operacional, que as informações sensíveis

tenham tratamentos diferenciados, que os investimentos para proteger a informação sejam compatíveis com as expectativas da organização e com o valor da informação, e garantir, ainda, que a organização se adéqüe às legislações e códigos de ética vigentes, mantendo sua imagem íntegra e transparente para investidores, auditores e sociedade.

5. UM MODELO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Neste capítulo apresentaremos nossa proposta de modelo de Gestão da Segurança da Informação, o qual chamaremos de Modelo Faseado de Gestão da Segurança da Informação ou simplesmente Modelo Faseado. Esta denominação é devido à estrutura modular de componentes e principalmente pela sua forma de aplicação e desenvolvimento gradual dentro das organizações.

O Modelo Faseado será capaz de integrar e endereçar os componentes que compreendem os Elementos Gerais da Gestão da Segurança da Informação apresentados no Capítulo 3, e por isso, deverá fornecer os níveis necessários de segurança para os negócios da organização.

O Modelo é composto por duas estruturas distintas, definidas abaixo:

- Entradas;
- Recursos de Mensuração e Controle.

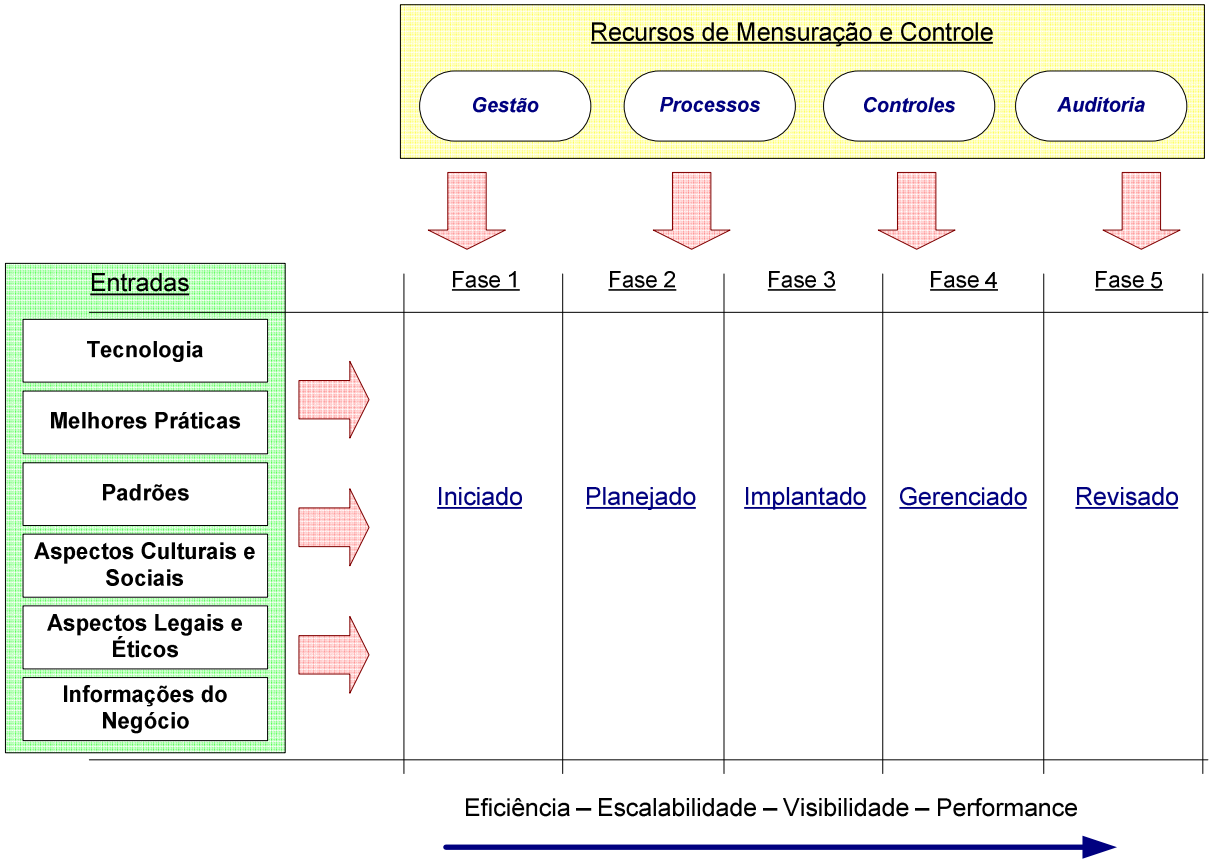

Figura 5.1 - Modelo Faseado de Gestão da Segurança da Informação

As Entradas do Modelo são compostas por uma série de elementos que formam a base de conhecimento da segurança da informação, e servem como orientadores para as tomadas de decisões e planejamento da GSI.

Os Recursos de Mensuração e Controle são as estruturas responsáveis pelo planejamento da Gestão da Segurança da Informação, e por selecionar, definir, integrar, implantar, manter e revisar os elementos apresentados pelas Entradas do Modelo. Eles também definem as responsabilidades, os objetivos e as métricas da GSI, e alinha-os aos objetivos do negócio.

Os Recursos de Mensuração e Controle são compostos por práticas de gestão, controle, processos e auditoria, e estão escalonados em cinco fases progressivas, que servem para coordenar e promover o desenvolvimento da segurança da informação dentro da organização, além de garantir seu processo evolutivo por meio de práticas de revisão e auditoria.

As práticas dos Recursos de Mensuração e Controle estão alinhadas e conectadas entre si, formando uma cadeia de processos e interações, facilitando a coordenação e agregando visibilidade à Gestão da Segurança da Informação.

Assim, as estruturas que compõem o Modelo Faseado são complementares, e a forma como se dá a integração entre elas permite que o Modelo seja capaz de se adaptar às necessidades e às mudanças das organizações, garantido proteção aos investimentos e alinhamento com os negócios.

5.1. ENTRADAS DO MODELO

As Entradas do Modelo constituem o núcleo de práticas e guias de segurança do Modelo Faseado, além de ser uma fonte diretora para normas, leis, códigos de ética e informações do negócio. As Entradas do Modelo Faseado são compostas por:

- Tecnologia;
- Melhores Práticas;
- Padrões;
- Aspectos Culturais e Sociais;
- Aspectos Legais e Éticos;

- Informações do Negócio.

O objetivo das Entradas é assessorar os processos da Arquitetura de Mensuração e Controle no planejamento e nas definições de quais implementações devem ser feitas, quais regras, leis ou melhores práticas devem ser seguidas, servindo como referência para todos os níveis do Modelo Faseado de Gestão da Segurança da Informação.

No entanto, diferente da norma ISO/IEC 17799:2005, as Entradas do Modelo não pré-determinam padrões e os aspectos relacionados à tecnologia e melhores práticas, informações do negócio, aspectos culturais, legais, éticos e sociais. Estes devem ser identificados, analisados e definidos previamente, por cada organização, durante os níveis 1 e 2 do Modelo Faseado. Devido ao dinamismo desses elementos e à particularidade de negócio de cada organização, torna-se impraticável que as Entradas contenham, de maneira pré-definida, quais atividades as organizações devem praticar, quais leis devem ser seguidas, como conscientizar os funcionários e como obter sucesso nos negócios.

5.1.1. Tecnologia

Sabe-se que Segurança da Informação não é meramente um problema de natureza técnica, no entanto, conforme apresentado por Harris (2004), a tecnologia pode auxiliar em diversas áreas de negócio e necessidades de segurança da organização, como exemplo, proporcionar métodos confiáveis de autenticação e acesso à informação, seja por meio de biometria, utilizando identificadores de voz, verificadores de retina e assinaturas dinâmicas, ou por meio de senhas, utilizando protocolos criptográficos e funções *hash*[16].

Os benefícios de aplicar a tecnologia nos processos e práticas de Gestão da Segurança da Informação são inúmeros, dentre eles, conforme apresentado por CertiNews (2008), está o aumento na confiabilidade e agilidade nas transações de negócio, redução de custos operacionais e aumento nos lucros e arrecadações, alcançados por meio de certificados digitais em transações de imposto de renda, notas fiscais eletrônicas e compras *on-line*.

[16] De acordo com Bellare, M. e Rogaway, P. (2005), funções h*ash* são definidas como funções ou algoritmos que comprimem mensagens de comprimentos arbitrários, ou quase arbitrários, para um resultado de comprimento fixo, denominado *digest*, além de ser computacionalmente inviável encontrar uma mensagem que corresponda à um dado *digest*, ou encontrar duas mensagens que produzam o mesmo *digest* (esta última propriedade é conhecida como Resistência à Colisão). Definição similar é encontrada na padronização do NIST (*National Institute of Standards and Technology*) (2000).

No entanto, a aplicabilidade da tecnologia para uso da segurança da informação não se limita à criptografia e à proteção de dados computacionais, tendo aplicações na proteção física e na salvaguarda de documentos e mídias magnética (EUROPEAN..., 2008), bem como no combate à pirataria e à falsificação de produtos e marcas (SANT'ANNA, 2008), por meio do desenvolvimento de compostos, proporcionando proteção à imagem da organização, entre outros.

Destacamos que não há limites quando se trata de aplicação de tecnologia para o negócio. Portanto, o objetivo da Entrada Tecnologia não é descrever ou pré-listar as inovações existentes ou as possíveis aplicações da tecnologia para a segurança da informação, mas apresentar um elemento essencial que deve ser abordado, identificado e analisado pela Gestão da Segurança da Informação, a fim de obter sucesso nos objetivos pretendidos.

A tecnologia deve ser aplicada em conformidade com as necessidades de segurança do negócio, balanceando os níveis de investimentos com o valor do bem protegido, cuidando para que os custos não excedam os benefícios.

Além disso, cabe considerar que inovações tecnológicas são acompanhadas de adaptações, mudanças de paradigmas e aprendizado, e conforme apresentado por Martins (2003), treinamento, conhecimento e educação são elementos que compõem e formam a cultura de segurança de uma organização. Portanto, as Entradas de Tecnologia não devem ser analisadas isoladamente, mas em conjunto com todos os elementos que compõem as Entradas do Modelo.

5.1.2. Melhores práticas

As melhores práticas em segurança da informação são compostas, normalmente, por listas de técnicas e procedimentos comumente aceitos, testados e difundidos em organizações que utilizam segurança da informação, e normalmente derivam de um processo contínuo de desenvolvimento do estudo da segurança da informação dentro das organizações.

As melhores práticas não são verdades absolutas e a simples aplicação delas não garante que a organização estará livre de incidentes de segurança, no entanto, servem como ponto de partida para a identificação, a seleção e o estabelecimento das práticas e

procedimentos de segurança, assim como podem ser utilizadas como guias em processos de auditoria e conformidade.

Não faz parte do escopo da Entrada Melhores Práticas do Modelo Faseado pré-listar ou pré-definir as possíveis melhores práticas de segurança da informação, como ocorrem nos modelos ISM3, CobiT e ISO/IEC 17799:2005. Há inúmeras listas de melhores práticas[17] que abordam diversas áreas da Gestão da Segurança da Informação, assim como também existem práticas descritas por fabricantes de produtos, que detalham os meios mais seguros de configurar, armazenar, transmitir, publicar e acessar os dados através de seus produtos. Portanto, a criação de uma nova lista concorrente de melhores práticas de segurança é um esforço desnecessário.

Não obstante, cada organização requer um nível específico de segurança, e conforme apresentado por Peltier (2003), somente após uma análise do negócio da organização, da definição dos objetivos da GSI, do alinhamento desses objetivos com os objetivos de negócio e de uma avaliação prévia dos riscos e dos custos, é possível determinar quais práticas e controles de segurança a organização deve adotar.

A adoção imediata de melhores práticas incorre nas deficiências apontadas no CobiT e no ISM3, os quais apresentam, respectivamente, uma base de guias e práticas que não endereçam todas necessidades dos níveis operacionais, e práticas pré-determinadas que podem não corresponder às necessidades do negócio da organização.

Destacamos ainda que, conforme apresentado por Martins (2003), a eficiência e a eficácia dos controles e práticas de segurança dependem do comportamento das pessoas que estão ao redor dessas práticas, portanto, o comportamento humano e a cultura organizacional devem ser levados em consideração no momento da seleção dos controles e das práticas de segurança.

Desta forma, a Entrada Melhores Práticas tem o objetivo de identificar as práticas e controles de segurança, nortear os processos de seleção dessas práticas, e fazer as interações com os outros elementos que compõem as Entradas do Modelo Faseado. Isso permite que a GSI estabeleça, de maneira precisa, as práticas e os controles de segurança necessários para que a organização atinja e mantenha os seus níveis esperados de segurança.

[17] Podemos destacar BRASIL (2003), NIST (EUA, NIST, 2005), ISO (2005), RFC 2196 (1997).

5.1.3. Padrões

Padrões, normalmente, são recomendações testadas e aceitas pelas organizações e, de maneira geral, são definidas por instituições normativas. Por tais motivos, os padrões costumam ser práticas amadurecidas e confiáveis.

Uma dos benefícios de se adotar padrões nas decisões da GSI é a linguagem universal que eles proporcionam, permitindo trocas de experiências entre organizações e facilitando os processos de auditoria, negociações de fusões de empresas ou verificação de conformidade com alguns requisitos. O Tribunal de Contas da União[18], por exemplo, apesar de reconhecer que a norma ISO/IEC 17799:2005 não tem poder lei, utiliza-a em seus acórdãos e decisões, conforme apresentado por Brasil (2007). Procedimento similar é adotado pelo ITGI (2006a), no qual as práticas do Modelo CobiT são mapeadas e correlacionadas às práticas da norma ISO/IEC 17799:2005.

Assim como ocorrem com as Melhores Práticas, nem sempre os Padrões devem ser seguidos indiscriminadamente, há necessidade de avaliações prévias e correlação deles com as necessidades do negócio. No entanto, alguns padrões possuem um caráter muito mais normativo do que simples recomendações, e por isso, é importante que sejam observadas as diferenças entre os padrões e as melhores práticas.

O objetivo desta Entrada é identificar os padrões que estabelecem e normatizam as melhores práticas de segurança, provendo orientações aos processos de seleção de práticas e controles do Modelo Faseado, e possibilitando que a GSI estabeleça procedimentos universais.

Portanto, assim como ocorrem nas demais Entradas do Modelo Faseado, os padrões devem ser identificados, avaliados e definidos pela Gestão da Segurança da Informação, e também devem ser integrados às demais Entradas, formando uma base de informações para serem analisadas e definidas pelos níveis 1 e 2 dos Recursos de Mensuração e Controle.

[18] A Constituição Federal de 1988 conferiu ao Tribunal de Contas da União (TCU) o papel de auxiliar o Congresso Nacional no exercício do controle externo. As competências constitucionais privativas do Tribunal constam dos artigos 71 a 74 e 161.

5.1.4. Aspectos legais e éticos

De acordo com Harris (2004), os aspectos legais compreendem elementos importantes para o sucesso da Gestão da Segurança da Informação, pois eles regem as obrigações das organizações, determinam as responsabilidades, definem as penalidades, delimitam os limites de atuação e criam as proteções legais, além de proporcionarem oportunidades de negócios.

São comuns leis que determinam as responsabilidades e obrigações pela proteção das informações, como exemplo a lei Norte-Americana Sarbanes-Oxley (SOX), citada no Capítulo 1, que impõe responsabilidades sobre os executivos das organizações pela veracidade do conteúdo dos relatórios financeiros, afetando todas as empresas do mundo com capitais negociáveis no mercado de ações estadunidense. Encontramos ainda o Ato Norte-Americano de Responsabilidade e Portabilidade dos Seguros de Saúde, HIPAA – *Health Insurance Portability and Accountability Act*, (apud Harris (2004)), que define os procedimentos para armazenamento, uso e transmissão de informações médicas e de saúde das pessoas, garantindo a privacidade e autenticidade dos dados, impondo ainda responsabilidades e penalidades sobre os manuseadores dessas informações.

No âmbito da administração pública federal brasileira, encontramos o Decreto nº 4.553 de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, o qual determina, por exemplo, que "para a guarda de documentos ultra-secretos e secretos é obrigatório o uso de cofre forte ou estrutura que ofereça segurança equivalente ou superior, (...), e na impossibilidade de se adotar o disposto, os documentos ultra-secretos deverão ser mantidos sob guarda armada"(BRASIL, 2002, art. 30).

Os aspectos legais proporcionam ainda condições para o desenvolvimento de pesquisas, inovações e tecnologias, através de leis que asseguram a propriedade intelectual e industrial[19], e leis que regulamentam as patentes[20], conferindo "ao seu titular o direito de impedir terceiro, sem o seu consentimento, de produzir, usar, colocar à venda, vender ou importar produtos objeto de patentes"(BRASIL, 1996, art. 42). Dessa forma, é importante que a Gestão da Segurança da Informação utilize estes artifícios para a obtenção de sucesso nos seus objetivos.

[19] Brasil (2004)
[20] Brasil (1996)

Além das leis, as questões contratuais e acordos comerciais devem ser compreendidos pelos Aspectos Legais do Modelo Faseado, de maneira que sejam assegurados meios de legitimar, validar e comprovar as identidades de documentos digitais, vinculando-os ainda às obrigações e responsabilidades das organizações. De maneira sucinta, as características de não-repúdio[21] dos meios digitais devem ser avaliadas pela GSI, de sorte identificar o que constituem documentos legais nas trocas de informações, e neste quesito, a tecnologia vem dando grandes contribuições.

De acordo com Pinheiro (2007), os aspectos legais contribuem para identificar os limites de ação da Gestão da Segurança da Informação, principalmente nos processos de auditoria, na criação de políticas de aceitação de uso[22], nas investigações de fraudes e de outros incidentes. Dado que as garantias de privacidade e sigilo de informações pessoais são regidas por leis, a GSI deve compreendê-las para evitar invasões ou danos legais que prejudiquem os negócios das organizações.

"Só porque alguma coisa não é ilegal não significa que seja correta" (HARRIS, 2004, cap. 10, p. 02), pois além das leis, existem os valores da sociedade e o julgamento do que é ou não ético. Conforme definido por Valls (1989), ética é a manifestação de valores e dos costumes considerados corretos por uma realidade humana, construída histórica e socialmente a partir das relações coletivas dos seres humanos.

Os aspectos éticos devem ser levados em consideração pela Gestão da Segurança da Informação, pois compreendem elementos importantes para o sucesso do negócio e da imagem da organização. Se o aspecto ético não for observado, pode ocorrer, por exemplo, uma situação em que a organização poderá ter seu endereço eletrônico (@organizacao.com.br) inserido em uma lista negra[23] devido à mensagens eletrônicas, com conteúdos ofensivos, enviadas por seus funcionários. Isso gera situações constrangedoras para a organização, além de prejuízos por perda de produtividade ou até mesmo negócios cancelados devido à esta ação.

Por tais motivos, os Aspectos Legais e Éticos tem o objetivo de identificar, avaliar e definir os elementos legais e éticos que contribuem para o sucesso da Gestão da Segurança da Informação. Por conseqüência, auxiliam nos objetivos do negócio.

---

[21] Conforme definido no Capítulo 3, não-repúdio é impedir que uma entidade participe de uma dada operação e posteriormente negue esta participação

[22] Documento que define o que pode e o que não pode ser feito nos vários componentes de um sistema, incluindo tipo de tráfego de redes, tipos de acesso e outros, descrevendo ainda as penalidades. Definição encontra na RFC 2196, "Security Site Handbook", September 1997.

[23] Lista negra é o nome dado a uma lista de endereços eletrônicos classificados como maliciosos, utilizada pelos sistemas de correio eletrônico para restringir o acesso de *emails* oriundos desses endereços.

5.1.5. Aspectos culturais e sociais

De acordo com Gaunt (2000), Andress (2000) e Von Solms (2000), o sucesso da implantação de modelos de GSI depende muito mais da inseminação dos conceitos de segurança dentro da cultura da organização do que de configuração de equipamento, implantação de tecnologia, aplicação de normas e decretos. Por isso, conforme apresentado por OECD (2002), todos participantes da organização são peças importantes para o sucesso do programa de Segurança da Informação. A cultura é expressa em valores coletivos e costumes, que normalmente resulta em ações, comportamentos e maneiras de interagir dentro de um ambiente.

De acordo com Von Solms e Von Solms (2004), programas de treinamento e educação desempenham um papel importante na disseminação dos conceitos de segurança da informação. No entanto, para que a segurança incorpore a cultura da organização é preciso algo mais. Segundo Martins (2003) a cultura organizacional de segurança é composta por confiança, condutas éticas, políticas e procedimentos, treinamento e educação. Para este autor, é necessário que seja dada devida importância e incentivo ao comportamento de segurança da informação dentro das organizações. Além disso, devem existir políticas para nortear o comportamento humano e descrever as expectativas de segurança da organização. Não obstante, a liderança e a participação intensa dos executivos da organização são peças chaves para o sucesso da inseminação da cultura da Segurança da Informação na organização.

Diante desses fatos, os Aspectos Culturais e Sociais do Modelo são responsáveis por planejar, coordenar e moldar a cultura de segurança dentro da organização. Por meio da Arquitetura de Mensuração e Controle, os Aspectos Culturais e Sociais da organização são identificados, avaliados e definidos, garantindo que estejam sempre em conformidade com as necessidades de segurança da organização.

5.1.6. Informações do negócio

As informações do negócio constituem o principal elemento de Entrada do Modelo Faseado, e certamente, o principal elemento de qualquer modelo de Gestão. De acordo com Koontz e O'Donnell (1974), a mais fundamental das cinco funções administrativas é o

planejamento, visto que envolve seleção entre alternativas de cursos de ação futuros para a organização, além de definir os seus objetivos e metas e determinar maneiras de alcançá-los. “O planejamento é responsável por contrabalancear as incertezas e as modificações, por assegurar um funcionamento econômico, por facilitar o controle e por estabelecer os objetivos da organização” (KOONTZ; O’DONNELL, 1974, p; 48).

Segundo Abell (1991), a definição do negócio da organização é o ponto de partida para o seu planejamento estratégico, e o principal responsável pela participação de uma organização no mercado e pelo seu sucesso.

Esta Entrada do Modelo Faseado tem o objetivo de coletar informações do negócio da organização para assessorar a GSI na elaboração do seu planejamento, na definição dos seus objetivos, metas e escopo, e nos processos de identificação e seleção das demais Entradas.

Assim, a Entrada Informações do Negócio é responsável por identificar os objetivos do negócio, os fatores críticos de sucesso da organização, a estrutura organizacional, o ramo de atuação, a parte central do negócio (*core business*), as áreas de mercado, as relações de negócio, os planos e estratégias organizacionais, e enfim, todo elemento que contenha informações sobre o negócio.

Não faz parte dos objetivos desta Entrada definir o que a organização faz, mas sim, elencar os elementos relativos ao negócio da organização para que os processos da Arquitetura de Mensuração e Controle do Modelo Faseado possam alinhar os objetivos da GSI com os objetivos do negócio, garantindo os níveis necessários de segurança para a organização.

5.2. RECURSOS DE MENSURAÇÃO E CONTROLE

Os Recursos de Mensuração e Controle são a responsáveis pelo planejamento da Gestão da Segurança da Informação, e por selecionar, definir, integrar, implantar, manter e revisar os elementos apresentados pelas Entradas do Modelo, além de definir as responsabilidades, os objetivos, as métricas e os custos da GSI, alinhando-os aos objetivos do negócio.

Os Recursos de Mensuração e Controle são compostos por práticas de gestão, controle, processos e auditoria, e estão divididos em cinco fases ou etapas, conforme descritos abaixo:

- Fase 1 – Iniciado
- Fase 2 – Planejado
- Fase 3 – Implantado
- Fase 4 – Gerenciado
- Fase 5 – Revisado

As fases servem para delimitar o campo de atuação da Gestão da Segurança da Informação, e para coordenar e promover o desenvolvimento gradual da Segurança da Informação dentro da organização, permitindo que os investimentos sejam canalizados para as necessidades do negócio, que os esforços sejam orientados para atingir os objetivos almejados, e que exista visibilidade no processo de gestão.

Em modelos como o CobiT, os níveis de maturidade representam o grau de organização da GSI e de alinhamento com o negócio. Já no caso do ISM3, os níveis representam o volume de investimento *versus* redução de riscos, e em relação ao SSE-CMM, os níveis representam a quantidade de práticas genéricas (*generic pratices*) que já foram cumpridas. Diferente desses modelos, as fases do Modelo Faseado de Gestão da Segurança da Informação representam o grau de desenvolvimento da Gestão da Segurança da Informação.

Isto significa que uma organização na Fase 1 está na etapa inicial da Gestão, ou seja, está definindo as responsabilidades pelos processos de Gestão, está conhecendo seu negócio, os elementos de Entrada que influenciam o sucesso do negócio e da Gestão e os elementos que possuem valores para a organização. A Fase 1, portanto, é uma etapa de pré-planejamento ou visão. Somente ao término da Fase 1 que a organização passará à Fase 2, e assim por diante.

Uma organização na Fase 2 já conhece o seu negócio e sabe o que tem valor e importância, assim como já identificou os elementos de Entrada que influenciam o seu negócio e as responsabilidades pelos processo de gestão. Portanto, na Fase 2, a organização deve estabelecer os objetivos da GSI, que nortearão as decisões daí por diante. Ainda nesta etapa, devem ser avaliados e definidos os elementos de Entrada (melhores práticas, leis e padrões que serão seguidos, assim como os aspectos culturais, sociais e éticos que devem ser abordados). Devem ser determinados e definidos ainda os custos da GSI, assim como o nível de segurança necessário para a organização e a escala de atividades da GSI. A Fase 2, portanto, planeja e define os objetivos, metas, escopo e atividades da GSI.

A Fase 3 é responsável por coordenar a execução das atividades definidas na Fase 2, e por validar essas implementações, garantindo que o nível de segurança desejado pela organização seja alcançado. É na Fase 3 que são implantados os controles e as métricas da GSI, garantindo que os seus objetivos sejam alcançados e que os custos de implantação não excedam os benefícios esperados. Ou seja, ao término desta etapa as práticas de segurança estão implantadas na organização.

No entanto, é necessário que o nível de segurança implantado pela Fase 3 seja mantido. Portanto, o objetivo da Fase 4 do Modelo Faseado é manter os níveis de segurança da informação da organização conforme os objetivos e o escopo da GSI, que foram definidos na Fase 2 e implantados na Fase 3. Nesta etapa são aplicadas práticas de gestão, como gestão dos riscos, dos incidentes, das mudanças, dos custos, da cultura e outras.

A Fase 5 é responsável pela melhoria contínua do processo de gestão e pelas atividades de auditoria da GSI. Nesta etapa as informações de negócio da organização são revistas e contrapostas aos objetivos da GSI, além de estabelecer um processo de auditoria para assegurar que a GSI está cumprindo o que foi determinado e planejado.

Portanto, as fases do Modelo Faseado representam o grau de desenvolvimento da Gestão da Segurança da Informação dentro da organização. É importante destacar que as fases do Modelo Faseado não fazem e não pretendem fazer analogia aos níveis de maturidade e capacidade dos modelos CMM. A Fase 4, por exemplo, apesar de possuir a mesma nomenclatura do nível 4 dos modelos CMM, representa situações diferentes.

As fases são compostas por processos, que estão alinhados e conectados entre si, formando uma cadeia de processos e interações, facilitando a coordenação e dando visibilidade à Gestão da Segurança da Informação. De maneira geral, todo processo possui elementos de entradas (*inputs*) e elementos de saídas (*outputs*), também conhecidos como resultados. Em algumas situações os *inputs* de um processo são compostos pelos elementos dos *outputs* de outros processos, conforme representado na figura a seguir:

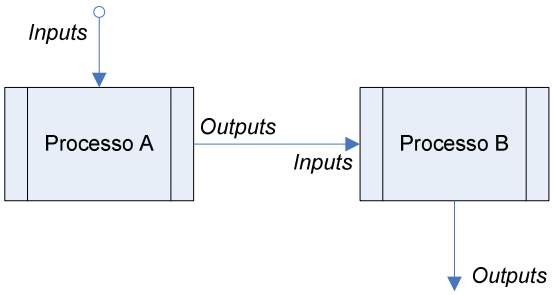

Figura 5.2 - Elementos de entrada (inputs), saída (outputs) e interação entre processos

5.2.1. Fase 1 – Iniciado

A Fase 1 é responsável pelo início das atividades da GSI ou atividades de pré-planejamento, e por isso é denominado Iniciado, e suas principais funções são:

- Estabelecer as responsabilidades pela Gestão da Segurança da Informação;
- Conhecer o negócio da organização;
- Estabelecer, de maneira preliminar, os elementos de negócio que devem ser endereçados pela GSI;
- Identificar as Entradas que influenciam no negócio;
- Identificar os valores da organização;

A etapa Iniciado é composto por cinco processos, conforme apresentados abaixo:

- Atribuição das Responsabilidades;
- Análise do Negócio;
- Escopo Preliminar;
- Identificação dos Ativos;
- Identificação das Entradas.

A organização dos processos e a maneira como eles interagem ente si estão representadas no diagrama de processos da figura abaixo:

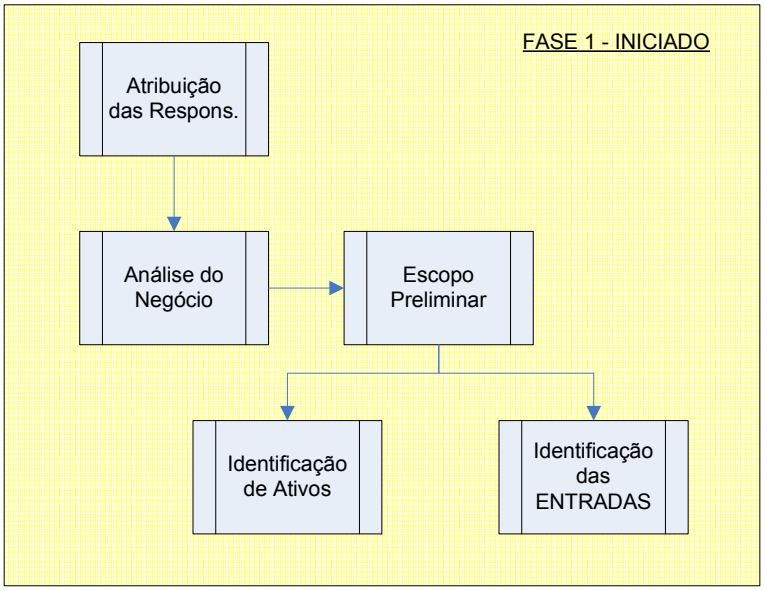

Figura 5.3 - Diagrama de Processos da Fase 1 do Modelo Faseado de GSI

5.2.1.1.Processo de Atribuição das Responsabilidades

De acordo com Koontz e O'Donnell (1974), a autoridade é o fundamento para a responsabilidade e a força de ligação na organização. A autoridade é o poder legítimo para comandar ou agir dentro de uma organização, sendo o elemento base para a coordenação de atividades e interações entre superiores e subordinados. Há, portanto, relações de autoridade e responsabilidade em toda organização. Ainda segundo Koontz e O'Donnell, apesar da importância da autoridade, evita-se o uso deste termo devido à sua sugestão de poder, e por isso, diz-se que responsabilidades são delegadas a subordinados, no entanto, o que se delega são autoridades e não responsabilidades.

Von Solms e Von Solms (2004), e o *Institute of Internal Auditors* (2001) destacam que o comprometimento dos executivos da organização é um fator crítico para o sucesso da Gestão da Segurança da Informação, sendo deles a responsabilidade legal pelas informações da organização. No entanto, cabe a eles delegar autoridades pela Gestão da Segurança da Informação, visando explicitar a toda organização as autoridades do Gerente da Segurança da Informação, suas competências, a estrutura hierárquica e os limites de atuação, evitando ferir os princípios de delegação apresentados por Koontz e O'Donnell (1974).

Assim, o processo de Atribuição de Responsabilidades – que assim o denominaremos em virtude do eufemismo da palavra, pois o correto seria Atribuição das Autoridades – deve

ser executado pelos executivos da organização, visando determinar as competências e limites de atuação da Gestão da Segurança da Informação.

Os ***inputs*** deste processo são quaisquer elementos que motivem e fundamentem as decisões dos executivos da organização na criação de uma Gestão da Segurança da Informação. Esses motivadores podem ser problemas que a organização vem enfrentando, oportunidades de negócio ou até mesmo ações para cumprimento de determinações.

O elemento de ***output*** deste processo deve ser um documento formal que delega e descreve as competências da Gestão da Segurança da Informação, estabelecendo as responsabilidades e subordinações.

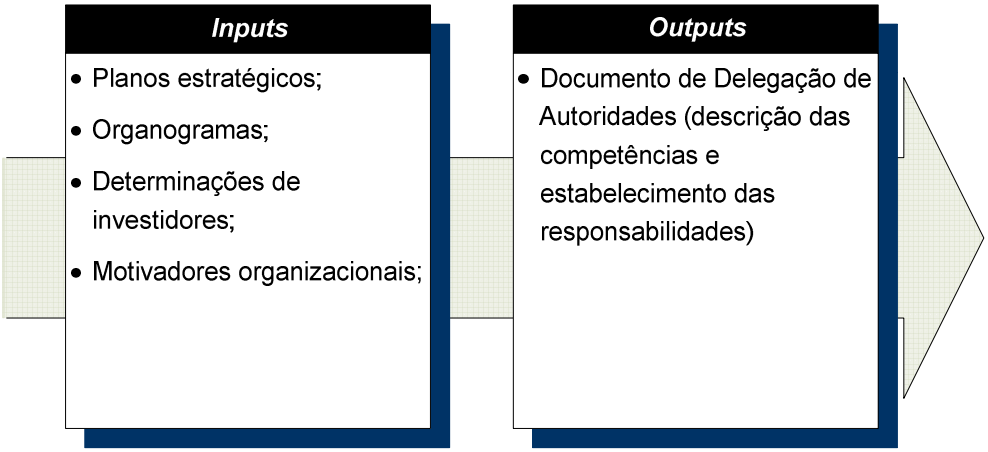

Figura 5.4 - Inputs e Outputs do Processo de Atribuição de Responsabilidades

5.2.1.2.Processo de Análise do Negócio

O processo de Análise do Negócio é a primeira atividade da Gestão da Segurança da Informação. Neste processo as informações de negócio, tais como objetivos, relações de negócio, entre outros, são apresentadas à GSI, que deve realizar uma análise visando identificar e conhecer os pontos críticos do negócio da organização, suas expectativas e requisitos de segurança.

Os ***inputs*** deste processo são as informações elencadas pela Entrada Informações de Negócio, e o Documento de Delegação de Autoridades.

As informações do negócio devem ser analisadas, de acordo com a autoridade e a competência da GSI, a fim de conhecer o negócio a ser protegido, mapear os seus pontos

críticos, identificar os requisitos de segurança e as expectativas da organização com a GSI. Por exemplo, ao implantar gestão da segurança da informação a organização criou uma expectativa ou espera algum retorno, quais são essas expectativas e o retorno esperado?

Além disso, o processo é responsável por identificar ações prévias de segurança. Por exemplo, uma organização adotava algumas ações de segurança para proteger certos projetos que eram importantes para o negócio. Desta forma, além de identificar os projetos como elementos críticos para o negócio, as ações prévias de segurança devem ser identificadas.

Esses elementos são definidos neste processo, e compõem os ***outputs*** do processo de Análise do Negócio.

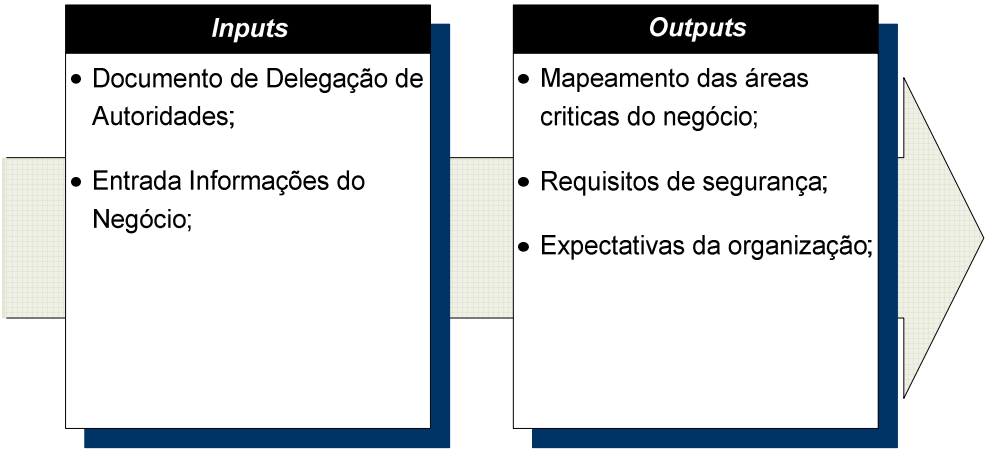

Figura 5.5 - Inputs e Outputs do Processo de Análise do Negócio

5.2.1.3.Processo do Escopo Preliminar

O processo do Escopo Preliminar é responsável por definir, de maneira preliminar, a área de atuação da GSI. Seu principal objetivo é analisar o mapeamento das áreas críticas do negócio, os requisitos e as expectativas da organização e elaborar um Plano Preliminar de Gestão da Segurança da Informação.

Este Plano Preliminar deve conter as orientações para a identificação das Entradas do Modelo Faseado, e dos elementos de valor da organização. Tais orientações devem determinar quais são os limites de atuação da GSI, indicando, por exemplo, se a GSI irá atuar apenas nos elementos de Tecnologia da Informação ou em outras áreas de negócio, como salvaguarda de documentos ou proteção de dados de projetos, e etc.

De fato, o plano é preliminar, pois não endereça todos os objetivos da GSI nem faz considerações de longo e curto prazo. No entanto, consiste em um processo importante, visto que fornece orientações para os esforços de identificação das Entradas e elementos de valores, evitando, por exemplo, perda de tempo buscando elementos que enderecem questões que a GSI não tem responsabilidades, ou seja, que está fora do escopo.

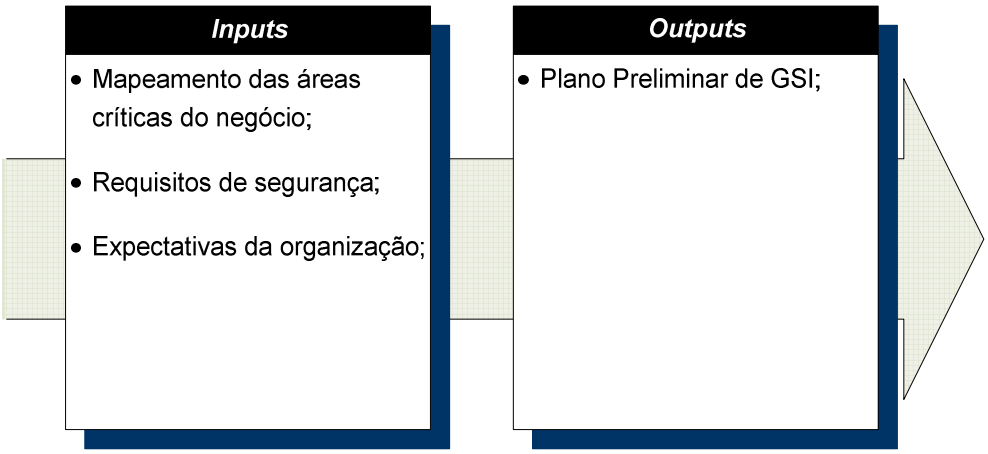

Figura 5.6 - Inputs e Outputs do Processo de Escopo Preliminar

5.2.1.4.Processo de Identificação dos Ativos

O processo de Identificação dos Ativos consiste em elencar o que contêm valor para a organização e é passível de proteção da GSI. O processo não deve se preocupar em definir os valores destes ativos ou até mesmo em classificá-los, atividades estas que serão endereçadas em etapas posteriores.

O processo visa, portanto, montar um banco de dados dos elementos importantes para o negócio da organização, obedecendo às definições do processo de escopo preliminar.

Portanto, o Plano Preliminar de GSI é o elemento de ***input*** deste processo, e o Banco de Dados de Ativos é o elemento de ***output***.

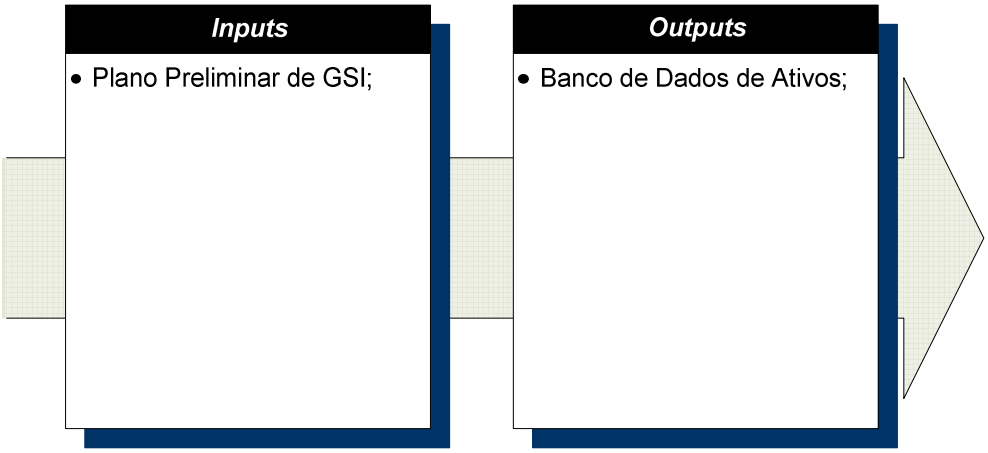

Figura 5.7 - Inputs e Outputs do Processo de Identificação dos Ativos

5.2.1.5.Processo da identificação das Entradas

Este processo tem o objetivo de elencar todas as possíveis Entradas que endereçam o escopo preliminar da GSI, sendo, portanto, relevantes para o negócio da organização. O Plano Preliminar de GSI é o elemento de ***input*** deste processo, e as possíveis Melhores Práticas, Padrões, Aspectos Legais e Éticos, Aspectos Culturais e Sociais, e Tecnologia são identificados ao término deste processo, compreendendo os ***outputs*** do processo.

Não cabe ao Processo de Identificação das Entradas promover análises desses elementos de ***outputs***. Portanto, se o escopo da GSI é proteger os dados da organização, então devem ser elencados todos os elementos que descrevem as melhores práticas de salvaguarda, as leis e os aspectos éticos que regem a proteção de arquivos e outros, sem considerar, por exemplo, o custo de implantar certas melhores práticas, ou a relevância das leis. Estas atividades serão endereçadas em etapas posteriores, nas quais serão analisadas as viabilidades de custos, as condições de riscos e as aceitações.

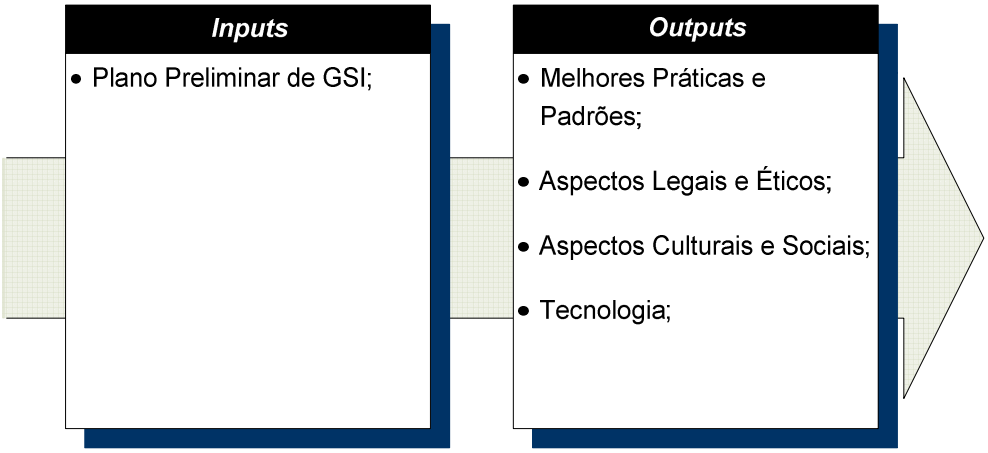

Figura 5.8 - Inputs e Outputs do Processo de Identificação dos Ativos

5.2.2. Fase 2 – Definido

A Fase 2 é responsável pelo planejamento da Gestão da Segurança da Informação, e pela definição dos elementos que compõem a GSI, e por isso é denominado Planejado, e suas principais funções são:

- Estabelecer os Objetivos, Metas e Escopo da Gestão da Segurança da Informação;
- Estabelecer a Política de Segurança da organização;
- Avaliar e definir as Entradas que serão adotadas pela GSI;
- Definir o nível de segurança aceitável pela organização;
- Definir os custos de implantação do nível de segurança aceitável pela organização;
- Identificar os riscos do negócio e definir os níveis de aceitação dos riscos;
- Classificar os ativos da organização;
- Definir as atividades da GSI;

A etapa Definido é composto por sete processos, conforme apresentados abaixo:

- Definição do Plano de Gestão da Segurança da Informação;
- Definição da Política de Segurança;
- Avaliação dos Custos;
- Avaliação dos Riscos;

- Avaliação das Entradas;
- Classificação dos Ativos;
- Definição das Atividades;

A organização que se encontra na Fase 2 do Modelo Faseado já identificou as suas expectativas por segurança, já identificou os seus ativos, assim como os seus elementos de Entrada que influenciam o seu negócio e as responsabilidades pelos processos de gestão. Os processos da etapa Definido são muito importantes para a GSI, pois além de estabelecerem o nível de segurança necessário para a organização, o que implica decisões de custos e riscos, os seus resultados (***outputs***) nortearão os dois níveis subseqüentes, que são etapas de implantação e manutenção.

A organização dos processos e a maneira como eles interagem ente si estão representadas no diagrama de processos da figura abaixo:

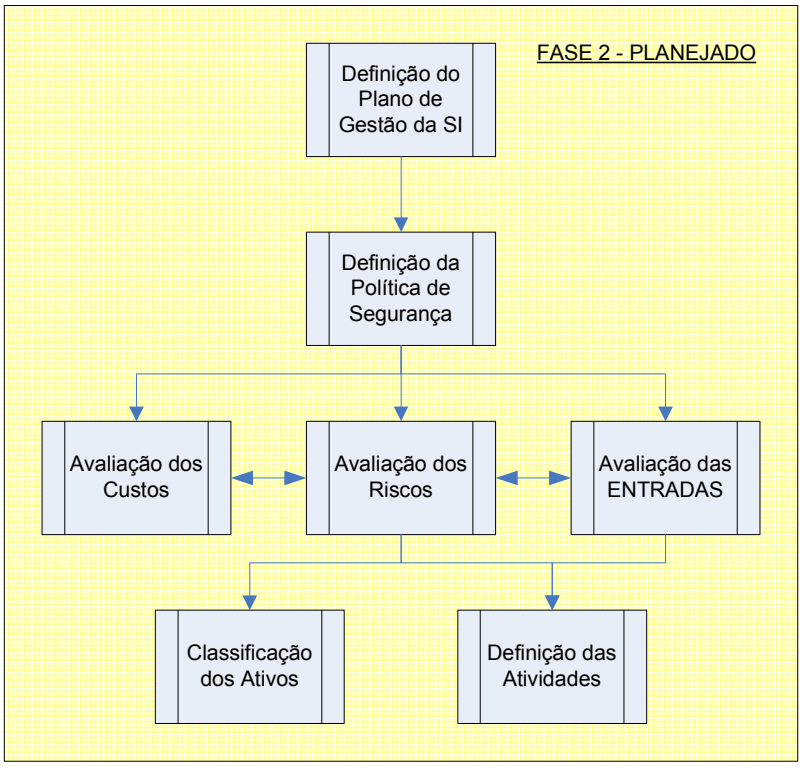

Figura 5.9 - Diagrama de Processos da Fase 2 do Modelo Faseado de GSI

5.2.2.1.Processo de definição do Plano de Gestão da Segurança da Informação

"A identificação de objetivos é o primeiro passo no planejamento e requer cuidadosa atenção. Ninguém pode especificar como irá cumprir um objetivo vago e indeterminado. Cumpre identificar os objetivos de forma que se possa determinar o sucesso ou o fracasso final." (KOONTZ; O'DONNELL, 1974, p. 128)

Segundo Koontz e O'Donnell (1989), objetivos são os fins pelos quais as pessoas lutam, e alternadamente são chamados de *finalidades, missões, objetivos, metas* ou *alvos*. Ainda segundo Koontz e O'Donnell, os objetivos representam as esperanças e os desejos da organização, no entanto, devem ser razoavelmente passíveis de realização.

> Para que haja algum sentido prático no estabelecimento de metas e objetivos nos planejamentos, é necessário que eles sejam verificáveis, do contrário, inexistirá uma medida de eficácia, pois é impossível saber se um objetivo vago está ou não sendo atingido. Também não pode haver medida de eficiência se não forem conhecidos tanto os *outputs* como os *inputs*. (KOONTZ; O'DONNELL, 1989, p. 580)

Outro passo importante do planejamento é a determinação do escopo do trabalho, identificando os elementos que devem ser endereçados pela gestão e a sua abrangência. Neste processo, o escopo deve ser definido por meio de análises mais profundas e detalhadas das expectativas e dos requisitos do negócio, já que existem mais informações sobre o negócio, como ativos e elementos de Entrada.

Desta forma, compõem os ***inputs*** deste processo os elementos de Entradas identificados, as expectativas e os requisitos do negócio, o Plano Preliminar de GSI e o Banco de Dados de Ativos. O principal ***output*** deste processo é o Plano de Gestão da Segurança da Informação, que deve conter os objetivos e o escopo da GSI.

De acordo com Harris (2004), para que um plano de GSI de uma organização tenha sucesso é necessário que ele contenha uma abordagem estratégica das necessidades da organização, compreendendo todos os domínios da GSI. No entanto, abordagens detalhadas e específicas devem ser endereçadas em planos específicos. Desta forma, para Harris, o Plano de GSI deve nortear a seleção e elaboração dos planos menores, como avaliação das melhores práticas que devem ser implantadas, leis que devem ser seguidas e treinamentos que devem ser ministrados.

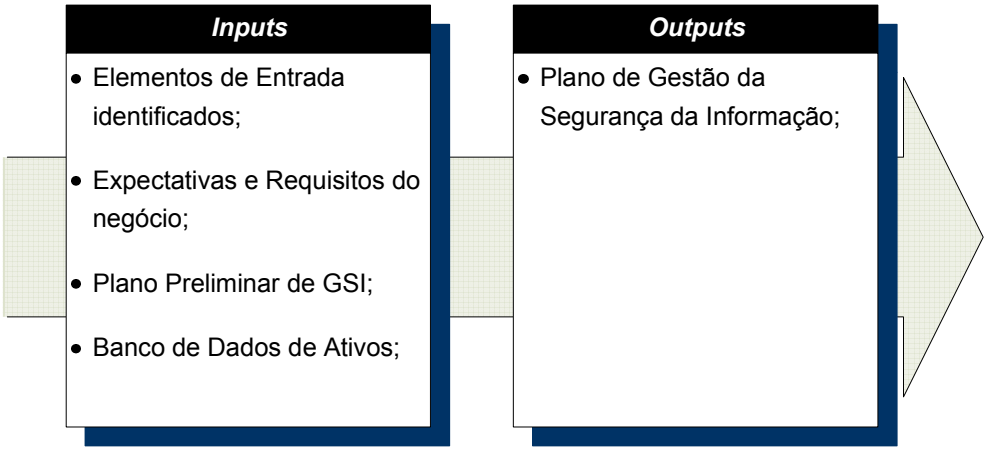

Figura 5.10 - Inputs e Outputs do Processo de Definição do Plano de GSI

5.2.2.2.Processo de Definição da Política de Segurança

De acordo com Harris (2004), a Política de Segurança de uma organização deve enfatizar, de maneira clara e sucinta, os objetivos da Gestão da Segurança da Informação e demonstrar que esses objetivos estão alinhados com os objetivos do negócio. Ainda segundo Harris, o principal objetivo da Política de Segurança é explicitar a delegação de autoridade da alta direção da organização para a Gestão da Segurança da Informação.

A ação de delegar autoridades, ou de maneira eufêmica, delegar responsabilidades, demonstra o comprometimento da alta direção da organização com a GSI, e que de acordo com NIST (EUA, NIST, 2006) e OECD (2002) é um fator importante para o sucesso da Gestão da Segurança da Informação.

Entendimento similar ao de Harris é encontrado no padrão ISO/IEC 17799:2005. Ambos mencionam ainda que a Política de Segurança deve ser um documento de fácil entendimento, pois servirá como ponto de referência para toda organização.

Segundo a RFC 2196 – *Site Security Handbook* (1997), a Política de Segurança da Informação (PSI) deve conter os objetivos da GSI, assim como as responsabilidades de cada membro da organização. No entanto, a RFC 2196 defende que a PSI deve ser um documento mais detalhado, contendo, por exemplo, guias de aquisição de tecnologia, especificando os requisitos de segurança que produtos devem ter, e as definições do que pode e do que não pode ser feito ou acessado na rede.

Harris (2004) sugere que sejam criadas políticas específicas quando houver a necessidade de endereçar questões mais detalhadas, como o que pode ou o que não pode ser acessado.

A RFC 2196 é extremamente voltada para a segurança de computadores e sistemas que estão publicados na Internet e, portanto, é uma referência para organizações que tem como negócio a prestação de serviços na Internet.

Desta forma, o objetivo do processo de Definição da Política de Segurança é divulgar os objetivos, o escopo e as responsabilidades da GSI, demonstrando, inclusive, o comprometimento da alta direção da organização com o sucesso da GSI. Assim, os principais ***inputs*** deste processo são o Plano de GSI e o Documento de Delegação de Autoridades, e o resultado deste processo é a Política de Segurança da Informação.

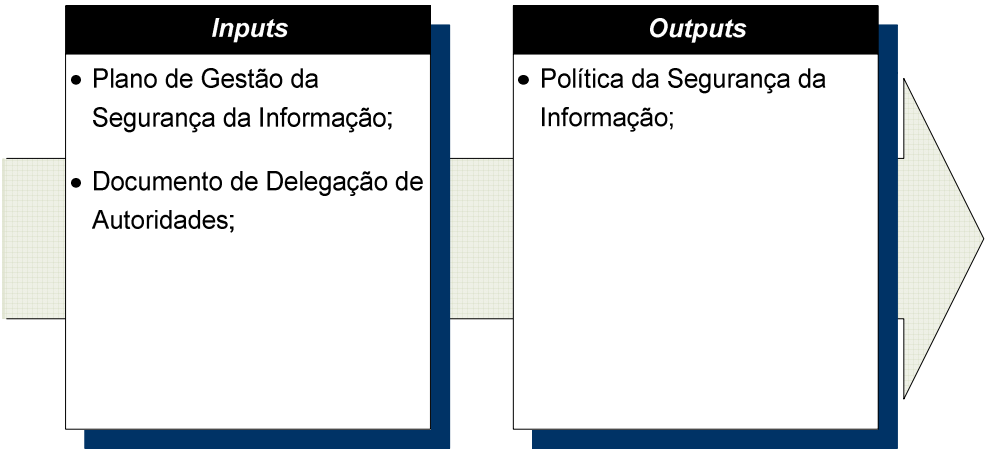

Figura 5.11 - Inputs e Outputs do Processo de Definição da Política de Segurança

5.2.2.3.Processo de Avaliação dos Custos

O Processo de Avaliação dos Custos visa identificar o valor dos ativos da organização, o quanto é necessário para manter este ativo, e o custo da perda deste ativo. Determina, portanto, os valores necessários para alcançar e manter os níveis de segurança desejáveis pela organização, assim como os custos por não cumprir regulamentações e códigos de ética.

Segundo Harris (2004), a determinação dos custos dos ativos é o passo inicial para se determinar quais mecanismos de segurança devem ser colocados em prática e qual o orçamento da GSI.

De fato, determinar os custos dos ativos permite à GSI definir Entradas eficientes para o negócio da organização e realizar análises mais precisas sobre a aceitação e a redução dos riscos. Por tais motivos, o processo de Avaliação dos Custos está interligado ao processo de Avaliação dos Riscos e ao processo de Avaliação das Entradas, que em conjunto, formam a base de análises da GSI.

Ilustramos a integração desses três processos da seguinte forma:

1. O processo de Avaliação dos Custos analisa o Banco de Dados de Ativos, as Entradas, e os objetivos do negócio e determina o valor desses ativos;

2. O processo de Avaliação dos Riscos analisa os riscos atuais da organização, de acordo com os objetivos, com o Banco de Dados de Ativos e com as Entradas, e determina os Níveis Aceitáveis de Riscos da organização.

3. O processo de Avaliação das Entradas analisa as Entradas, os Níveis Aceitáveis de Riscos da organização e os objetivos do negócio e define as Entradas necessárias para endereçar os objetivos e os níveis necessários de segurança.

4. O processo de Avaliação dos Custos analisa os custos de implantar e manter os níveis necessários de segurança da organização com as entradas definidas, e determina se esse custo é superior aos benefícios esperados. Também analisa se a falta de uma Entrada pode acarretar em prejuízos para a organização.

5. O processo de Avaliação dos Riscos avalia os níveis de aceitação, redução e transferência dos riscos, conforme custos determinados pelo processo de Avaliação dos Custos e Entradas definidas pelo processo de Avaliação das Entradas, e define os níveis aceitáveis de riscos.

Desta forma, compreendem os ***inputs*** do processo de Avaliação dos Custos o Banco de Dados de Ativos, o Plano de GSI, as Entradas e os Níveis Aceitáveis de Riscos. O resultado deste processo é a Definição dos Custos da GSI.

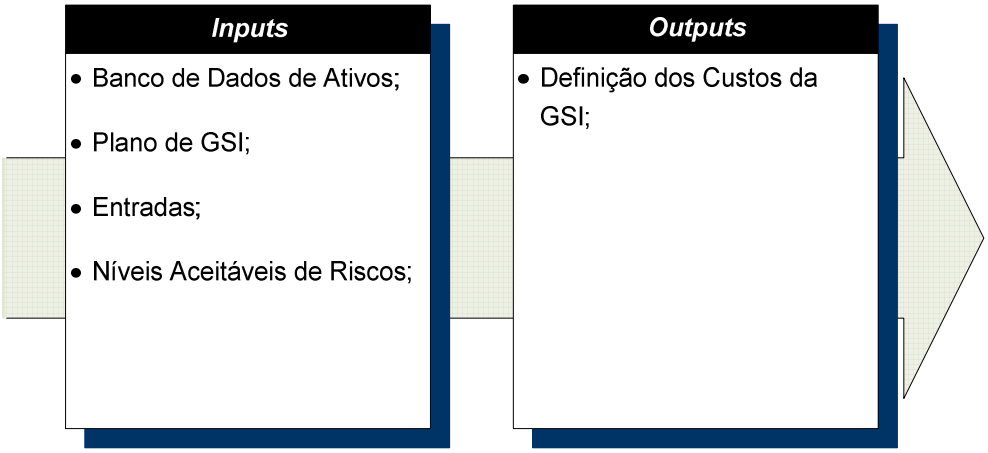

Figura 5.12 - Inputs e Outputs do Processo de Avaliação dos Custos

5.2.2.4.Processo de Avaliação dos Riscos

De acordo NIST (EUA, NIST, 2006), Chapin e Akridge (2005) e ISO (2005), a avaliação de riscos oferece métodos eficientes para identificar vulnerabilidades e selecionar controles e práticas de segurança que visam alcançar os níveis de segurança necessários para a organização.

O processo de Avaliação dos Riscos visa definir os níveis aceitáveis de riscos da organização, explicitando os riscos que devem ser reduzidos, aceitados ou transferidos[24], proporcionando diretrizes para os processos de Avaliação dos Custos e Avaliação das Entradas.

Segundo a publicação 800-100 do NIST (EUA, NIST, 2006), a análise de riscos deve compreender métodos de caracterização do sistema a ser protegido, identificação das vulnerabilidades e riscos, análise de impactos, análise de probabilidades de ocorrência, recomendação dos controles de proteção e documentação dos resultados.

Os principais ***inputs*** do processo são: O Banco de Dados de Ativos, o Plano de GSI, as Entradas e a Definição dos Custos da GSI. O elemento de ***output*** do processo é a Definição dos Níveis Aceitáveis de Riscos.

[24] De acordo com Harris (2004), reduzir os riscos significa executar atividades e contramedidas de segurança, reduzindo a probabilidade um evento negativo acontecer. A aceitação dos riscos, segundo Harris, significa aceitar a probabilidade do risco acontecer, isto se deve por alguns motivos, entre eles o custo de redução dos riscos. Ainda segundo Harris, transferir os riscos significa contratar um empresa de seguros, visando minimizar o impacto do evento negativo.

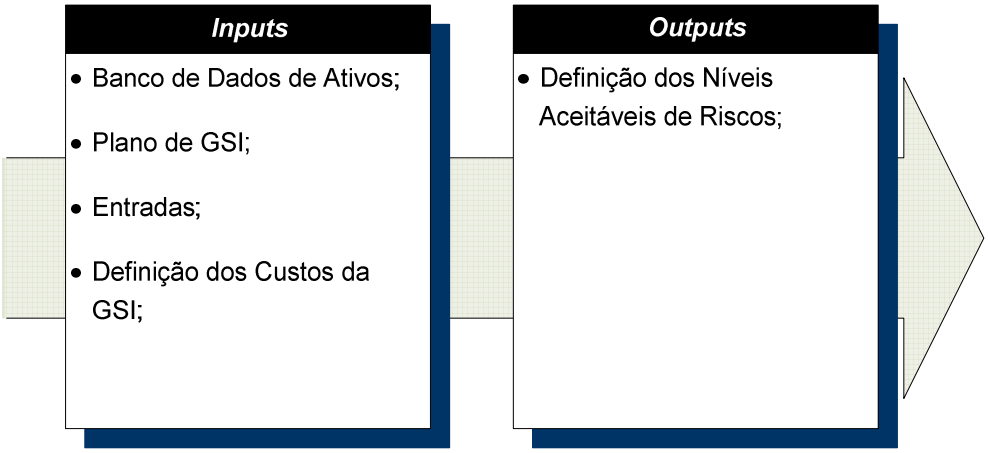

Figura 5.13 - Inputs e Outputs do Processo de Avaliação dos Riscos

5.2.2.5.Processo de Avaliação das Entradas

O objetivo do processo de Avaliação das Entradas é definir os controles, melhores práticas, tecnologias, leis, padrões, códigos de ética e aspectos culturais e sociais mais eficientes para as necessidades de segurança do negócio, obedecendo aos objetivos e escopo definidos no plano de Gestão da Segurança da Informação.

Compreendem os ***inputs*** deste processo as informações das Entradas relacionadas ao negócio e identificadas no processo de Identificação das Entradas, da fase 1, os Níveis Aceitáveis de Riscos, o Plano de GSI, o Banco de Dados de Ativos e a Definição dos Custos da GSI.

O principal ***output*** do processo é a Definição das Entradas. O processo deve promover uma seleção e análise das Entradas, e não somente selecionar um padrão de melhores práticas ou uma lei. Assim, o resultado deste processo é a definição de quais Entradas (Ex.: cláusulas 9.1 e 10.3 da ISO/IEC 17799:2005) devem ser implementadas para alcançar os níveis de segurança definidos no processo de Avaliação dos Riscos.

Suponhamos que o processo de Avaliação dos Riscos identificou que o procedimento de acesso remoto à *intranet* da organização é falho, e definiu que a organização precisa de mecanismos de proteção de acesso remoto. O processo de Avaliação das Entradas deve avaliar, dentre as possíveis entradas, a que oferece o melhor custo/benefício para a organização.

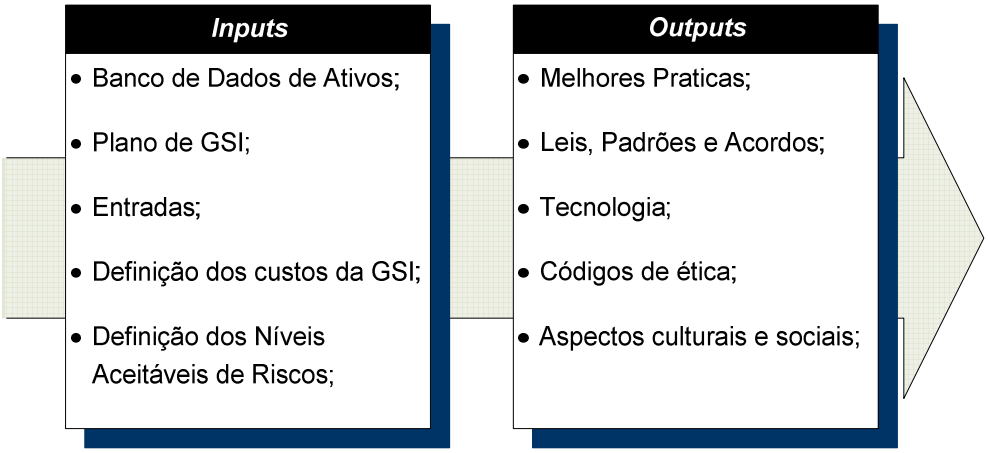

Figura 5.14 - Inputs e Outputs do Processo de Avaliação das Entradas

5.2.2.6.Processo de Classificação dos Ativos

O processo de Classificação dos Ativos tem como objetivo consolidar as informações de custos, riscos e controles de proteção dos ativos, além de classificar a importância e a criticidade do ativo para a organização, montando uma base de informações dos elementos de valor para a organização.

Dentre os benefícios de consolidar as informações dos ativos da organização estão a rápida análise de incidentes de segurança e impactos sobre os negócios, facilitando procedimentos de mudanças e futuras análises; agilidade nos processos de auditoria e checagem dos objetivos.

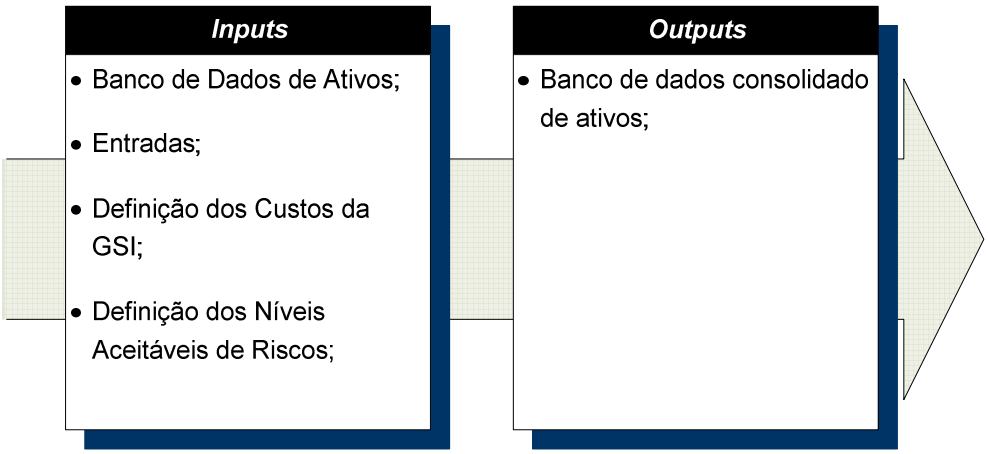

Figura 5.15 - Inputs e Outputs do Processo de Classificação dos Ativos

5.2.2.7.Processo de Definição das Atividades

O processo de Definição das Atividades é o responsável pela elaboração do Plano de Execução das Atividades. Este plano descreve, detalhadamente, os procedimentos e as atividades que devem ser adotados para atender às definições dos níveis de riscos, custos e entradas. Além disso, o plano deve definir os controles antecipados que devem ser adotados nos processos de implantação da segurança da informação.

Como todo plano, o Plano de Execução das Atividades deve conter objetivos e escopo, no entanto, os objetivos e o escopo do plano de execução das atividades não apresentam nenhum mistério, dado que seu objetivo é implementar as entradas definidas pelo processo de Avaliação das Entradas, alcançando os níveis de riscos definidos no processo de Avaliação dos Riscos, ao custo definido no processo de Avaliação dos Custos. E o escopo está descrito no Plano de GSI.

Segundo Koontz e O'Donnell (1989), existem dois tipos de controles: Os que visam prever situações futuras e evitar desvios antes que eles aconteçam, além de nortear o rumo das atividades, e por isso são chamados de controles antecipados; e os que visam verificar se as atividades continuam nos rumos estabelecidos e detectam os desvios à medida que vão ocorrendo. "Talvez não haja elemento mais importante num sistema apropriado e eficaz de controle que os controles antecipados"(KOONTZ; O'DONNELL, 1989, p. 580), que devem ser estabelecidos nas etapas de planejamento.

Ainda segundo Koontz e O'Donnell (1989), os controles adequados devem refletir a natureza e as necessidades da atividade, acusar prontamente os desvios, voltar-se para o futuro, apontar as exceções em pontos críticos, ser objetivos, ser flexíveis, refletir o modelo organizacional, ser econômicos, ser compreensíveis, e por fim, acarretar medidas corretivas.

Desta forma, um dos objetivos do processo de Definição das Atividades é estabelecer os controles antecipados das atividades de segurança da informação. Ferramentas de análise de redes de planejamento, como PERT (*Program Evaluation and Review Technique*) e CPM (*Critical Path Method*), são úteis na elaboração do planejamento e controle de atividades.

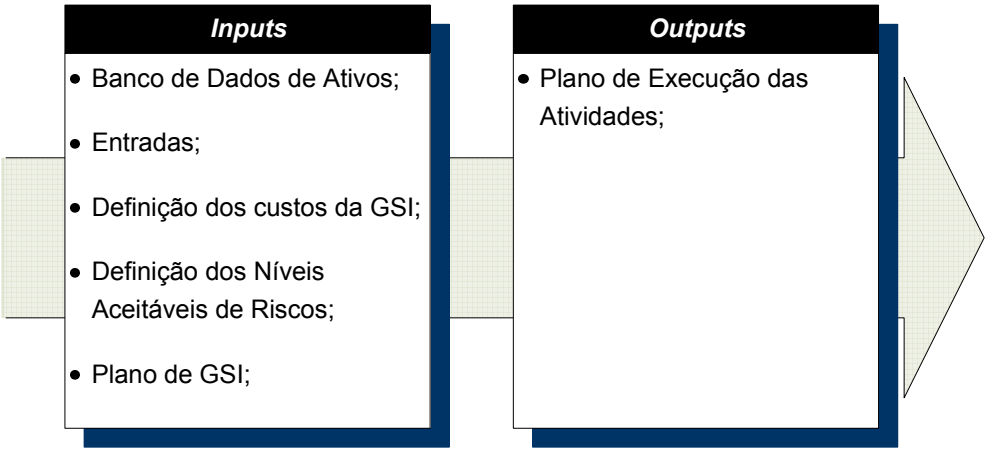

Figura 5.16 - Inputs e Outputs do Processo de Definição das Atividades

5.2.3. Fase 3 – Implantado

A Fase 3 é responsável pela execução do planejamento da Gestão da Segurança da Informação, pela coordenação das atividades definidas na Fase 2 e pela implantação das práticas e controles de segurança, e por isso é denominado Implantado, e suas principais funções são:

- Coordenar a execução das atividades definidas pela Gestão da Segurança da Informação;
- Executar o Plano de Execução das Atividades;
- Implantar os níveis de segurança necessários ao negócio;
- Acompanhar e controlar a implantação do Plano de Execução das Atividades;
- Validar a implantação dos níveis de segurança em conformidade com o Plano de GSI.

A Fase Implantado é composto por quatro processos, conforme apresentados abaixo:

- Implantação de Controles;
- Execução das Atividades;
- Verificação;
- Validação.

A Fase 3 é responsável por coordenar a execução das atividades definidas na Fase 2, e por validar essas implementações, garantindo que o nível de segurança desejado pela organização seja alcançado. É na Fase 3 que são implantados os controles e as métricas da GSI, garantindo que os custos de implantação não excedam os benefícios esperados e que haja visibilidade nos processos da GSI. Ou seja, ao término deste etapa as práticas de segurança estão implantadas na organização.

A organização dos processos e a maneira como eles interagem ente si estão representadas no diagrama de processos da figura abaixo:

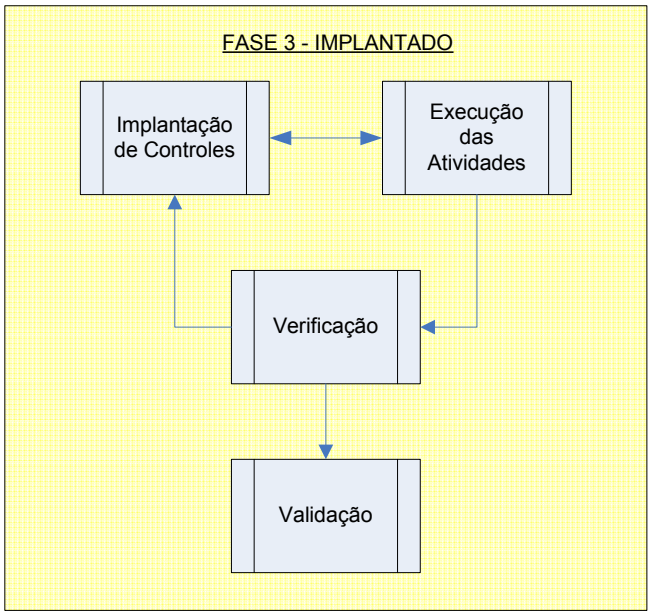

Figura 5.17 - Diagrama de Processos da Fase 3 do Modelo Faseado de GSI

5.2.3.1.Processo de Implantação de Controles

Segundo Koontz e O'Donnell (1989), a finalidade básica do controle é medir e corrigir o desempenho das atividades a fim de assegurar que os objetivos empresariais e os planos idealizados para atingi-los estão sendo realizados. Desta forma, os principais objetivos do processo de Implantação de Controles são o estabelecimento e a manutenção de técnicas de mensuração do andamento das atividades, visando garantir que os objetivos da GSI sejam alcançados, que os custos da GSI não sejam extrapolados e que os níveis de segurança sejam atingidos.

O processo de Implantação de Controles deve implantar os controles antecipados definidos no Plano de Execução das Atividades, no entanto, controles extras podem ser desenvolvidos por este processo, conforme necessidades, visando melhorar a eficiência e a visibilidade do processo de Execução das Atividades, mantendo o alinhamento com os objetivos estabelecidos no Plano de GSI.

Desta forma, compreendem os ***inputs*** deste processo o Plano de Execução das Atividades, as definições do custo da GSI, as definições dos níveis aceitáveis de riscos, a lista de atividades, a documentação dos resultados e a lista de desvios.

Os resultados deste processo são os controles adicionais de segurança, métricas de segurança e a documentação dos controles implantados.

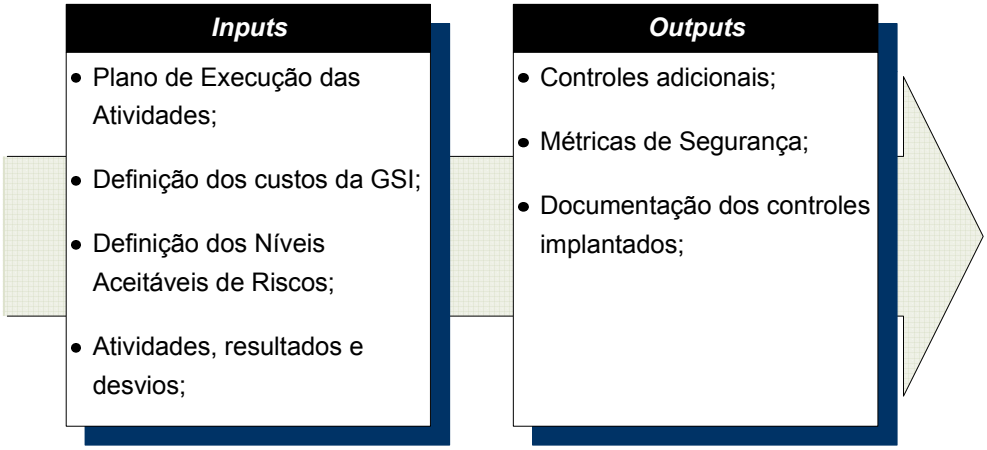

Figura 5.18 - Inputs e Outputs do Processo de Implantação de Controles

5.2.3.2.Processo de Execução das Atividades

O processo de Execução das Atividades é o responsável pela execução das atividades definidas no Plano de Execução das Atividades, e têm como norteadores, as métricas e os controles definidos no Plano e implantados pelo processo de Implantação de Controles.

Desta forma, são atribuições do processo de Execução das Atividades a organização e o seqüenciamento das atividades, além de coordenar e acompanhar os envolvidos no processo de execução e confrontar os resultados com os controles definidos.

Deve existir a interação entre o processo de Execução das Atividades e o processo de Implantação de Controles, de maneira que, o processo de Execução das Atividades siga os nortes indicados pelo processo de Implantação de Controles. Mas, em contrapartida, deve haver o repasse dos resultados obtidos ao processo de Implantação de Controles para que seja certificado que os controles estão sendo corretamente aplicados.

A Lista de Atividades Executadas e a Documentação dos Resultados, que inclui a atualização do Banco de Dados de Ativos, são os principais resultados do processo, e os elementos de ***inputs*** do processo são as atividades e os controles descritos e definidos no Plano de Execução das Atividades, e os controles adicionais.

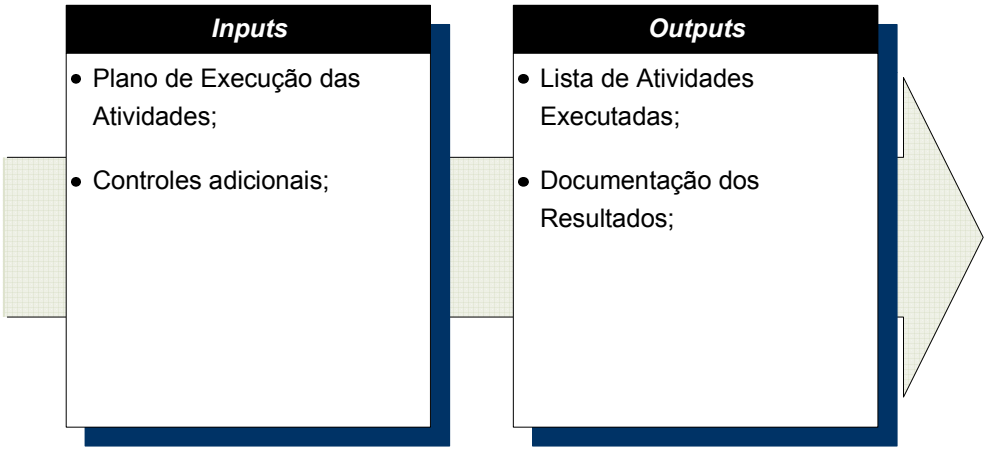

Figura 5.19 - Inputs e Outputs do Processo de Execução das Atividades

5.2.3.3.Processo de Verificação

O processo de verificação tem como objetivo identificar os desvios resultantes do processo de Execução das Atividades ou antecipar os possíveis desvios.

Os desvios são todos os resultados que estão em desconformidade ou não endereçam os objetivos do planejamento, e desta forma, representam desperdícios de recursos, falhas ou até mesmo vulnerabilidades.

Desta forma, o objetivo deste processo não é confrontar os resultados com métricas ou controles definidos, pois estas atividades já são endereçadas pelo processo de Execução das Atividades. O objetivo deste processo é confrontar os resultados com os objetivos definidos

no Plano de Gestão da Segurança da Informação, observando o cumprimento dos requisitos definidos pela organização e o atendimento das expectativas do negócio.

Assim, o processo de Verificação é responsável por assegurar que os resultados atingirão os níveis de segurança necessários pela organização dentro dos custos desejados, e com isso, a GSI cumprirá com seus objetivos.

Os principais elementos de ***output*** deste processo são os desvios ou a inexistência deles, e compreendem os elementos de ***input*** o Plano de Gestão da Segurança da Informação, a Definição dos Níveis Aceitáveis de Riscos e a Documentação dos Resultados.

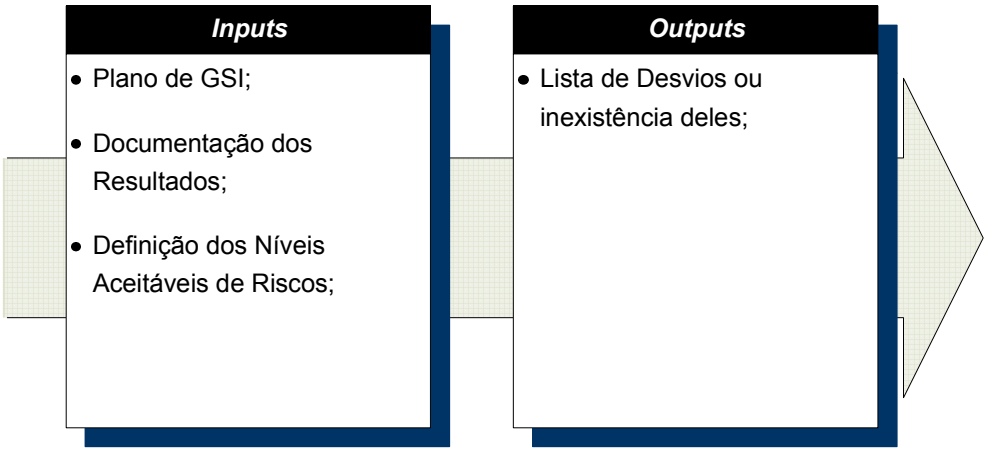

Figura 5.20 - Inputs e Outputs do Processo de Verificação

Os desvios identificados pelo processo de Verificação são utilizados como elementos de ***inputs*** no processo de Implantação de Controles, que deve proceder ao desenvolvimento de controles adicionais para que auxilie o processo de Execução das Atividades a realizar as atividades necessárias para alcançar os objetivos remanescentes.

A inexistência de desvios garante que os resultados do processo de Execução das Atividades alcançaram as expectativas da organização, e determina, portanto, que as atividades que endereçavam aquelas expectativas foram concluídas. Neste momento, o processo de Validação é iniciado.

5.2.3.4.Processo de Validação

O processo de Validação é responsável por consolidar as informações e os resultados dos processos de Implantação de Controles, Execução das Atividades e Verificação, e dar legitimidade a esses resultados através do Termo de Aceitação dos Resultados.

Desta forma, o processo de Validação delimita o encerramento da Fase Implantado por meio do Termo de Aceitação dos Resultados da GSI, que deve ser aprovado e aceito pela direção da organização ou pelos responsáveis pela delegação de autoridade à GSI, conforme definição no processo de Atribuição de Responsabilidades, ainda na Fase Iniciado do Modelo Faseado.

A inexistência de desvios, a documentação dos resultados, o Plano de GSI e a Definição dos Níveis Aceitáveis de Riscos compõem os elementos de ***inputs*** do processo, e o Termo de Aceitação dos Resultados é o elemento de ***output***.

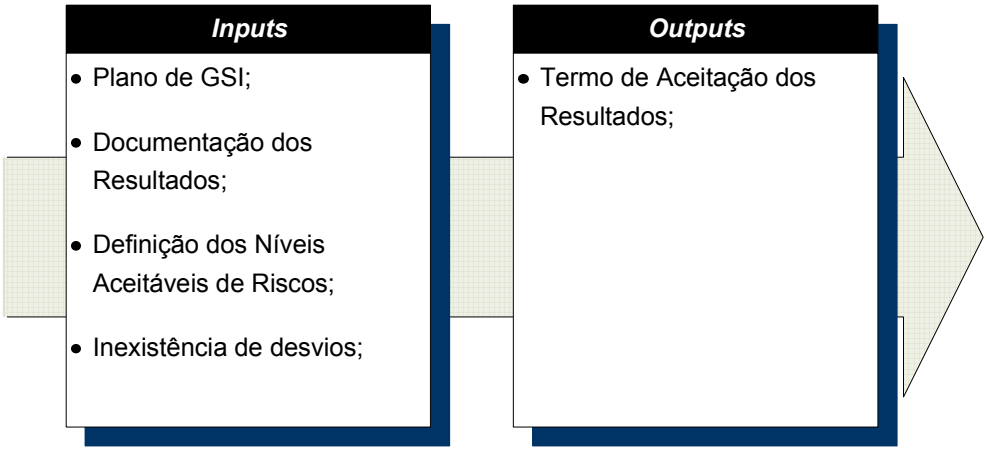

Figura 5.21 - Inputs e Outputs do Processo de Validação

5.2.4. Fase 4 – Gerenciado

A Fase 4 do Modelo Faseado de GSI é responsável por manter os níveis de segurança da organização nos patamares planejados, implantados e aceitos nas Fases 1, 2 e 3, sendo assim, o principal objetivo da Fase Gerenciado é prover estabilidade nos indicadores de segurança.

É possível considerar que uma organização está em constante evolução, e por isso, a GSI deve acompanhar essa evolução organizacional e prover um ambiente seguro para auxiliar este processo evolutivo. Desta maneira, a GSI deve estabelecer indicadores e controles de segurança para acompanhar os níveis de segurança da organização e tomar as ações cabíveis para que estes índices se mantenham estáveis, compreendam os objetivos da GSI e mantenham-se alinhados aos objetivos do negócio, e para isso, as ações da GSI devem ser organizadas e coordenadas, permitindo um acompanhamento pró-ativo e controlado.

É importante observar que a etapa Gerenciado objetiva a estabilidade dos níveis de segurança da organização, no entanto, seus processos não devem ser compostos por práticas e controles estáticos, sob pena de não acompanharem a evolução organizacional, mas por práticas dinâmicas e contínuas, capazes de endereçar situações diárias, como incidentes, mudanças, novas vulnerabilidades e riscos, novos funcionários, novas tecnologias, e etc.

A Fase Gerenciado é composto por oito processos, conforme apresentados abaixo:

- Processo de Gestão da Segurança;
- Processo de Gestão de Riscos;
- Processo de Gestão de Incidentes;
- Processo de Gestão de Problemas;
- Processo de Gestão de Mudanças;
- Processo de Gestão da Cultura Organizacional
- Processo de Gestão de Custos;
- Processo de Gestão da Configuração;

A organização dos processos e a maneira como eles interagem ente si estão representadas no diagrama de processos da figura seguinte:

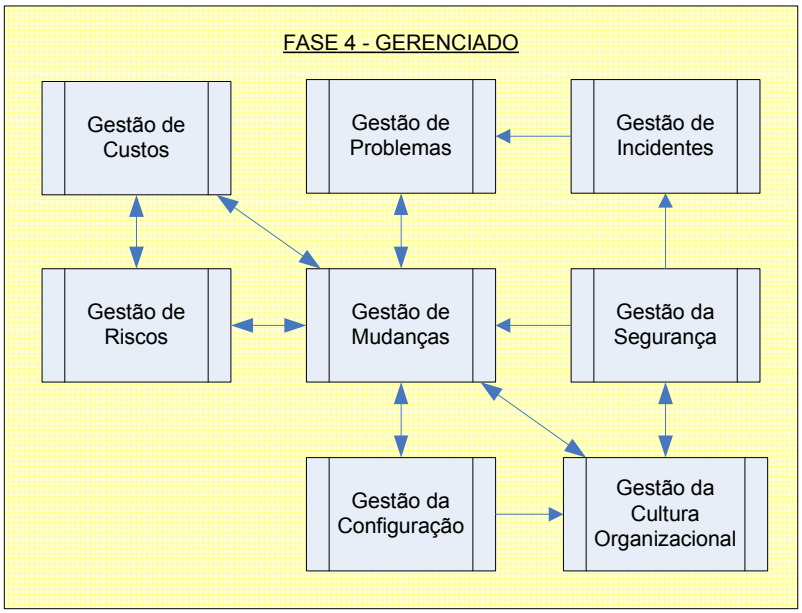

Figura 5.22 - Diagrama de Processos da Fase 4 do Modelo Faseado de GSI

5.2.4.1.Processo de Gestão da Segurança

O processo de Gestão da Segurança é o responsável por elaborar, estabelecer, implantar e acompanhar os controles, os indicadores e as métricas dos níveis de segurança para a organização. O processo é o responsável pela elaboração e manutenção dos Procedimentos de Gestão da Disponibilidade, da Continuidade, da Conformidade, da Capacidade, da Autenticidade, da Integridade e dos Níveis de Riscos da Informação.

O processo de Gestão da Segurança é, portanto, o responsável pelo monitoramento pró-ativo da segurança, utilizando indicadores e controles para determinar o curso da GSI e antecipar possíveis desvios, além de ser o responsável pela elaboração dos Planos de Reação e Contramedidas, utilizados no processo de Gestão de Incidentes.

Os Procedimentos de Gestão, os Planos de Reação e Contramedidas, os Indicadores, as Métricas, os Controles e os Desvios, compreendem os ***outputs*** do processo.

Os desvios iminentes, identificados pelo processo, são encaminhados como ***inputs*** ao processo de Gestão de Mudanças para que sejam providenciadas correções e mudanças pertinentes, a fim de evitar o desvio. No entanto, quando os desvios são identificados ao longo do curso e, portanto, já aconteceram, são encaminhados como ***inputs***, juntamente com os

Planos de Reação e Contramedidas, ao processo de Gestão de Incidentes, que deve executar os planos e outras medidas a fim de restabelecer os níveis de segurança da organização.

O Plano de Gestão da Segurança da Informação, o Banco de Dados da Configuração, o Mapa de Riscos e o Plano de Capacitação e Cultura Organizacional são os elementos de ***inputs*** do processo de Gestão da Segurança.

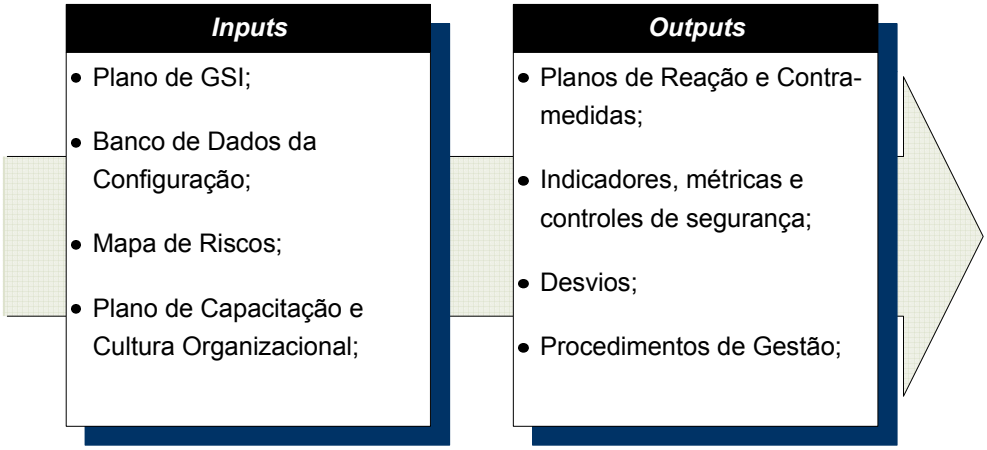

Figura 5.23 - Inputs e Outputs do Processo de Gestão da Segurança

5.2.4.2.Processo de Gestão de Riscos

O processo de Gestão de Riscos é responsável por efetuar análises contínuas dos riscos e das vulnerabilidades que impactam nos objetivos do negócio da organização, e elaborar o Mapa de Riscos dos Ativos, um documento periódico que avalia e descreve os níveis de riscos dos ativos com relação aos níveis aceitáveis de riscos da organização. Este processo determina ainda os riscos que devem ser aceitos, reduzidos ou transferidos em função da descoberta de novas vulnerabilidades, dos custos de operação ou dos Planos de Mudança.

O Mapa de Riscos dos Ativos é utilizado como elemento de ***input*** pelos processos de Gestão da Segurança, Gestão de Mudança e Gestão de Custos, norteando a elaboração dos procedimentos de Gestão, a elaboração dos Planos de Mudança para redução ou transferência dos riscos, e a definição dos Custos de Segurança, respectivamente.

A Gestão de Riscos constitui, portanto, um processo pró-ativo de identificação de novas vulnerabilidades e riscos, apresentando o Mapa de Riscos e as Solicitações de Mudança

como elementos de ***outputs***, e os Planos de Mudança, o Plano de GSI, os Custos de Segurança e a Definição dos níveis aceitáveis dos riscos como elementos de ***input*** do processo.

Existe, portanto, uma interação entre os processos de Gestão de Riscos e Gestão de Custos, de maneira que a decisão de reduzir, aceitar ou transferir os riscos deve ser analisada em conjunto com os custos de operação, de sorte que os investimentos em segurança não ultrapassem os benefícios esperados e, por conseqüência, os objetivos no negócio.

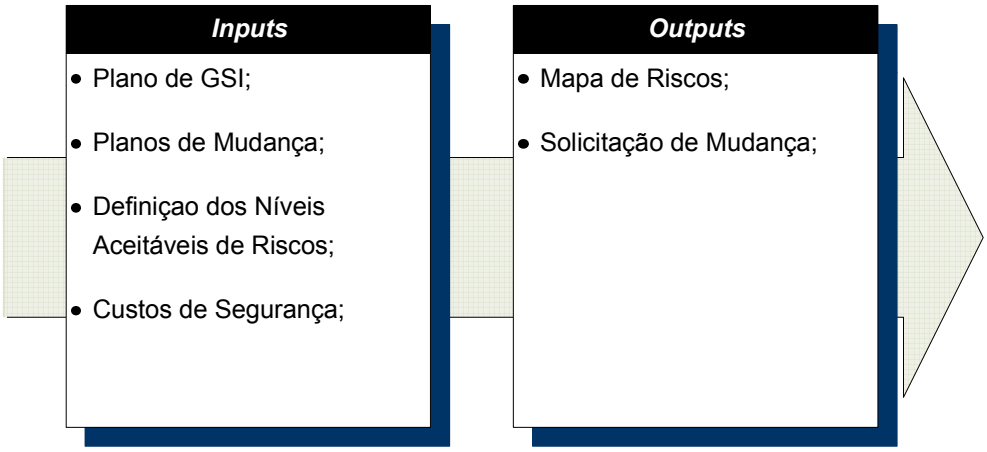

Figura 5.24 - Inputs e Outputs do Processo de Gestão de Riscos

5.2.4.3.Processo de Gestão de Incidentes

O processo de Gestão de Incidentes é responsável por restabelecer, de maneira rápida e eficiente, os níveis de segurança da organização, após incidentes[25] de segurança. O processo tem, portanto, uma característica reativa.

Os Planos de Reação e Contramedidas, e os indicadores, as métricas e os controles de segurança elaborados no processo de Gestão da Segurança constituem importantes elementos de ***input***, pois, baseado nesses documentos, o processo de Gestão de Incidentes executará suas atividades. Faz parte dos ***inputs*** do processo o Banco de Dados da Configuração, que contém a lista de ativos, seus indicadores, métricas, riscos, impactos e outras informações pertinentes, como exemplo, o tempo que determinado ativo pode ficar vulnerável, ou o tempo máximo aceito para o restabelecimento dos níveis de segurança.

[25] De acordo com Van Bon (2002), um incidente é qualquer evento que não faz parte dos padrões de operação de um serviço ou processo, e pode ser considerado como erro ou desvio, resultando em interrupções de serviços, redução da qualidade de serviços e vulnerabilidades.

O processo de Gestão de Incidentes não realiza nenhuma análise dos motivos que levaram à ocorrência do incidente, assim como não realiza nenhuma mudança no ambiente ou nos ativos, exceto as previstas nos Planos de Reação e Contramedidas. No entanto, determinados incidentes podem parecer insolúveis e requererem investigações e análises. Desta forma o processo deve propor uma solução de contorno para o incidente e solicitar uma análise de problemas, que deve ser analisada pelo processo de Gestão de Problemas.

As solicitações de análise de problemas, as soluções de contorno, e o documento de restabelecimento do nível de segurança são os elementos de ***outputs*** do processo.

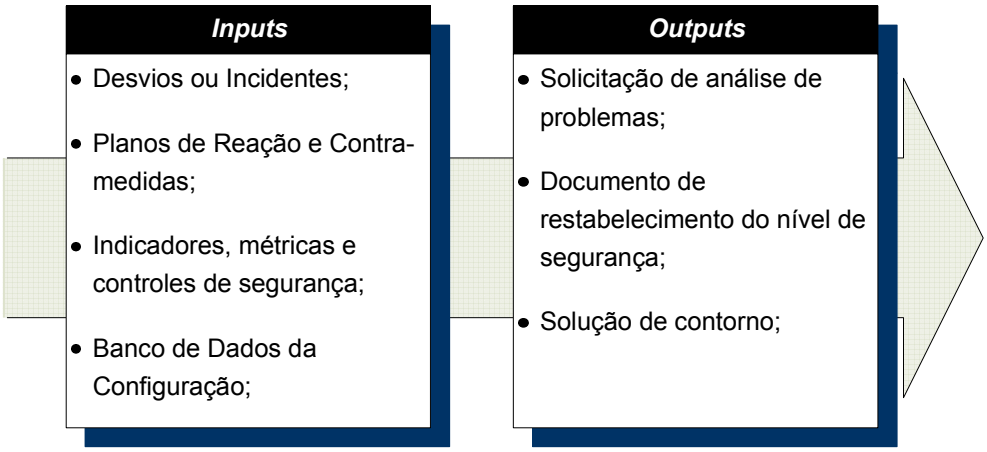

Figura 5.25 - Inputs e Outputs do Processo de Gestão de Incidentes

5.2.4.4.Processo de Gestão de Problemas

De acordo com Van Bon (2002), problema é a definição de um ou mais incidentes dos quais não são conhecidas as causas raízes, ou os motivos que levaram à ocorrência daqueles incidentes. Portanto, o objetivo do processo de Gestão de Problemas é analisar os incidentes, identificar a causa raiz deles e propor meios de corrigi-los.

Apesar de identificar o problema do incidente e os meios de saná-lo, o processo de Gestão de Problemas não é responsável por promover a sua eliminação, nem por promover mudanças nos controles ou nos procedimentos da GSI. Uma vez identificados os problemas dos incidentes e as propostas de correção, estes devem ser submetidos ao processo de Gestão de Mudanças, por meio de documento de Solicitação de Mudança, que deverá gerenciar o processo de implantação da correção.

O processo de Gestão de Problemas é também responsável por realizar análises pró-ativas, ou seja, por identificar possíveis problemas que decorreriam de mudanças. As análises pró-ativas são iniciadas por meio de Solicitação de Análise de Problemas. Consideremos, por exemplo, que o processo de Gestão de Riscos identificou nova vulnerabilidade em algum sistema protegido pela GSI, e por isso, fez uma solicitação de mudança ao processo de Gestão de Mudanças. O processo de Gestão de Mudança deve encaminhar uma solicitação de análise de problema ao processo de Gestão de Problema a fim de identificar possíveis problemas decorrentes dessa mudança.

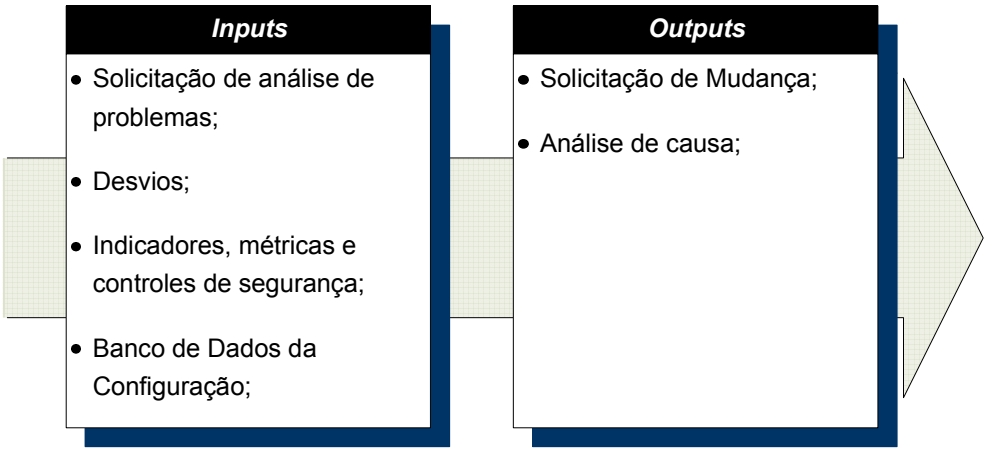

Figura 5.26 - Inputs e Outputs do Processo de Gestão de Problemas

5.2.4.5.Processo de Gestão de Mudanças

O processo de Gestão de Mudanças é responsável por planejar, organizar, coordenar, executar e registrar as mudanças de segurança, seja para correção de problemas, solução para mitigação de vulnerabilidades, ou melhorias em procedimentos e controles que visam evitar futuros desvios nos níveis de segurança da organização. Deve-se observar que “nem todas as mudanças são melhorias, mas todas as melhorias são mudanças” (VAN BON, 2002, p. 22), e portanto, devem ser submetidas ao processo de Gestão de Mudanças.

O processo de Gestão de Mudanças tem o objetivo de assegurar que as mudanças não trarão impactos negativos aos objetivos da GSI, e serão realizadas em harmonia com os demais processos da Fase Gerenciado, garantindo que haverá registros das mudanças, que haverá atualização do Banco de Dados da Configuração, que os problemas relacionados às

mudanças serão rastreados, que os riscos de uma mudança serão analisados, que as mudanças não excederão os custos de segurança e que o nível de segurança da organização será mantido.

Portanto, é de responsabilidade do processo de Gestão de Mudança realizar a integração entre os processos da Fase Gerenciado com responsabilidades de análises (Gestão de Riscos, Gestão de Problemas, Gestão da Segurança e Gestão de Custos), de maneira que todo planejamento de mudança deve ser centralizado no processo de Gestão de Mudança.

Imaginemos por exemplo que o processo de Gestão de Riscos pretende realizar uma mudança para corrigir uma vulnerabilidade de um ativo da organização, mas ao invés de encaminhar essa solicitação ao processo de Gestão de Mudança, decide solicitar ao processo de Gestão de Problemas uma análise de futuros problemas decorrentes desta mudança, a fim de planejar a melhor maneira de executar a mitigação da vulnerabilidade.

Em paralelo, o processo de Gestão da Segurança necessita de uma correção nos controles de segurança a fim de antecipar a ocorrência de certos desvios, e decide planejar a execução desta mudança, solicitando análises de problemas e análises de riscos.

Ao término do planejamento das duas mudanças, os processos de Gestão de Riscos e de Gestão da Segurança encaminham seus planos ao processo de Gestão de Mudança, que ao analisá-los, observa que são mudanças conflitantes e concorrentes, e por tais motivos são planos inexeqüíveis, e devem ser refeitos, sendo necessárias novas análises de problemas, de riscos e de custos.

Percebe-se, portanto, que o planejamento de mudanças deve ser centralizado no processo de Gestão de Mudanças, sob pena de desperdício de tempo e recursos, comprometendo o sucesso dos objetivos da GSI, além disso, o processo de Gestão de Mudança é responsável por analisar as Entradas disponíveis para endereçar as correções e melhorias pretendidas, focado em todos os elementos que compreendem a GSI, como aspectos culturais, legais, tecnologias e práticas.

As Solicitações de mudança, os desvios, o Banco de Dados da Configuração, os Custos de segurança, as Entradas, o Plano de Capacitação e Cultura organizacional e o Plano de GSI compreendem os elementos de ***input*** do processo, e os Planos de Mudança, os registros de mudanças, as solicitações de análise de riscos, de custos e de problemas são os elementos de ***outputs*** do processo.

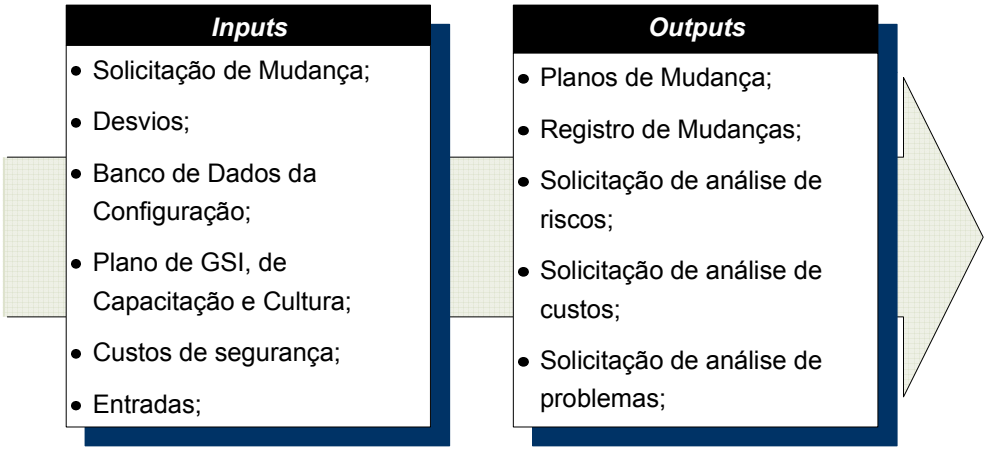

Figura 5.27 - Inputs e Outputs do processo de Gestão de Mudanças

5.2.4.6.Processo de Gestão da Cultura Organizacional

O processo de Gestão da Cultura Organizacional é responsável por elaborar, estabelecer, implantar e acompanhar os controles do comportamento humano dentro da organização, garantindo que os objetivos, responsabilidades, normas e procedimentos sejam conhecidos por todos os membros da organização, e sejam elementos de valores coletivos dentro da organização.

O processo de Gestão da Cultura Organizacional deve lidar com elementos de motivação, liderança e valores organizacionais, abordando, ainda, aspectos como condutas éticas, conhecimentos e treinamentos. É importante observar que os elementos críticos de sucesso da GSI foram identificados na Fase 2 do Modelo Faseado, e portanto, a principal função do processo de Gestão da Cultura Organizacional é dar continuidade aos programas culturais e éticos estabelecidos nos níveis anteriores, e implantar novos controles que visam manter os níveis desejados de segurança pela organização.

Assim como nos demais processos, as propostas de mudança devem ser encaminhas ao processo de Gestão de Mudança.

O Banco de Dados da Configuração, o Plano de GSI, os indicadores, métricas e controles de segurança, os Planos de Mudança e os custos de segurança, compreendem os elementos de ***inputs*** do processo.

O Plano da Cultura Organizacional, o Plano de Capacitação e as Solicitações de Mudança compreendem os elementos de ***outputs*** do processo.

O Plano da Cultura Organizacional deve endereçar tanto elementos normativos, tais como normas de segurança, termos de aceitação de uso e termos de responsabilidades, como termos de conduta e procedimentos. A principal finalidade do Plano da Cultura Organizacional é explicitar as expectativas da organização quanto ao comportamento humano, e detalhar os valores, a forma de pensar e agir da organização, servindo como norte e motivador para o comportamento humano da organização.

O Plano de Capacitação tem o objetivo de moldar os valores culturais da organização por meio de educação, treinamentos e conhecimentos.

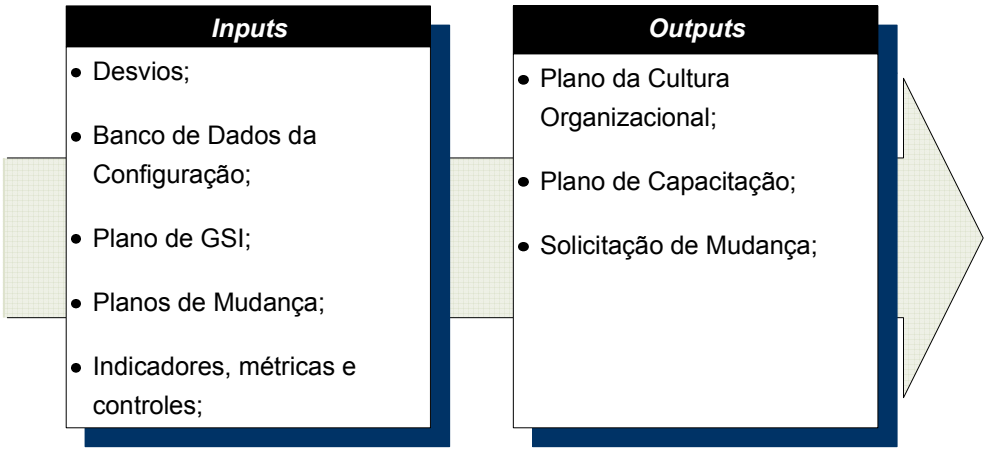

Figura 5.28 - Inputs e Outputs do processo de Gestão da Cultura Organizacional

5.2.4.7.Processo de Gestão de Custos

O processo de Gestão de Custos visa garantir que os recursos e os investimentos aplicados na proteção dos ativos da organização não excederão os benefícios esperados. Desta forma, o processo é responsável por elaborar, estabelecer, implantar e acompanhar os controles dos custos da segurança da informação.

Além dos controles, o processo deve ser responsável pela determinação dos custos futuros da GSI, ou do orçamento da GSI, garantindo que existirão recursos para manter a segurança da organização nos níveis pretendidos.

Por acompanhar e ter o controle sobre os custos de proteção dos ativos, o Processo apresenta informações importantes para a determinação do valor dos ativos da organização, sendo muito útil nas tomadas de decisões e nos processos de análises.

O processo de Gestão de Custos auxilia o processo de Gestão de Mudança na realização de estimativas dos custos relacionados às mudanças. De modo similar, o processo de Gestão de Riscos utiliza o valor dos ativos nas decisões de aceitação, redução ou transferência dos riscos.

Os Custos de Segurança e o Orçamento da GSI são os elementos de ***outputs*** do processo, e as Solicitações de Custos, o Plano de GSI e os Planos de Mudança são os elementos de ***input***.

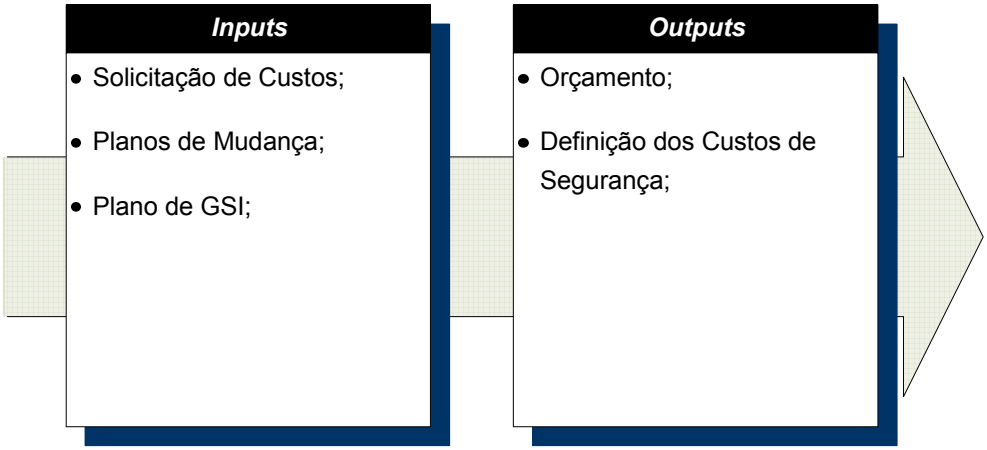

Figura 5.29 - Inputs e Outputs do processo de Gestão dos Custos

5.2.4.8.Processo de Gestão da Configuração

O processo de Gestão da Configuração é responsável pela consolidação das informações dos ativos da organização, mantendo-as atualizadas e guardando os registros das situações passadas. Desta forma, informações sobre custos, controles implantados, vulnerabilidades, níveis aceitáveis de riscos, histórico de incidentes, e outros, devem ser consolidados e mantidos pelo processo de Gestão da Configuração.

O principal elemento de ***output*** do processo é o Banco de Dados da Configuração, que estende as informações inicialmente listadas no Banco de Dados de Ativos e consolida as informações relacionadas aos ativos da organização. Os registros de mudança, o mapa de riscos, os indicadores, as métricas, os controles, os custos de segurança e o Banco de Dados de Ativos constituem os elementos de ***input*** do processo.

De acordo com Van Bon (2002), o gerenciamento da configuração contribui para um gerenciamento eficiente dos ativos da organização, pois existe uma cadeia de relacionamentos e interações entre os ativos e elementos de controle. Isto permite, por exemplo, que os processos de mudança sejam eficientes, devido à facilidade de análise das informações e dos impactos nos ativos, que as resoluções de incidentes e problemas sejam precisas, ajudando a diagnosticar os elementos envolvidos nos desvios.

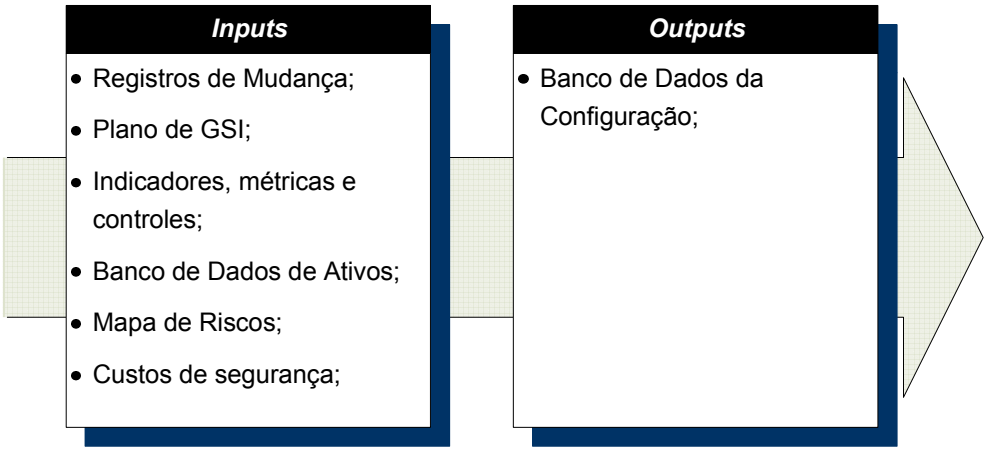

Figura 5.30 - Inputs e Outputs do processo de Gestão da Configuração

5.2.5. Fase 5 – Otimizado

A Fase 5 é responsável pela melhoria contínua do processo de Gestão da Segurança da Informação e pelas atividades de auditoria da GSI. Nesta etapa as informações de negócio da organização, as expectativas e os requisitos de segurança são revistos e contrapostos aos objetivos da GSI, além de estabelecer auditoria nos processos para assegurar que a GSI está cumprindo os objetivos estabelecidos.

Um dos objetivos da etapa Otimizado é reavaliar as necessidades de segurança da organização. Enquanto a Fase 4 do Modelo coordena esforços para manter o nível de segurança da organização, a Fase 5 coordena esforços para assegurar que os níveis de segurança estabelecidos são os níveis reais e necessários para a organização.

O outro objetivo da etapa Otimizado é estabelecer um processo de auditoria da GSI, visando garantir para investidores, alta direção e autoridades pertinentes, que os resultados apresentados pela GSI estão em conformidade com as expectativas da organização.

A Fase Otimizado é composta por dois processos, conforme apresentados abaixo:

- Processo de Revisão do Processo;
- Processo de Auditoria do Processo;

A organização dos processos e a maneira como eles interagem ente si estão representadas no diagrama de processos da figura abaixo:

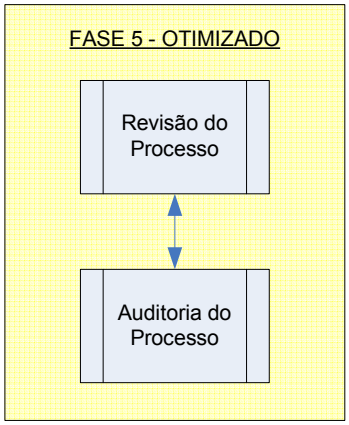

Figura 5.31 - Diagrama de Processos da Fase 5 do Modelo Faseado de GSI

5.2.5.1.Processo de Revisão do Processo

O processo de Revisão do Processo é responsável por reavaliar as informações de negócio, expectativas da organização e requisitos de segurança, permitindo rever o planejamento da GSI, e se necessário, redefinir os objetivos e escopo da GSI.

A reavaliação do planejamento da GSI é um meio de garantir que os esforços da GSI estarão sempre alinhados aos objetivos da organização, mantendo os níveis de segurança nos patamares necessários pela organização.

O Documento de Delegação de Autoridades, as informações do negócio, os requisitos de segurança, as expectativas da organização e o Plano de Gestão da Segurança da Informação compreendem os elementos de ***inputs*** do processo.

O principal elemento de ***output*** do processo é o Plano de Revisão do Processo, contendo as novas expectativas da organização, novos requisitos de segurança e novo plano de Gestão da Segurança da Informação.

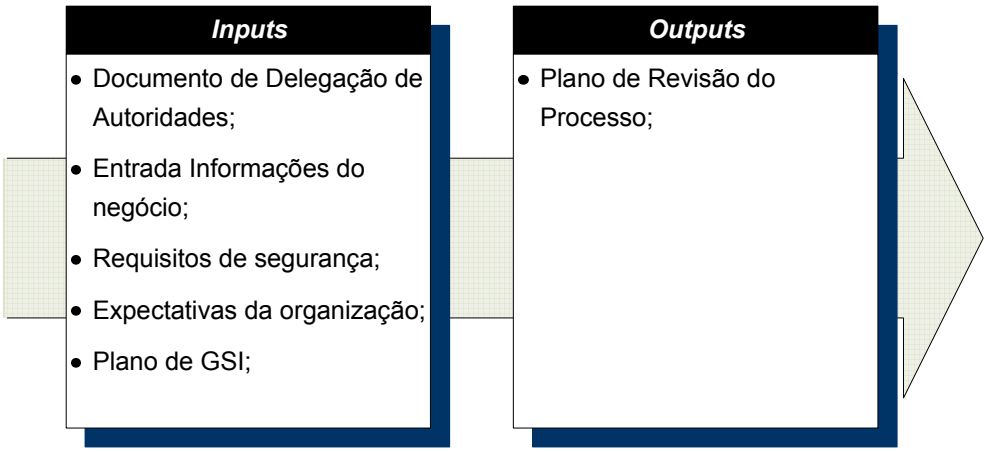

Figura 5.32 - Inputs e Outputs do processo de Revisão do Processo

5.2.5.2.Processo de Auditoria do Processo

O processo de Auditoria do Processo é responsável por estabelecer mecanismos de controle e avaliação dos resultados da Gestão da Segurança da Informação, permitindo verificar o cumprimento do Plano de Gestão da Segurança da Informação e o estabelecimento dos níveis de segurança, e comprovar a legalidade e a validade dos resultados da GSI.

O processo de Auditoria deve ser executado por autoridade autônoma ou distinta da autoridade da GSI, evitando interferências e induções nos resultados.

O Documento de Delegação de Autoridades, o Plano de Gestão da Segurança da Informação, a Definição dos Custos de Segurança e o Banco de Dados da Configuração compreendem os elementos de ***inputs*** do processo.

O Relatório de Auditoria do Processo é o elemento de ***output*** do processo, que deve conter recomendações e indicações do nível de conformidade da GSI. Além disso, podem conter sugestões de correções, que devem ser analisadas pelo processo de Gestão de Mudanças da Fase Gerenciado, a fim de adequar os controles e desempenho da GSI aos objetivos do negócio.

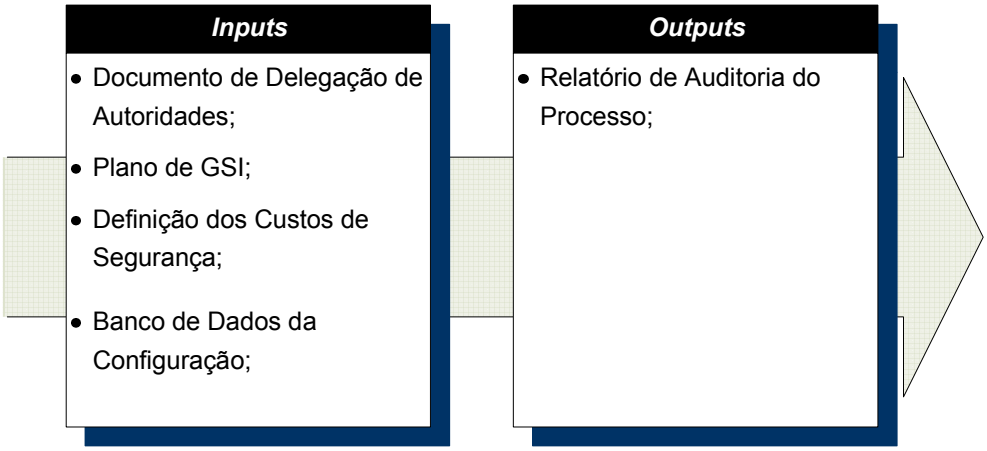

Figura 5.33 - Inputs e Outputs do processo de Auditoria do Processo

6. ANÁLISE COMPARATIVA

Neste Capítulo faremos uma análise comparativa da nossa proposta de Modelo Faseado de Gestão da Segurança da Informação com os principais modelos analisados no Capítulo 4, confrontando-os com base nos Elementos Gerais da GSI.

6.1. PRÁTICAS BASES E PADRÕES

O Modelo Faseado, por meio das Entradas Melhores Práticas e Padrões, enumera todas as possíveis práticas, controles e guias que endereçam as necessidades de segurança do negócio da organização. Além disso, nas Fases1 e 2 dos Recursos de Mensuração e Controle do Modelo Faseado, existem processos responsáveis por analisar, selecionar e mensurar, de acordo com o planejamento da GSI, as melhores práticas e padrões que regem a segurança do negócio. Durante essas etapas, são estimados ainda os custos de aplicação e os riscos para o negócio.

Portanto, se o escopo da GSI é proteger os documentos da organização, então, todos os elementos que descrevem as melhores práticas de salvaguarda e proteção de arquivos serão avaliados pelo Modelo Faseado, assim como serão analisadas as viabilidades de custos, as condições de riscos e as aceitações.

Não faz parte do escopo das Entradas Melhores Práticas e Padrões do Modelo Faseado pré-listar ou pré-definir as possíveis melhores práticas de segurança da informação, como ocorrem nos modelos ISM3, SSE-CMM, ITIL, CobiT e ISO/IEC 17799:2005. Há inúmeras listas de melhores práticas que abordam diversas áreas da Gestão da Segurança da Informação, assim como também existem práticas descritas por fabricantes de produtos, que detalham os meios mais seguros de configurar, armazenar, transmitir, publicar e acessar os dados através de seus produtos. Portanto, a criação de uma nova lista concorrente de melhores práticas de segurança é um esforço desnecessário.

Não obstante, cada organização requer um nível específico de segurança, e conforme apresentado por Peltier (2003), somente após uma análise do negócio da organização, da definição dos objetivos da GSI, do alinhamento desses objetivos com os objetivos de negócio

e de uma avaliação prévia dos riscos e dos custos, é possível determinar quais práticas e controles de segurança a organização deve adotar.

A adoção imediata de melhores práticas incorre nas deficiências apontadas no CobiT e no ISM3, os quais apresentam, respectivamente, uma base de guias e práticas que não endereçam todas necessidades dos níveis operacionais, e práticas pré-determinadas que podem não corresponder às necessidades do negócio da organização.

Destacamos ainda que, conforme apresentado por Martins (2003), a eficiência e a eficácia dos controles e práticas de segurança dependem do comportamento das pessoas que estão ao redor dessas práticas, portanto, o comportamento humano e a cultura organizacional devem ser levados em consideração no momento da seleção dos controles e das práticas de segurança.

A tabela abaixo apresenta um resumo comparativo entre os modelos analisados.

Tabela 6-1 - Comparativo entre modelos - Melhores Práticas e Padrões

MODELO	CARACTERÍSTICAS
ISO/IEC 17799	Lista de Melhores Práticas de Segurança, compostas de Trinta e nove categorias principais de segurança distribuídas entre onze cláusulas
CobiT	Lista de Melhores Práticas de Governança de TI, algumas práticas são destinadas à Segurança da Informação. Aproximadamente 1.600 Práticas de Controles (*Control Practices*).
ITIL	Estabelecimento de atividades e práticas para cada um dos 10 processos que visam alcançar os objetivos dos processos.
SSE-CMM	128 práticas bases (*base pratices*) utilizadas para endereçar as áreas de segurança de sistemas.
ISM3	44 práticas ou processos, distribuídos entre 4 processos bases, para endereçar questões de Gestão da Segurança da Informação
ISO/IEC 27001	Apresentação de práticas e objetivos para o estabelecimento de sistemas de gerenciamento da segurança da informação.
Modelo Faseado	Estabelecimento de processos para seleção, implantação e revisão de melhores práticas e guias de segurança conforme a necessidade do negócio.

6.2. CONTROLES DE SEGURANÇA

No Modelo Faseado, assim como ocorre com o domínio das Melhores Práticas e Padrões, os controles de segurança são selecionados de acordo com as necessidades de segurança da organização e com os objetivos da GSI. Diferentemente do que ocorre com os demais modelos analisados, os quais enumeram os controles que auxiliam em determinadas atividades.

Durante o processo de Definição das Atividades, ainda na Fase 2 dos Recursos de Mensuração e Controle do Modelo Faseado, é elaborado o Plano de Execução das Atividades. Neste Plano, são definidos os controles antecipados que devem ser adotados nos processos de implantação da segurança da informação.

Segundo Koontz e O'Donnell (1989), existem dois tipos de controles: Os que visam prever situações futuras e evitar desvios antes que eles aconteçam, além de nortear o rumo das atividades, e por isso são chamados de controles antecipados; e os que visam verificar se as atividades continuam nos rumos estabelecidos e detectam os desvios à medida que vão ocorrendo, e por isso são chamados de controles de correção. "Talvez não haja elemento mais importante num sistema apropriado e eficaz de controle que os controles antecipados" (KOONTZ; O DONNELL, 1989, p. 580), que devem ser estabelecidos nas etapas de planejamento.

Os controles de correção, são desenvolvidos durante o processo de Implantação de Controles, já na Fase 3 do Modelo Faseado. Os principais objetivos do processo de Implantação de Controles são o estabelecimento e a manutenção de técnicas de mensuração do andamento das atividades, visando garantir que os objetivos da GSI sejam alcançados, que os custos da GSI não sejam extrapolados e que os níveis de segurança sejam atingidos.

Além disso, o processo de Gestão da Segurança, alocado na Fase 4 do Modelo Faseado, é responsável por elaborar, estabelecer, implantar e acompanhar os controles, os indicadores e as métricas dos níveis de segurança da organização. Este processo é acionado no momento em que a organização atinge os níveis pretendidos de segurança, e por isso, sua principal função é manter a organização nestes níveis, mesmo que isso implique em desenvolver novos controles.

Portanto, os controles de segurança passam por processos de revisão dentro do Modelo Faseado, e com isso, nossa proposta de modelo endereça tanto o planejamento e a seleção dos controles, como a sua implantação, verificação e revisão.

A tabela abaixo apresenta um resumo comparativo entre os modelos analisados.

Tabela 6-2 - Comparativo entre modelos - Controles de Segurança

MODELO	CARACTERÍSTICAS
ISO/IEC 17799	Cada uma da trinta e nove categorias principais de segurança contém um objetivo de controle, que determina o que deve ser alcançado naquele item, e um ou mais controles que podem ser aplicados a fim de atingir os objetivos das categorias.
CobiT	Estabelecimento de objetivos, métricas e indicadores chaves de performance, para cada um dos 34 Controles Objetivos (*Control Objetives*).
ITIL	Estabelecimento de Controles de Processos, apresentando os fatores críticos de sucesso e indicadores de desempenho para cada um dos 10 processos.
SSE-CMM	28 práticas gerais (*generic pratices*) utilizadas para determinar o nível de maturidade dos processos.
ISM3	Cada prática possui indicadores e métricas que controlam: - Atividades: Indicam os resultados produzidos em determinado período; - Escopo: Indicam o percentual atingido pelo processo; - Atualizações: O tempo da ultima atualização do processo; - Disponibilidade: A disponibilidade do processo.
ISO/IEC 27001	Apresentação de controles que podem ser aplicados a fim de atingir os objetivos das cinco clausulas.
Modelo Faseado	Estabelecimento de processos para seleção, implantação e revisão de controles antecipados e corretivos.

6.3. PROCESSOS E GESTÃO

O Modelo Faseado de Gestão da Segurança da Informação é completamente voltado para processos, composto, ao todo, por vinte e seis processos que formam uma cadeia de interações e resultados por meio de *inputs* e *outputs*.

Dentre os modelos analisados, apenas os padrões ISO/IEC 17799:2005 e 27001:2005 não possuem processos, apesar de apresentarem práticas de gerenciamento da continuidade de

serviços e de revisão de procedimentos. No entanto, nenhuma dessas práticas está encadeada ou apresenta resultados por meio de *inputs* e *outputs.*

De acordo com Fayol (1990), *gestão* é o conjunto de ações ou processos responsáveis por planejar, organizar, liderar, coordenar e controlar atividades e pessoas a fim de atingir os objetivos pretendidos. Neste quesito, o Modelo Faseado está estruturado de tal forma que permite endereçar todo o conjunto de ações descrito por Fayol, senão vejamos:

- **PLANEJAR:**
    - As Fases 1 e 2 da Arquitetura de Mensuração e Controle são responsáveis pelas etapas inicias de visão e planejamento da GSI de acordo com os objetivos do negócio.
    - As Fases 4 e 5 são responsáveis por planejamentos de mudanças e de revisão.
    - Destacam-se os processos de Escopo Preliminar, Definição do Plano de Gestão da Segurança da Informação, Definição das Atividades e Revisão do Processo, pois resultam em planos.
- **ORGANIZAR:**
    - Os processos de avaliação e classificação da Fase 2 são responsáveis por organizar, arranjar e selecionar os recursos de acordo com o planejamento definido.
    - Por ser focado em resultados, a estruturada do Modelo Faseado permite que as atividades sejam organizadas conforme o interesse da organização.
- **LIDERAR:**
    - O primeiro processo do Modelo Faseado, denominado Atribuição das Responsabilidades, tem o objetivo de delegar as autoridades e definir os limites de atuação da GSI.
    - Todos os demais processos são executados em conformidade com os limites definidos.

- **COORDENAR:**
    - Todos os esforços da Gestão da Segurança da Informação são harmonizados e sincronizados pelo Modelo Faseado, de maneira que são traçados os objetivos, os meios e os fins de cada ação.
    - De modo geral, o Modelo Faseado é organizado de forma que as atividades de planejamento, execução, manutenção e melhoria estão seqüenciadas e com objetivos claros.
- **CONTROLAR:**
    - O Modelo Faseado é composto por Recursos de Mensuração e Controles, que permitem identificar os processos que estão sendo executados, os recursos envolvidos e os resultados alcançados, agregando visibilidade ao processo de gestão..

A tabela abaixo apresenta um resumo comparativo entre os modelos analisados.

Tabela 6-3 - Comparativo entre Modelos - Processos e Gestão

MODELO	CARACTERÍSTICAS
ISO/IEC 17799	-
CobiT	Elementos de *input* e *output* para cada um dos 34 Controles Objetivos
ITIL	Elementos de *input* e *output* para cada um dos 10 processos
SSE-CMM	Identificação de relacionamentos entre os processos e identificação dos resultados de cada processo.
ISM3	Elementos de *input* e *output* para cada um dos 44 processos
ISO/IEC 27001	-
Modelo Faseado	Elementos de *input* e *output* para cada um dos 26 processos. Além disso, alinhamento com as ações de planejamento, organização, controle, coordenação e liderança.

6.4. ARQUITETURA DE MENSURAÇÃO E AUDITORIA

A arquitetura de mensuração e auditoria do Modelo Faseado é diferente dos outros modelos analisados.

O CobiT utiliza um modelo de maturidade composto por cinco níveis, os quais descrevem o grau de alinhamento de determinado processo com os objetivos do negócio. Assim, cada processo é mensurado de maneira independente e o último nível indica que o processo está totalmente alinhado ao objetivo do negócio.

Os modelos ISM3 e SSE-CMM possuem um modelo de maturidade composto por cinco níveis, os quais indicam se determinadas atividades foram executadas. Assim, cada um desses modelos apresenta uma lista de práticas que devem ser concluídas em cada nível de maturidade. O último nível indica que todas as atividades foram concluídas.

O Modelo Faseado possui Recursos de Mensuração e Controle, os quais indicam o estágio de desenvolvimento da Gestão da Segurança da Informação dentro da organização. De maneira geral, em todas as fases (daí a origem do nome do nosso modelo), a GSI está alinhada aos objetivos do negócio.

A Fase 1, por exemplo, é a etapa de pré-planejamento ou visão. Somente ao término da Fase 1 que a organização passará à Fase 2, e assim por diante. A Fase 2, por sua vez, planeja e define os objetivos, metas, escopo e atividades da GSI.

Já na Fase 3, são executadas as atividades e implantados os controles e as métricas da GSI, e por isso, ao término desta etapa as práticas de segurança estão implantadas na organização. O objetivo da Fase 4 é manter os níveis de segurança da informação da organização conforme os objetivos definidos na Fase 2 e implantados na Fase 3.

A Fase 5 é responsável pela melhoria contínua do processo de gestão por meio de atividades de auditoria e revisão da GSI.

Conforme definido por NIST (2007), Chapin e Akridge (2005), e Baker e Wallace (2007), uma arquitetura de mensuração deve prover orientação, integração e visão dos processos da organização, além disso, ela deve fornecer de maneira clara a situação da Gestão da Segurança da Informação. Isto permite canalizar os esforços e os recursos da organização, além de criar um histórico de informações que podem ser utilizadas para demonstrar o

desempenho e as melhorias dos processos de gestão, principalmente durante etapas de auditoria.

A tabela seguinte apresenta um resumo comparativo entre os modelos analisados.

Tabela 6-4 - Comparativo entre modelos - Arquitetura de Mensuração e Auditoria

MODELO	CARACTERÍSTICAS
ISO/IEC 17799	-
CobiT	Modelo de maturidade composto por cinco níveis, os quais descrevem o grau de alinhamento de determinado processo com os objetivos do negócio. O último nível indica que o processo está alinhado ao objetivo do negócio, e cada processo é avaliado de modo independente.
ITIL	-
SSE-CMM	Modelo de maturidade composto por cinco níveis e 28 práticas genéricas (*generic pratices*). À medida que as práticas genéricas são cumpridas, o nível de maturidade do processo de desenvolvimento de software aumenta.
ISM3	Modelo de maturidade composto por cinco níveis e uma lista de atividades que devem ser cumpridas em cada nível. O último nível indica que todas as atividades foram concluídas e são mensuradas.
ISO/IEC 27001	-
Modelo Faseado	Arquitetura de Mensuração e Controle, composta por cinco níveis que definem o estágio de implantação da segurança da informação dentro da organização. Todos os níveis estão alinhados aos objetivos do negócio.

6.5. TECNOLOGIA

De maneira geral, nenhum dos modelos analisados apresenta um guia específico de tecnologia ou referências de tecnologias de segurança. No entanto, modelos como o CobiT, ISO/IEC 17799:2005, ISM3, ITIL e SSE-CMM sugerem a aplicação de ferramentas criptográficas ou indicam práticas que requerem o uso de tecnologia. Por exemplo, quase todos os modelos indicam a necessidade de ferramentas de proteção de softwares maliciosos (vírus) e analisadores de eventos.

Desta forma, se durante o processo de gestão da segurança da informação for identificada a necessidade de configurar um servidor de correio eletrônico de maneira segura, nenhum desses modelos indicará a melhor forma de fazê-lo.

Mesmo as ferramentas de análise de riscos, que suportam muitos desses modelos, têm como base guias específicos de fabricantes ou melhores práticas específicas a fim de identificar as vulnerabilidades de tecnologia e indicar correções.

Neste quesito, o Modelo Faseado é similar aos modelos analisados.

A Entrada Tecnologia do Modelo Faseado é responsável por identificar e listar as tecnologias disponíveis para a segurança do negócio da organização. Além disso, nas duas primeiras etapas dos Recursos de Mensuração e Controle, existem processos responsáveis por analisar, selecionar e mensurar, de acordo com o planejamento da GSI, as questões tecnológicas.

A tabela abaixo apresenta um resumo comparativo entre os modelos analisados.

Tabela 6-5 - Comparativo entre modelos - Tecnologia

MODELO	CARACTERÍSTICAS
ISO/IEC 17799	Práticas para seleção e revisão de tecnologias.
CobiT	Práticas para seleção e revisão de tecnologias.
ITIL	Práticas para seleção e revisão de tecnologias para entrega e suporte a serviços.
SSE-CMM	Práticas para seleção e revisão de tecnologias para o desenvolvimento de sistemas seguros.
ISM3	Práticas para seleção e revisão de tecnologias.
ISO/IEC 27001	-
Modelo Faseado	Processos para seleção e revisão de tecnologias que endereçam as necessidades de segurança do negócio.

6.6. ASPECTOS CULTURAIS, SOCIAIS, LEGAIS E ÉTICOS

As Entradas Aspectos Culturais e Sociais do Modelo Faseado são responsáveis por identificar a cultura de segurança dentro da organização. De maneira similar, as Entradas Aspectos Legais e Éticos têm o objetivo de enumerar os elementos legais e éticos que contribuem para o sucesso da Gestão da Segurança da Informação e, por conseqüência, auxiliam nos objetivos do negócio.

É por meio dos Recursos de Mensuração e Controle que os Aspectos Culturais, Sociais, Legais e Éticos da organização são identificados, avaliados, definidos, implantados e mantidos, garantindo que estejam sempre em conformidade com as necessidades de segurança da organização.

Todos os modelos analisados compreendem aspectos legais e éticos, e buscam realizar conformidade com leis, contratos, acordos, regulamentações e outros. No entanto, modelos como o ITIL e o SSE-CMM buscam elementos legais que endereçam questões específicas da sua área de atuação, como os contratos de serviço e o desenvolvimento de sistemas.

Dentre os modelos analisados, nenhum apresenta processos ou práticas que envolvam completamente os aspectos culturais de segurança. No entanto, todos os eles endereçam questões relacionadas a treinamento e educação. Mas, conforme já fora apresentado por Von Solms e Von Solms (2004), programas de treinamento e educação desempenham um papel importante na disseminação dos conceitos de segurança da informação. No entanto, segundo Martins (2003) para que a segurança incorpore a cultura da organização é preciso que seja dada devida importância e incentivo ao comportamento de segurança da informação dentro das organizações. Além disso, devem existir políticas para nortear o comportamento humano e descrever as expectativas de segurança da organização, fortalecendo as relações de confiança entre as pessoas da organização.

O Modelo Faseado, por meio do Processo de Gestão da Cultura Organizacional, elabora, estabelece, implanta e acompanha os controles do comportamento humano dentro da organização, garantindo que os objetivos, responsabilidades, normas e procedimentos sejam conhecidos por todos os membros da organização, e sejam elementos de valores coletivos dentro da organização.

A tabela a seguir apresenta um resumo comparativo entre os modelos analisados.

Tabela 6-6 - Comparativo entre modelos - Aspectos Legais, Éticos, Culturais e Sociais

MODELO	CARACTERÍSTICAS
ISO/IEC 17799	Práticas de treinamento, elaboração de políticas de segurança, responsabilidades claras e comprometimento dos executivos da organização. Práticas de conformidade com leis, regulamentações e códigos de ética.
CobiT	Endereça questões de treinamento, conhecimento e comprometimento dos executivos da organização. Apresenta processos para realizar conformidade com leis, regulamentações e códigos de ética.
ITIL	Conformidade com os Acordos de Níveis de Serviço.
SSE-CMM	Praticas Bases para identificação de questões legais que afetam os negócios.
ISM3	Processos para identificação de questões legais que afetam os negócios. Processos para definição de responsabilidades e treinamentos.
ISO/IEC 27001	Práticas para identificação de questões legais que envolvem o desenvolvimento de sistemas de gerenciamento da segurança da informação.
Modelo Faseado	Processos para identificação de questões legais, éticas e culturais que afetam os negócios. Processo para Gestão da Cultura Organizacional.

6.7. ASPECTOS DE NEGÓCIO

O Modelo Faseado é totalmente voltado para as necessidades de segurança do negócio, e por isso, estabelece processos e mecanismos para assegurar que os objetivos da GSI estão em conformidade com os objetivos da organização desde o início das atividades de segurança.

Segundo Abell (1991), a definição do negócio da organização é o ponto de partida para o seu planejamento estratégico, e o principal responsável pela participação de uma organização no mercado e pelo seu sucesso. Por tal motivo, além do Modelo Faseado apresentar uma Entrada Informações do Negócio, cujo objetivo é coletar elementos para o mapeamento das necessidades do negócio, existe ainda um processo chave, denominado Análise do Negócio, cujo objetivo é estabelecer os requisitos de segurança para o sucesso do negócio.

Desta forma, todo o planejamento e os investimentos em implantação e manutenção das práticas e controles de segurança são precedidos de uma análise das necessidades do negócio.

Podemos afirmar que o compromisso do Modelo Faseado é o estabelecimento dos níveis de segurança necessários para o sucesso da organização. Por isso, o Modelo não se preocupa somente em atingir níveis máximos absolutos de segurança ou implantar o estado da arte em tecnologia, mas assegurar que os investimentos para proteger a informação sejam compatíveis com o seu valor e com as expectativas da organização.

Esta visão é um pouco diferenciada de outros modelos que também endereçam as necessidades do negócio, como o ITIL e o SSE-CMM. Estes dois modelos visam atender as necessidades do negócio, desde que elas sejam a entrega de serviços de TI e o desenvolvimento de sistemas seguros, respectivamente, do contrário, inexistem processos para endereçar outras questões de segurança. Afinal, estes são os objetivos específicos dos modelos, e por isso, concentram seus esforços nas práticas que endereçam essas questões.

O CobiT, por exemplo, visa atender à todas as necessidades de segurança da organização, no entanto, apenas no nível cinco é que os processos e atividades de segurança estão alinhadas aos objetivos do negócio.

A tabela abaixo apresenta um resumo comparativo entre os modelos analisados.

Tabela 6-7 - Comparativo entre modelos - Negócio

MODELO	CARACTERÍSTICAS
ISO/IEC 17799	-
CobiT	Voltado para o negócio.
ITIL	Voltado para a entrega e o suporte de serviços de TI.
SSE-CMM	Voltado para o desenvolvimento de sistemas seguros.
ISM3	Voltado para o negócio.
ISO/IEC 27001	Voltado para o estabelecimento de sistemas de gerenciamento da segurança da informação.
Modelo Faseado	Voltado para o negócio.

7. CONCLUSÕES E TRABALHOS FUTUROS

As práticas de segurança da informação não são recentes, no entanto, diversos fatores contribuíram para a necessidade de métodos capazes de planejar, coordenar, integrar e controlar tais práticas, visando alinhá-las aos objetivos do negócio da organização.

Observamos que as práticas de Segurança da Informação tendem a evoluir de atividades pontuais e descoordenadas para uma posição sistemática e estratégica dentro das organizações, exigindo o uso e desenvolvimento de metodologias capazes de lidar com diferentes questões, que não somente aquelas relacionadas à tecnologia.

Diante destes desafios surgem os modelos de Gestão da Segurança da Informação (GSI), que visam sistematizar e organizar a aplicação das práticas de Segurança da Informação para que os negócios das organizações estejam seguros e seus objetivos sejam alcançados com sucesso. Os Modelos de Gestão da Segurança da Informação foram os objetos de estudo deste trabalho.

Esta obra fez uma análise das definições de Gestão da Segurança da Informação, e encontrou uma relação de alinhamento entre as práticas de segurança e as necessidades de proteção da organização, com foco nos objetivos do negócio. No entanto, as definições estudadas não demarcaram o que seriam as práticas de gestão de segurança, assim como não definiram o que seriam informações e qual a relação entre estas e o negócio da organização.

Por isso, fizemos uma breve análise dos termos *Informação*, *Segurança* e *Gestão*, delimitamos o conceito de cada um, de acordo com os objetivos deste trabalho, e entendemos que *Gestão da Segurança da Informação* é um conjunto de práticas e métodos de **gestão** que visam prover e manter os **ativos** da organização em níveis aceitáveis e necessários de **segurança** para que os objetivos do negócio sejam atingidos conforme planejado.

Como uma primeira contribuição, este trabalho realizou uma pesquisa nas literatura e analisou os modelos atuais e mais utilizados de gestão da segurança da informação. Para a realização dessas análises, criamos uma base de comparação, resultante do estudo das diversas orientações de gestão e da definição dos Elementos Gerais de gestão da segurança da informação, o qual é composto por aspectos relacionados à:

- Processos e Gestão;
- Controles de Segurança;

- Arquitetura de Mensuração e Auditoria;
- Tecnologia;
- Práticas Bases e Padrões;
- Aspectos Culturais, Sociais, Legais e Éticos;
- Negócio.

Como resultado dessas análises, apontamos as características e desvantagens de cada modelo, e reafirmamos o entendimento que isoladamente estes modelos não endereçam, de maneira completa, todas as questões de Segurança da Informação exigidas pelas organizações.

A segunda e principal contribuição desta obra foi a proposta de um modelo faseado de gestão da segurança da informação, denominado Modelo Faseado. O Modelo conseguiu abordar, de maneira mais completa que os modelos atuais, os Elementos Gerais da GSI.

Dentre as vantagens do Modelo Faseado está sua metodologia orientada a processos, que permite a estruturação das atividades de segurança e garante rastreabilidade e visibilidade para a GSI. O Modelo apresenta etapas e resultados bem definidos, por meio de documentos e planos, o que possibilita uma auditoria ou avaliação precisa das ações da gestão da segurança da informação.

Além disso, o Modelo se desenvolve por meio de estágios ou fases, possibilitando uma aplicação gradual e planejada das práticas de segurança de acordo com as necessidades da organização.

O diferencial do Modelo Faseado para os outros modelos analisados, é que seus processos visam de manter as ações de segurança alinhadas com os objetivos do negócio em qualquer dos níveis ou fases do Modelo. Desta forma, é possível que as organizações controlem e direcionem seus investimentos nas atividades de segurança da informação de maneira eficiente e objetiva. Assim, empresas com restrições orçamentárias ganham confiança para realizar investimentos em segurança da informação.

Portanto, concluímos que o Modelo Faseado de Gestão da Segurança da Informação é uma opção exeqüível para organizações que não dispõem de recursos para integrar diversos modelos e manter uma estrutura complexa de gestão.

A figura 7.1 seguinte, ilustra os processos que são executados em cada fase do modelo.

Tabela 7-1 - Mapeamento dos Processos do Modelo por Fases

		FASES				
Subitem	**Processos**	**1**	**2**	**3**	**4**	**5**
5.2.1.1	Atribuição das Responsabilidades	x				
5.2.1.2	Análise do Negócio	x				
5.2.1.3	Escopo Preliminar	x				
5.2.1.4	Identificação dos Ativos	x				
5.2.1.5	Identificação das Entradas	x				
5.2.2.1	Definição do Plano de Gestão da Segurança da Informação		x			
5.2.2.2	Definição da Política de Segurança		x			
5.2.2.3	Avaliação dos Custos		x			
5.2.2.4	Avaliação dos Riscos		x			
5.2.2.5	Avaliação das Entradas		x			
5.2.2.6	Classificação dos Ativos		x			
5.2.2.7	Definição das Atividades		x			
5.2.3.1	Implantação de Controles			x		
5.2.3.2	Execução das Atividades			x		
5.2.3.3	Verificação			x		
5.2.3.4	Validação			x		
5.2.4.1	Processo de Gestão da Segurança				x	
5.2.4.2	Processo de Gestão de Riscos				x	
5.2.4.3	Processo de Gestão de Incidentes				x	
5.2.4.4	Processo de Gestão de Problemas				x	
5.2.4.5	Processo de Gestão de Mudanças				x	
5.2.4.6	Processo de Gestão da Cultura Organizacional				x	
5.2.4.7	Processo de Gestão de Custos				x	
5.2.4.8	Processo de Gestão da Configuração				x	
5.2.5.1	Processo de Revisão do Processo					x
5.2.5.2	Processo de Auditoria do Processo					x
		Iniciado	**Planejado**	**Implantado**	**Gerenciado**	**Revisado**

7.1. CONSIDERAÇÕES FINAIS

Dentre uma das certificações profissionais mais valorizadas e procuradas na área de Gestão da Segurança da Informação, está o CISM (*Certified Information Security Manager*). O CISM é um programa de certificação, desenvolvido pelo ISACA, para acreditar profissionais com experiência e conhecimento em práticas de Gestão da Segurança da Informação.

O CISM estabelece uma série de atividades e responsabilidades que são consideradas essenciais aos gestores de segurança da informação, e por isso, formam o conteúdo programático do exame. Essas atividades estão distribuídas em cinco Domínio de Conhecimento, conforme apresentado pelo ISACA (2008).

Realizamos um mapeamento dessas atividades e responsabilidades exigidas pelo CISM com os processos estabelecidos no Modelo Faseado. Este mapeamento está representado na tabela à seguir.

Como podemos observar, os processos do Modelo Faseado cobrem, completamente, as atividades e responsabilidades definidas pelo CISM. Desta forma, o Modelo Faseado permite aos gestores de segurança da informação aplicar, de forma estruturada, suas habilidades e conhecimentos.

Tabela 7-2 - Mapeamento entre os Domínios de Conhecimento definidos pelo CISM e os Processos do Modelo Faseado

Domain 1 - Information Security Governance		
Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.		
Task/Responsibility Statements:		**Processo**
1.1	Develop an information security strategy aligned with business goals and objectives.	4.2.1.3 4.2.2.1
1.2	Align information security strategy with corporate governance.	4.2.1.2
1.3	Develop business cases justifying investment in information security.	4.2.2.1 4.2.2.3
1.4	Identify current and potential legal and regulatory requirements affecting information security.	4.2.1.5
1.5	Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.	4.2.1.5
1.6	Obtain senior management commitment to information security.	4.2.1.1
1.7	Define roles and responsibilities for information security throughout the organization.	4.2.1.1
1.8	Establish internal and external reporting and communication channels that support information security.	4.2.1.1 4.2.4

Domain 2 - Information Risk Management		
Identify and manage information security risks to achieve business objectives.		
Task/Responsibility Statements:		**Processo**

2.1	Establish a process for information asset classification and ownership.	4.2.1.4 4.2.2.6 4.2.4.8
2.2	Implement a systematic and structured information risk assessment process.	4.2.2.4 4.2.4.2
2.3	Ensure that business impact assessments are conducted periodically.	4.2.4.2
2.4	Ensure that threat and vulnerability evaluations are performed on an ongoing basis.	4.2.4.1
2.5	Identify and periodically evaluate information security controls and countermeasures to mitigate risk to acceptable levels.	4.2.4.1
2.6	Integrate risk, threat and vulnerability identification and management into life cycle processes (e.g., development, procurement and employment life cycles).	4.2.4
2.7	Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.	4.2.4

Domain 3 -Information Security Program Development		
Create and maintain a program to implement the information security strategy.		
Task/Responsibility Statements:		**Processo**
3.1	Develop and maintain plans to implement the information security strategy.	4.2.1.3 4.2.2.1
3.2	Specify the activities to be performed within the information security program.	4.2.2.7 4.2.4
3.3	Ensure alignment between the information security program and other assurance functions (e.g., physical, HR, quality, IT).	4.2.2.5
3.4	Identify internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program).	4.2.1.5 4.2.2.5
3.5	Ensure the development of information security architectures (e.g., people, processes, technology).	4.1 4.2
3.6	Establish, communicate and maintain information security policies that support the security strategy.	4.2.2.2
3.7	Design and develop a program for information security awareness, training and education.	4.2.2.7 4.2.4.6
3.8	Ensure the development, communication and maintenance of standards, procedures and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.	4.2.2 4.2.3 4.2.4
3.9	Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).	4.2.4 4.2.5

3.10	Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).	4.2.2 4.2.4
3.11	Establish metrics to evaluate the effectiveness of the information security program.	4.2.2.7 4.2.3.1 4.2.4.1

Domain 4 - Information Security Program Management		
Oversee and direct information security activities to execute the information security program.		
	Task/Responsibility Statements:	**Processo**
4.1	Manage internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.	4.2.3.1 4.2.3.2 4.3.3.3
4.2	Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.	4.2.3.1 4.2.3.3
4.3	Ensure that the information security controls agreed to in contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties) are performed.	4.2.4.1
4.4	Ensure that information security is an integral part of the systems development process.	4.2.4.1
4.5	Ensure that information security is maintained throughout the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).	4.2.4
4.6	Provide information security advice and guidance (e.g., risk analysis, control selection) to the organization.	4.2.2.2
4.7	Provide information security awareness, training and education to stakeholders (e.g., business process owners, users, information technology).	4.2.4.6
4.8	Monitor, measure, test and report on the effectiveness and efficiency of information security controls and compliance with information security policies.	4.2.4.1 4.2.5.2
4.9	Ensure that noncompliance issues and other variances are resolved in a timely manner.	4.2.4.3 4.2.4.4 4.2.4.5

Domain 5 - Incident Management & Response		
Plan, develop and manage a capability to detect, respond to and recover from information security incidents.		
	Task/Responsibility Statements:	**Processo**

5.1	Develop and implement processes for detecting, identifying, analyzing and responding to information security incidents.	4.2.4.1 4.2.4.3 4.2.4.4 4.2.4.5
5.2	Establish escalation and communication processes and lines of authority.	4.2.4.1 4.2.4.3
5.3	Develop plans to respond to and document information security incidents.	4.2.4.3
5.4	Establish the capability to investigate information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing).	4.2.4.3
5.5	Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers).	4.2.4.1
5.6	Integrate information security incident response plans with the organization's Disaster Recovery (DR) and Business Continuity Plan (BCP).	4.2.4.1 4.2.4.3 4.2.4.8
5.7	Organize, train and equip teams to respond to information security incidents.	4.2.4.6
5.8	Periodically test and refine information security incident response plans.	4.2.4.1
5.9	Manage the response to information security incidents.	4.2.4.5
5.10	Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk.	4.2.4.4

7.2. TRABALHOS FUTUROS

Apesar dos esforços empenhados neste trabalho para desenvolver um modelo de Gestão da Segurança da Informação capaz de endereçar os Elementos Gerais da GSI, é essencial que sejam realizados trabalhos de aplicação prática do modelo.

Estes trabalhos de aplicação prática devem verificar a eficácia dos processos estabelecidos no Modelo Faseado, assim como validar os resultados esperados através do Modelo e compará-los com resultados conhecidos. Esta comparação, conhecida como *benchmark*, permitirá o aprimoramento, evolução e amadurecimento do Modelo Faseado.

A estrutura modular e orientada a processos do Modelo Faseado possibilita ainda o desenvolvimento de sistemas computacionais (*softwares*) capazes de otimizar a implantação, manutenção, monitoramento e auditoria dos processos do Modelo.

REFERÊNCIAS BIBLIOGRÁFICAS

ABELL, Derek F., **Definição do negócio: Ponto de partida do planejamento estratégico**, trad. Carlos Roberto Vieira de Araújo, São Paulo, Ed. Atlas, 1991.

ACKOFF, R. L., **From Data to Wisdom**, Journal of Applied Systems Analysis, Volume 16, 1989 p 3-9.

ALABOODI, S. S., **Towards evaluating security implementations using the Information Security Maturity Model (ISMM)**, Msc. thesis, Department of Eletrical and Computer Engineering, University of Waterloo, Ontario, Canada, 2007.

ALGER, John I., **On Assurance, Measures, and Metrics: Definitions and Approaches**, Applied Computer Security Associates Workshop on Information-Security-System Rating and Ranking, Williamsburg, Virginia, 21-23, Março 2001: 1-2. Disponível em http://www.acsac.org/measurement , acesso em 20 dez 2007.

ANDRESS, M., **Manage people to protect data**. InfoWorld, 2000, 22(46), November.

BAKER, W. and WALLACE, L. **Is Information Security Under Control?** IEEE Security and Privacy, Volume 5, Issue 1, ISSN 1540-7993, pp. 36-44, Jan-Feb 2007.

BASEL II: **International Convergence of Capital Measurement and Capital Standards: a Revised Framework**, June 2004, disponível em http://www.bis.org/publ/bcbs128.pdf, acesso em 20 jan 2008.

BELLARE, M., ROGAWAY, P., **Introduction to Modern Cryptography**, May 2005,

BEMBERGER, J., **Essence of the Capability Maturity Model**. IEEE Computer, Vol 30, Issue 6, Jun 1997, p. 112-114.

BRASIL, Comitê Gestor da Internet no Brasil, **Práticas de Segurança para Administradores de Redes Internet**, versão 1.2, 16 de maio de 2003, disponível em http://www.cert.br/docs/seg-adm-redes, acesso em 05 nov 2007

BRASIL, **Decreto nº 3.505** de 13 de junho de 2000, Diário Oficial da União de 14/6/2000, disponível em http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm, acesso em 05 nov 2007.

BRASIL, **Decreto nº 4.553** de 27 de dezembro de 2002, Diário Oficial da União de 30/12/2002, disponível em http://www.planalto.gov.br/ccivil_03/decreto/2002/D4553.htm, acesso em 05 nov 2007.

BRASIL, **Lei nº 10.973** de 2 de dezembro de 2004, Diário Oficial da União de 03/12/2004, disponível em http://www.planalto.gov.br/Ccivil_03/_Ato2004-2006/2004/Lei/L10.973.htm, acesso em 03 mar 2008.

BRASIL, **Lei nº 9.279** de 14 de maio de 1996, Diário Oficial da União de 15/5/1996, disponível em http://www.planalto.gov.br/ccivil/LEIS/L9279.htm, acesso em 03 mar 2008.

BRASIL, Tribunal de Contas da União, **Boas práticas em segurança da informação,** Tribunal de Contas da União – 2. ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007, disponível em http://www.tcu.gov.br, acesso em 16 mai 2008.

BRENNER, B., **Numbers: ISACA Says Survey Illustrates Benefits of CISM Cert**, disponível em: http://www.csoonline.com/article/379914/Numbers_ISACA_Says_ Survey_Illustrates_Benefits_of_CISM_Cert , acesso em 07 jun 2008.

BUSINESS SOFTWARE ALLIANCE. **Information Security Governance: Toward a Framework for Action**. Outubro 2003. Disponível em http://www.bsa.org/usa, acesso em 20 nov 2007.

CANAL, Vicente Aceituno (2007), ISM3 Consortium, **Information Security Management Maturity Model, Version 2.00**. Creative Commons. Disponível em http://www.ism3.com, acesso em 07 nov 2007.

CERT, 2007 **E-Crime Watch Survey**, Carnegie Mellon University's Software Engineering Institute, disponível http://www.cert.org, acesso em 05 jan 2008.

CERTINEWS, disponível em http://www.certisign.com.br/certinews/banco_noticias, acesso em 20 fev 2008.

CHESWICK, William R., BELLOVIN, Steven M., **Firewalls and Internet Security: Repelling the Wily Hacker**, Addison-Wesley Publishing Company, Reading, MA, 1994.

COMMON CRITERIA, disponível em http://www.commoncriteriaportal.org, acesso em 20 nov 2007.

COMPUTER SECURITY INSTITUTE, **CSI Survey 2007**, disponível em http://gocsi.com, acesso em 24 nov 2007.

CROSBY, P. B. **Quality is Free**. New York, New York: McGraw-Hill, 1979.

D. A. CHAPIN, and S. AKRIDGE, 2005, **How Can Security Be Measured?**, Information Systems Control Journal, Volume 2, 2005.

DE OLIVEIRA ALVES, G.A.; DA COSTA CARMO, L.F.R.; DE ALMEIDA, A.C.R.D., **Enterprise Security Governance; A practical guide to implement and control Information Security Governance (ISG),** The First IEEE/IFIP International Workshop on Business-Driven IT Management. 2006. BDIM apos;06, Vol , Issue , 07-07 April 2006 pp. 71 – 80.

DEBRACENY, R.S. (2006). **Re-engineering IT Internal Controls - Applying capability Maturity Models to the Evaluation of IT Controls**. Proceedings of the 39th Hawaii International Conference on System Sciences.

DEMING, W. Edward., **Out of the Crisis**. Cambridge, MA, MIT Center for Advanced Engineering, 1986.

DHILLON, G., BACKHOUSE, J., **Information Systems Security Management in the New Millennium**, Comm. ACM, vol. 43, no. 7, 2000, pp. 125-128.

DONN B. Parker, **Fighting Computer Crime: A New Framework for Protecting Information** (New York: John Wiley & Sons, Inc., 1998), p. 240.

ELOFF, J., ELOFF, M., **Information Security Management - A New Paradigm**, Proceedings of ACM International Conference Proceeding Series; Vol. 47 , Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology, SAICSIT, 2003, Pages: 130 – 136.

ENDORF, C. **Outsourcing Security: The Need, the Risks, the Providers, and the Process**. Information Security Management, (2004) 17-23.

ENTERPRISE STRATEGY GROUP (ESG), ISO, ITIL and COBIT triple play fosters optimal security management execution, April 02, 2008, disponível em http://www.scmagazineus.com/ISO-ITIL-and-COBIT-triple-play-fosters-optimal-security-management-execution/article/108620/, acesso em 22 mai 2008.

ESTADOS UNIDOS DA AMÉRICA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - NIST, **An Introduction to Computer Security: The NIST Handbook**, Special Publication 800-12, NIST (1998). Disponível em http://csrc.nist.gov/publications/nistpubs/800-12, acesso em 05 nov 2007.

ESTADOS UNIDOS DA AMÉRICA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST, **FIPS 180-2, Secure hash standard**, August 2000, disponível em http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf, acesso em 20 jan 2008.

ESTADOS UNIDOS DA AMÉRICA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - NIST, **Information Security Guide For Government Executives - NISTIR 7359**, disponível em http://csrc.nist.gov/publications/nistir/ir7359/NISTIR-7359.pdf, acesso em 19 nov 2007.

ESTADOS UNIDOS DA AMÉRICA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - NIST, **Information Security Handbook: A Guide for Managers, Special Publication 800-100**, NIST (2006). Disponível em http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf, acesso em 19 nov 2007.

ESTADOS UNIDOS DA AMÉRICA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - NIST, **Performance Measurement Guide for Information Security (DRAFT), Special Publication 800-55 - Revision 1 (DRAFT),** NIST (2007). Disponível em http://csrc.nist.gov/publications/drafts/800-55-rev1/Draft-SP800-55r1.pdf, acesso em 19 nov 2007.

ESTADOS UNIDOS DA AMÉRICA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST, **Recommended Security Controls for Federal**

Information Systems, Special Publication 800-53, NIST (2005). Disponível em http://csrc.nist.gov/publications/nistpubs/800-53/sp800-53.pdf, acesso em 05 nov 2007.

ESTADOS UNIDOS DA AMÉRICA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST, **Risk Management Guide for Information Technology Systems**, Special Publication 800-30, NIST (2006). Disponível em http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, acesso em 19 nov 2007.

ESTADOS UNIDOS DA AMÉRICA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST, **Security Metrics Guide for Information Technology Systems, Special Publication 800-55**, NIST, 2003, disponivel em http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf, acesso em 20 dez 2007.

ESTADOS UNIDOS DA AMÉRICA, **Public Law 100-235 (H.R. 145)**, Computer Security Act of 1987, January 8, 1988, disponível em http://www.epic.org/crypto/csa/csa.html, acesso em 05 nov 2007.

ESTADOS UNIDOS DA AMÉRICA, **Public Law No. 107-204**, 116 Stat. 745, Sarbanes-Oxley Act 2002, July 30, 2002, disponível em http://www.sarbanes-oxley.com/, acesso em 05 nov 2007.

EUROPEAN CERTIFICATION BOARD-SECURITY SYSTEMS, disponível em http://ecb-s.com/english/home_ecbs_e.htm, acesso em 25 fev 2008.

FAYOL, H., **Administração industrial e geral: previsão, organização, comando, coordenação e controle**, 1990, 10ª edição, São Paulo, Ed. Atlas.

FERRAIOLO, Karen; SACHS, Joel, **Determining Assurance Levels by Security Engineering Process Maturity**, Proceedings of the Fifth Annual Canadian Computer Security Symposium, May 1993.

GAUNT, N., **Practical approaches to creating a security culture**, International Journal of Medical Information,2000, 60(2), November:151-157.

GLAZER, R. (2003). **Measuring the value of information**: The information-intensive organization, IBM SYSTEMS JOURNAL, Vol 32, No 1, 1993, (12) 99–110.

GONÇALVES, Luís Rodrigo de Oliveira (2003). **Pequeno histórico sobre o surgimento das Normas de Segurança**, Laboratório RAVEL/COPPE/UFRJ, disponível em http://www.lockabit.coppe.ufrj.br, acesso em 05 nov 2007.

GULDENTOPS, E. (2004). **Governing Information Technology through COBIT**. In: Van Grembergen, W. (ed.): Strategies for Information Technology Governance. Idea Group Publishing.

HARRIS, M. W., **Process visibility: the key to optimizing business operations**, KMWorld, 2002, disponível em http://www.kmworld.com, acesso em 25 nov 2007.

HARRIS, Shon. (2004), Editora McGraw Hill, **CISSP All-inOne Exam Guide**, 3º Edição.

HOLTON, Glyn A. (2004). **Defining Risk**, Financial Analysts Journal, 60 (6), 19–25.

HOWARD, J. D., **An Analysis of Security Incidents on the Internet 1989–1995**, Ph.D. thesis, Department of Engineering and Public Policy, Carnegie Mellon University, April 7, 1997.

HUMPHREY, Watts S. **Managing the Software Process**. Reading, MA: Addison-Wesley, 1989.

ICSA LABS – INTERNATIONAL COMPUTER SECURITY ASSOCIATION, disponível em http://www.icsalabs.com, acesso em 19 nov 2007.

INGLATERRA, BRITISH STANDARDS INSTITUTE - BSI, disponível em http://www.bsi-global.com/, acesso em 20 nov 2007;

INSTITUTE OF INTERNAL AUDITORS, **Information Security Governance: What Directors Need to Know**, 2001, pp. 43-48, National Cyber Security Summit Task, disponível em http://www.cyberpartnership.org/InfoSecGov4_04.pdf, acesso em 19 nov 2007.

INTERNATIONAL ACCOUNTING STANDARDS BOARD. disponível em http://www.iasb.org, acesso em 05 nov 2007.

ISACA, **CISM Exam Job Practice Areas**, disponível em http://www.isaca.org/Template.cfm?Section=CISM_Exam_Info&Template=/ContentManagement/ContentDisplay.cfm&ContentID=42648&SuppressBreadCrumb=True , acesso em 05 jun 2008

ISO (2001), International Organization for Standardization, **ISO/IEC 15288**, Information technology – Systems Life Cycle Processes.

ISO (2002), International Organization for Standardization, **ISO/IEC 21827**, Information technology- Systems Security Engineering - Capability Maturity Model (SSE-CMM®).

ISO (2004), International Organization for Standardization, **ISO/IEC 13335**, Information technology - Security techniques - Management of information and communications technology security.

ISO (2005), International Organization for Standardization**, ISO/IEC 17799**, Information technology - Security techniques - Code of practice for information security management.

ISO (2005b), International Organization for Standardization**, ISO/IEC 27001**, Information Technology – Security techniques – Information Security Management Systems - Requirements.

ISSEA (2007), International Systems Security Engineering Association, disponível em http://www.issea.org, acesso em 05 nov 2007.

IT GOVERNANCE INSTITUTE, (2003), **Board Briefing on IT Governance**, 2nd edition, ISBN 1-893209-64-4, USA.

IT GOVERNANCE INSTITUTE, (2005) **Control Objectives for Information and related Technology (COBIT), Version. 4**, USA, disponível em http://www.itgi.org, acesso em 22 nov 2007.

IT GOVERNANCE INSTITUTE, (2006a) **COBIT Mapping: Overview on International IT Guidance**, Second Edition, USA, disponível em http://www.itgi.org, acesso em 28 fev 2008.

IT GOVERNANCE INSTITUTE, (2006b) **Information Security Governance: Guidance for Boards of Directors and Executive Management**, 2nd edition, ISBN 1-893209-28-8, USA.

IT GOVERNANCE INSTITUTE, (2007) **IT Assurance Guide: Using CobiT**, ISBN 1-933284-74-9, USA.

J.M. CAPONE, J. FRITSCH, R. SMITH, S. BHATTACHARYA, S. PALANGALA, **Concepts for a Network Maturity Model**, asset, p. 102, 1998 IEEE Workshop on Application - Specific Software Engineering and Technology, 1998.

JURAN, J. M., **on Planning for Quality**. New York, New York: MacMillan, 1988.

KAJAVA, J., ANTTILA, J., et al. **Information Security Standards and Global Business**, IEEE International Conference, Volume , Issue , 15-17 Dec. 2006, pp. 2091 – 2095, ISBN: 1-4244-0726-5

KAJAVA, J., SAVOLA, R., **Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes**, 2005. Disponível em http://ww.manchester.ac.uk/eunis2005/medialibrary/papers/paper_154.pdf, acesso em 05 nov 2007.

KAPP, J., How to Conduct a Security Audit, PC-Network Advisor, Issue 120, July 2000, pg 3-8.

KOONTZ, H., O'DONNELL, C., (1989), **Fundamentos de administração**, 2º ed., Trad: Carlos Afonso Malferrari, São Paulo: Pioneira, 1989. 580p. Título Original: Essentials of Management.

KOONTZ, H., O'DONNELL, C., (1974), **Princípios de Administração — Uma Análise das Funções Administrativas**. 8º ed., São Paulo: Editora Pioneira, 1974.

MARTINS, A., **Information security culture**, Thesis MCom, Department of Business Management, etd-04292004-110222, University of Johannesburg, jan 2003.

MASACCI, F., PREST, M., ZANNONE, N. **Using a security requirements engineering methodology in practice**: The compliance with the Italian data protection legislation. Computer Standards & Interfaces 27, (2005) 445-455.

MCGARRY, K. J. **O contexto dinâmico da informação: Uma análise introdutória**, tradução de Helena Vilar de Lemos – Brasília, Library Association Publishing, 1993. 03p.

MODULO SECURITY, **9º Pesquisa Nacional de Segurança da Informação**, 2003, disponível em http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf, acesso em 20 nov 2007.

MODULO SECURITY, **10ºPesquisa Nacional de Segurança da Informação**, 2006, disponível http://www.modulo.com.br/pdf/10a-PNacional-Seguranca07.pdf, acesso em 20 nov 2007.

MOITRA, S. D., KONDA, S. L., **The Survivabiliity of Networks Systems: An Empirical Analysis**, Carnegie Mellon University, Dec 2000.

MOSSE, Claude. Instituições gregas(as), Lisboa: Ed 70, 1985. 214 p

OECD, **Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**. Paris, July 2002. Disponível em http://www.oecd.org/dataoecd/16/22/15582260.pdf, acesso em 05 nov 2007.

ON LINE http://www.leadership501.com/node/24/definition-of-management, acesso em 10 jan 2008.

PELTIER, T.R. **Preparing for ISO 17799**. Security Management Practices, jan/feb, (2003) pp. 21-28.

PINHEIRO, Patrícia Peck, Direito Digital, São Paulo: Ed. Saraiva, 2007.

PIPKIN, D. L., **Information security: Protecting the global enterprise**, Prentice Hall, 2000.

REPO, A., **The Dual Approach to the Value of Information: An Appraisal of Use and Exchange Values**, Information Processing and Management 22, No. 5, 373-383 (1986).

RFC 2196, **Security Site Handbook**, September 1997.

ROBERTS, N., **Social Considerations Towards a Definition of Information Science**, Journal of Documentation, 1976, Vol. 32, Issue 4, pp 249 – 257.

RUSSELL, D., GANGEMI, Sr. G. T., **Computer Security Basics** (New York: Thunder Mountain Press, 1994).

SÁNCHEZ, L. E., VILLAFRANCA, D., **Practical Approach of a Secure Management System based on ISO/IEC 17799**. Proc. of the First International Conference on Availability, Reliability and Security (ARES'06). IEEE Computer Society (2006).

SANT'ANNA, J.P, Revista Química e Derivados, **Combate à pirataria exige técnicas de alta segurança**, disponível http://www.quimica.com.br/revista/qd461/atualidades4.html, acesso em 25 fev 2008.

SIMONSSON, M., JONHSON, P. WIJKSTRÖM, H., **Model-based IT Governance maturity assessments with Cobit**, European Conference on Information Systems, June 2007.

SSE-CMM (2007), **Systems Security Engineering – Capability Maturity Model**, disponível em http://www.sse-cmm.org/index.html, acesso em 05 nov 2007.

STEPHENS, D. W., **Variance and the Value of Information**, The American Naturalist, Vol. 134, No. 1. (Jul., 1989), pp. 128-140.

THEOHARIDOU, M., GRITZALIS, D., **Common Body of Knowledge for Information Security**, Security & Privacy Magazine, IEEE, March/April 2007, vol 5, no 2, pp. 64-67.

TOMHAVE, B. L., **Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies**, online http://falcon.secureconsulting.net/professional/papers, acesso em 21 dez 2007.

TSUJII, S. **Paradigm of Information Security as Interdisciplinary Comprehensive Science**. Proc. of the 2004 International Conference on Cyberworlds (CW'04), IEEE Computer Society, (2004) 1-12.

TSUTSUI, M. W., **W. Edwards Deming and the Origins of Quality Control in Japan**, Journal of Japanese Studies, Vol. 22, No. 2. (Summer, 1996), pp. 295-325.

UNIVERSITY OF NEW HAVEN CENTER FOR CYBERCRIME AND FORENSIC COMPUTER INVESTIGATION AND THE UNIVERSITY OF SOUTHERN CALIFORNIA DEPARTMENT OF MATHEMATICS, **Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information**, Information Systems Control Journal, ISACA, Volume 2, 2001, disponível em http://www.isaca.org, acesso em 12 dez 2007.

VALENTIM, M. L. P., **Inteligência Competitiva em Organizações: dado, informação e conhecimento**, DataGramaZero - Revista de Ciência da Informação, v.3, n.4, ago/02.

VALLS, Álvaro L. M**. O que é Ética**. 3ª ed. São Paulo: Brasiliense, 1989. (Coleção Primeiros Passos).

VAN BON, J., **IT Service Management: An Introduction.** IT Service Management Forum (2002). Van Haren Publishing. ISBN 90-806713-4-7.

VAN GREMBERGEN, W., S. DE HAES, E. GULDENTOPS (2004). **Structures, Processes and Relational Mechanisms for IT Governance**. In: Van Grembergen, W. (ed.): Strategies for Information Technology Governance. Idea Group Publishing.

VON SOLMS, B., (2005a) **Information Security Governance: Cobit or ISO 17799 or both?** Computer & Security, Vol. 24, (2005) 99-104.

VON SOLMS, B., (2005b) **Information Security Governance e Compliance management vs operational Management**, Computers & Security, Vol. 24, Elsevier, pp. 443-447, 2005.

VON SOLMS, B., **Information security – The third wave?,** Computers and Security. 2000, 19(7), November: 615-620.

VON SOLMS, B., VON SOLMS, R. **Incremental Information Security Certification**. Computers & Security 20, (2001) 308-310.

VON SOLMS, B., VON SOLMS, R., **The 10 deadly sins of information security management**, Computers & Security, Vol.23, No 5, ISSN 0167–4048, Julho, 2004, pp. 371-376.

VON SOLMS, R., VON SOLMS, B., **From policies to culture**, Computers & Security, Vol. 23, Elsevier, pp. 275-279, 2004.

WURMAN, R. S., **Ansiedade de informação: como transformar informação em compreensão**. 1.ed. São Paulo: Cultura Editores Associados, 1991. 42p.