3º CONTECSI May 31 to June 02, 2006 São Paulo, Brazil

3rd International Conference on Information Systems and Technology Management
3º Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação
11th World Continuous Auditing Conference

De 31 de Maio a 02 de Junho de 2006 – São Paulo/SP – Brasil

MODELO DE MATURIDADE DO COBIT PARA AVALIAR O NÍVEL DE MATURIDADE DO PROCESSO DE AVALIAÇÃO DE RISCOS DE UMA EMPRESA QUE UTILIZA A NBR ISO/IEC 17799

COBIT MATURITY MODEL TO EVALUATE THE MATURITY LEVEL OF THE RISK EVALUATION PROCESS OF AN ENTERPRISE THAT USES NBR ISO/IEC 17799

Maristela Jesus da Silva
(Universidade Católica de Brasília, Distrito Federal, Brasil) maris.silva@superig.com.br

Maria do Carmo Mendonça
(UCB, DF, Brasil) marmendonça@terra.com.br

Waldomiro Oliveira Junior
(UCB, DF, Brasil) waldomiro.jr@gmail.com

Rejane Maria da Costa Figueiredo
(UCB, DF, Brasil) rejane@pos.ucb.br

Colaborador: Rildo Ribeiro dos Santos
(UCB, DF, Brasil) rildo@pos.ucb.br

ABSTRACT

Security information became a stable and recognized component of corporative management, specially the technology information management. There are several mechanisms that intend to serve to this purpose, such as COBIT and NBR ISO/IEC 17799. Using the COBIT maturity model, one evaluated the maturity level of the Risk Evaluation process of an enterprise, from the perception of the employees who integrate the Security Information Committee. The referred enterprise uses NBR ISO/IEC 17799 as a structure of information security. The methodology used was a survey by means of the application of a questionnaire. The discussed questions aimed at knowing if the process P09 – COBIT Risk Evaluation performance were aligned to the applications of the NBR ISO/IEC 17799 concerning the company's Risk Evaluation process, in order to thus identify the process' maturity level. Making the co-relation between the questionnaire answers and the process P09 – COBIT Risk Evaluation maturity levels, it was found that the organization has already scored the level 1 of maturity in its Risk Evaluation process, as it has responded to 100% of that level requirements, and it has conditions to provide the necessary progress towards the process improvement, being able to reach in a short time the levels 2 and 3.

Keywords: Evaluation risk; COBIT, NBR ISO/IEC 17799; Maturity level; Security information.

RESUMO

Segurança da informação tornou-se um componente estável e reconhecido da governança corporativa, especialmente da governança em tecnologia da informação. Vários são os mecanismos que auxiliam, como o COBIT e a NBR ISO/IEC 17799. No estudo de caso utilizou-se o modelo de maturidade do COBIT, para avaliar o nível de maturidade do Processo de Avaliação de Riscos de uma empresa a partir da percepção dos empregados que integram o Comitê de Segurança da Informação. A referida empresa utiliza a NBR ISO/IEC 17799 como estrutura de segurança da informação. A metodologia definida foi pesquisa de campo e questionário. As questões abordaram se as diretrizes relacionadas ao processo PO9 – Avaliação de Riscos do COBIT estavam alinhadas às aplicações da NBR ISO/IEC 17799 no que se refere ao processo de Avaliação de Riscos da empresa, para, então, identificar o nível de maturidade do processo. Verificou-se que a empresa já atingiu o nível 1 de maturidade do seu processo de Avaliação de Riscos, uma vez que atendeu a 100% dos requisitos desse nível, e que com poucas melhorias necessárias deverá alcançar os níveis 2 e 3.

Palavras-chave: Avaliação de Riscos; COBIT; NBR ISO/IEC 17799; Nível de Maturidade; Segurança da Informação.

1 INTRODUÇÃO

A preocupação com segurança da informação é uma exigência do mundo moderno que tem requerido das organizações maior agilidade e eficácia nos negócios, de modo que elas possam sobreviver em ambientes cada vez mais competitivos e instáveis (MENEZES e TEIXEIRA, 2005: 3). Em razão disso, informação passou a ser considerada um bem de alto valor estratégico para as organizações, porém vulnerável, devido as suas características de intangibilidade e volatilidade.

Embora segurança da informação seja considerada uma parte vital da estratégia das organizações, nem sempre é fácil para os gestores alinharem a política de segurança da informação às estratégias de negócio da empresa (HÖNE e ELOFF, 2002: 402). Existem diferentes opiniões sobre como constituir uma política de segurança da informação que atenda ao objetivo de minimizar riscos e vulnerabilidades e, ao mesmo tempo, seja flexível, para comportar a evolução dos negócios.

Vários são os mecanismos que buscam atender a esse objetivo, entre eles, o COBIT (ITGI, 2005), enquanto uma estrutura mais ampla no campo da governança em tecnologia da informação (TI), e a NBR ISO/IEC 17799 (ABNT, 2005), enquanto uma estrutura mais detalhada que provê melhor orientação com relação à implementação das estratégias de segurança da informação (SI).

Segundo Gherman (2005b), o COBIT permite o acompanhamento e o *benchmarking* das práticas de controle e segurança nos ambientes de tecnologia da informação, assegura aos usuários desses ambientes a existência de controles, tornando-os responsáveis por parte desses controles, e auxilia o trabalho dos auditores de sistemas e de segurança da informação. Por essa razão, o COBIT posiciona a governança em segurança da informação dentro de uma estrutura mais ampla de governança em tecnologia da informação, provendo uma boa orientação sobre o que deve ser feito com relação à segurança da informação. Entretanto, ele não especifica como implementar os processos de segurança da informação.

Nesse aspecto, a NBR ISO/IEC 17799 provê uma estrutura melhor, na medida em que fornece informações mais detalhadas de como as coisas devem ser feitas com relação à segurança da informação. Para Solms (2004b: 101), a sinergia de combinar os benefícios da referência mais ampla e da plataforma integrada do COBIT com as orientações mais detalhadas da NBR ISO/IEC 17799 pode representar uma vantagem para as organizações com relação à implementação dos seus processos de segurança da informação.

Neste trabalho, fazendo-se uso do modelo de maturidade do COBIT, avaliou-se o nível de maturidade do Processo de Avaliação de Riscos de uma empresa que utiliza como estrutura de segurança da informação a NBR ISO/IEC 17799, a partir da percepção dos empregados que integram o Comitê de Segurança da Informação.

Nas próximas Seções 2, 3 e 4, apresenta-se o referencial teórico relacionado à segurança da informação, a NBR ISO/IEC 17799 e ao COBIT. Na Seção 5, apresenta-se a metodologia utilizada. Na Seção 6, os resultados alcançados. Na Seção 7, as conclusões e, finalizando, algumas recomendações com base nos resultados apresentados.

2 SEGURANÇA DA INFORMAÇÃO

Segurança da informação não é uma novidade em si mesma, pois desde os primórdios da humanidade que o homem busca ter acesso e controle sobre as informações que são relevantes para a sua sobrevivência (CARUSO e STEFFEN, 1999: 83). O que é novidade é o fato de a informação ter se tornado um ativo estratégico para as organizações e seus negócios, em razão da evolução dos meios e formas de registro, armazenamento, controle, uso e benefício da informação (DHILLON, 2001: 24). Conforme afirmam McGee e Prusak (1994:

53), o sucesso de um gestor está associado à qualidade de suas decisões que, por sua vez, dependem da eficiência com relação ao uso, à qualidade e à precisão das informações disponíveis. Por isso, é fundamental estar atento para o "quê" e "como" a organização protege seus ativos informacionais.

Os incidentes em segurança da informação se tornam, a cada dia, mais sofisticados e velozes, e por mais que as organizações invistam em inteligência e tecnologia, elas não conseguem evitar, de forma totalmente segura, a ocorrência de danos e riscos aos seus recursos informacionais (DIAS, 2004: 1). Incidentes ocorrem em todos os elos da cadeia da segurança da informação, especialmente naqueles relacionados a processos, tecnologias e pessoas. Desses três, pessoas é considerado o elo mais fraco e, por essa razão, é o que mais precisa ser trabalhado, assistido e melhorado. Pessoas refere-se à cultura, conscientização, capacitação e aprendizagem. Sabendo-se disso, em se tratando de segurança da informação, uma das perguntas a fazer é: Todos os empregados sabem o que se espera deles em termos de uso da informação? Se a resposta para essa pergunta for não, a política de segurança da informação da organização precisa ser repensada (BRANDÃO, 2003: 3).

Nesse sentido, segurança da informação deve ser compreendida como um ramo do conhecimento no campo da governança em tecnologia da informação (SOLMS, 2004a: 373), envolvendo não apenas um conjunto de normas, padrões e procedimentos, mas também sendo tratada como uma questão de cultura. Da mesma forma que pais e professores educam e preparam as crianças para um futuro de realizações e de segurança, as organizações precisam conscientizar, educar e preparar os seus usuários para o uso seguro da informação, caso contrário, "estarão fadadas ao fracasso na proteção da sua informação, mesmo que tenham adquirido as melhores e mais atualizadas ferramentas". (FONTES, 2005, p. 4).

A NBR ISO/IEC 17799 (ABNT, 2005: ix) define segurança da informação como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Essa definição explicita a importância da informação para os negócios e a sua elevação à categoria de um ativo de alto valor estratégico, na medida em que ela passa a fazer parte de todos os processos que impactam a vida da organização. Daí a necessidade de garantir o máximo de segurança contra riscos e ameaças, no sentido de evitar perdas financeiras, de clientes e de vantagens competitivas, bem como de comprometimento da imagem da organização.

Entendida dessa forma, segurança da informação compreende três critérios básicos: confidencialidade, integridade e disponibilidade (ABNT, 2005: 1; *ITGI*, 2000; CAZEMIER, OVERBEEK e PETERS, 1999: 66). Confidencialidade refere-se à garantia de que a informação disponibilizada pela organização seja acessível apenas às pessoas autorizadas. Integridade, por sua vez, diz respeito à exatidão, completude e confiabilidade da informação disponível e dos métodos de processamento utilizados. Já disponibilidade consiste em garantir que as pessoas certas tenham acesso às informações de que necessitam, bem como aos bens associados, no momento requerido.

Assim, para que segurança da informação possa fazer parte da cultura organizacional, fortalecendo todos os elos da cadeia, com o objetivo de minimizar riscos e incidentes e maximizar o potencial competitivo das organizações, três ações são consideradas fundamentais: adoção de uma política de segurança da informação que indique as diretrizes e descreva os requisitos básicos e filosóficos da organização; adoção de uma norma que defina como a política deve ser operacionalizada e adoção de procedimentos que detalhem como as atividades relacionadas à segurança da informação devem ser realizadas. Essas ações devem ser determinadas pela organização e contar com o compromisso da alta direção e devem ser disseminadas, ensinadas e adotadas por todos os empregados e demais partes interessadas (FONTES, 2005: 5; SOLMS, 2004a: 372).

3 NORMA NBR ISO/IEC 17799

A norma internacional NBR ISO/IEC 17799:01, hoje ABNT NBR ISO/IEC 17799:2005, tem origem no padrão britânico BS 7799 parte 1, publicada pela *BSI* (British *Standards Institution*). A BS 7799 é um padrão de excelência internacional que orienta a organização quanto a um sistema de gestão de segurança da informação (SÊMOLA, 2003: 140-141).

A versão 2002 da BS 7799 apresenta evolução compatível com as demais normas que tratam da implementação de um sistema integrado de gestão, como a ISO/IEC 9000. A BS 7799 parte 2 é um *framework* de segurança e estabelece um Sistema de Gestão de Segurança da informação – SGSI, que somado aos controles da parte 1, serve de objeto para a certificação. Com a utilização dessas normas, as empresas podem conduzir as ações de segurança sob a orientação de uma base comum, além de se prepararem para o reconhecimento de conformidade, aferido por órgãos credenciados. Segundo Sêmola (2003: 141), a importância de seguir os padrões de segurança está associada a melhorias nas relações *business-to-business* e *business-to-consume.*

A norma NBR ISO/IEC 17799 foi traduzida e disponibilizada pela ABNT – Associação Brasileira de Normas Técnicas. Seu objetivo é definir um código de prática para a gestão da segurança da informação. Contém 11 seções de controles de segurança da informação, totalizando 39 categorias principais de segurança e 136 controles. Segundo as premissas da norma, para se estabelecer requisitos de segurança há que se avaliar os riscos. Por isso, a NBR ISO/IEC 17799 aborda uma seção introdutória sobre a avaliação de riscos. As seções que compõem a norma estão descritas na Tabela 1.

De acordo com a NBR ISO/IEC 17799 (ABNT, 2005: x), "embora todos os controles sejam importantes e devam ser considerados, a relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta". Isso significa que a abrangência da implementação dos controles de segurança da informação é diretamente proporcional ao risco do negócio.

Segundo Peltier (2001: 4), risco é alguma coisa que cria ou sugere perigo e, quando não mitigada, poderá implicar perda de vantagem competitiva. Dito de outro modo, risco é a combinação da probabilidade de um evento e sua conseqüência. Por isso, é importante que seja feita análise das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação, bem como da probabilidade de sua ocorrência. A análise de risco pressupõe um processo de melhoria contínua dentro de um Sistema de Gerenciamento de Segurança da Informação – SGSI, como descreve a BS 7799 ao estabelecer as regras do PDCA, em que *Plan* (estabelecimento do SGSI) + *Do* (implementação e operação) + *Check* (monitoramento e revisão) + *Act* (manutenção e melhoria) = processo de melhoria contínua.

Tabela 1. Seções da ISO/IEC 17799:2005 (ABNT, 2005)

Seções	Objetivo
Política de Segurança da Informação	Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
Organização da segurança	Gerenciar a segurança da informação na organização, considerando a infra-estrutura e partes externas.
Gestão dos ativos	Alcançar e manter a proteção adequada dos ativos da organização.
Segurança dos recursos humanos	Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir os riscos de roubo, fraude ou mau-uso de recursos.

Segurança física e do ambiente	Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.
Gestão das operações e comunicações	Garantir a operação segura e correta dos recursos de processamento da informação.
Aquisição, desenvolvimento e manutenção de sistemas de informação	Garantir que segurança é parte integrante de sistemas de informação.
Gestão de incidentes de segurança da informação (seção introduzida na versão de 2005)	Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados permitindo a tomada de ação em tempo hábil.
Gestão da continuidade do negócio	Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil.
Conformidade	Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.

Diante do exposto, entende-se que, para uma organização implementar os controles adequados ao seu negócio e alinhá-los a NBR ISO/IEC 17799, ela deva iniciar seu processo de segurança da informação a partir da análise de risco, com base no modelo do PDCA da BS 7799, conforme apresentado na Figura 1.

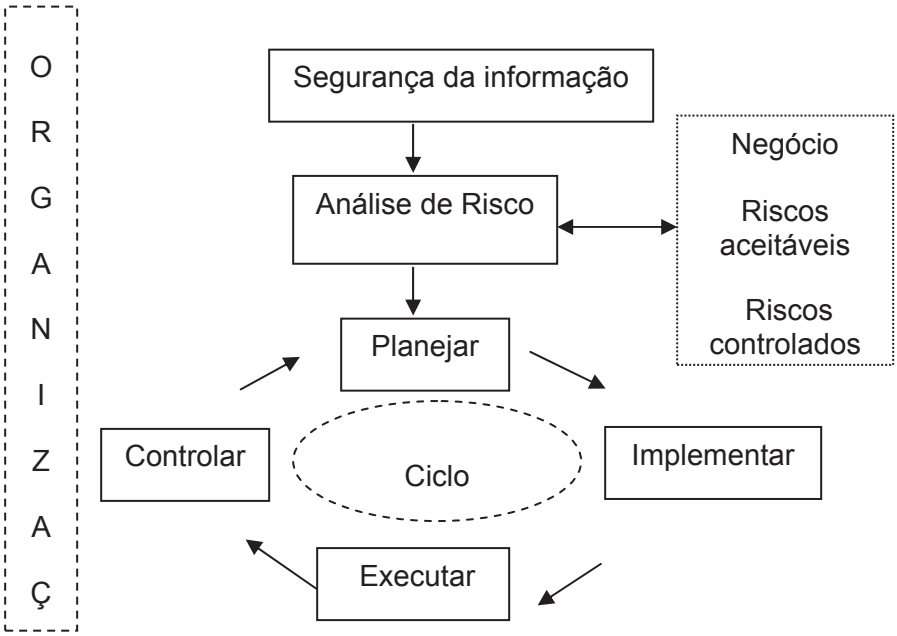

Figura 1. Modelagem de processos de análise de risco.

4 MODELO DE GOVERNANÇA – COBIT

O COBIT – Control Objectives for Information and Related Technology – foi desenvolvido pelo ISACF – *The Information* Systems Audit and Control Foundation. Posteriormente, o COBIT passou a ser mantido pelo ITGI – IT Governance Institute.

A estrutura do COBIT abrange: (i) Critérios da Informação – requerimentos de negócios para a informação: eficácia, eficiência, conformidade, confiabilidade (relacionados à confiança), confidencialidade, integridade e disponibilidade (relacionados à segurança); (ii) Recursos de TI – formado por pessoas, sistemas aplicativos, dados, tecnologias e instalações e (iii) Processos de TI – composto de domínios (agrupamentos de processos: Planejamento e Organização – PO, Aquisição e Implementação – AI, Entrega e Suporte – DS e Monitoração – MO), processos (objetivos de controle de alto nível) e atividades (desdobramentos dos processos em atividades de controle), conforme demonstrado na Figura 2.

O COBIT consiste de três modelos para o controle e gerenciamento da tecnologia da informação: Modelo de Processo (*framework*); Modelo de Governança e Modelo de Maturidade. A utilização do COBIT permite a uma instituição posicionar os seus processos de segurança da informação dentro de uma estrutura mais ampla de governança da tecnologia da informação (GHERMAN, 2005a).

O Modelo de Processo consiste de um conjunto de 318 atividades de controle, organizadas em 34 objetivos de controle de alto nível, agrupados nos 4 domínios. Cada processo visa atingir um objetivo de controle. Objetivo de controle é uma declaração de propósito ou resultado a ser alcançado por meio da implementação de controles de determinada atividade. Controles são políticas, procedimentos, práticas e estruturas organizacionais projetadas para prover razoável garantia de que os objetivos de negócio serão alcançados, e que eventos indesejáveis serão prevenidos, apagados ou corrigidos (*ITGI,* 2000: 8).

O Modelo de Governança identifica os fatores críticos de sucesso, os indicadores chave de meta e os indicadores chave de desempenho para acompanhar a implementação dos objetivos de controle. Os fatores críticos de sucesso definem os desafios mais importantes ou ações de gerenciamento que devem ser adotadas para o controle da gestão de TI, do ponto de vista estratégico, técnico, organizacional e processual. Os indicadores chave de meta, por sua vez, definem como serão mensurados os progressos das ações para atingir os objetivos da organização. Já, os indicadores de desempenho de desempenho definem medidas para determinar como os processos de TI estão sendo executados e se eles permitem atingir os objetivos planejados (FAGUNDES, 2004).

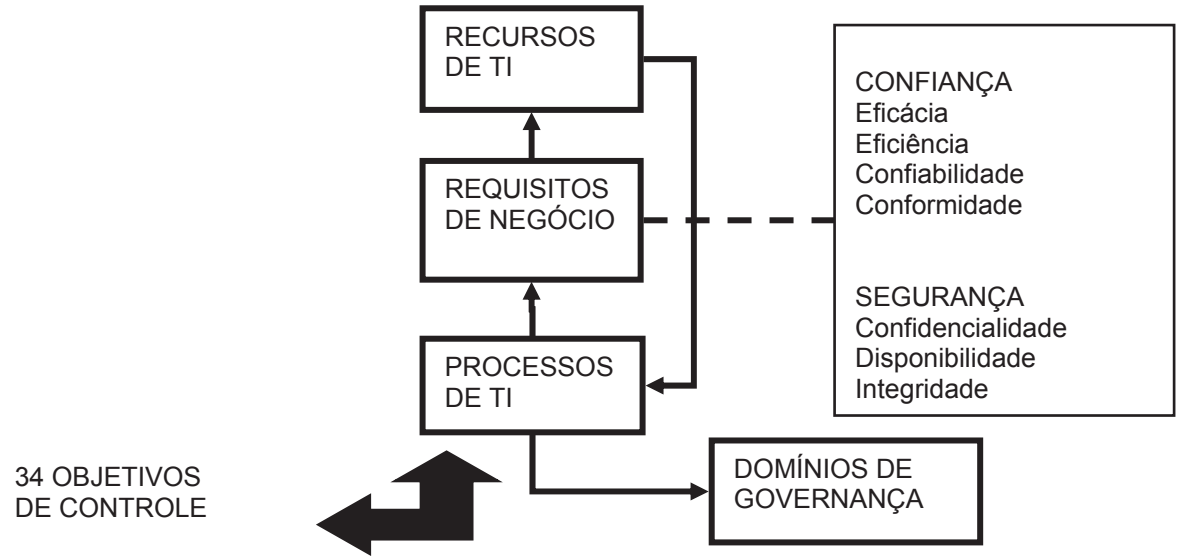

Figura 2. Estrutura do COBIT.

O Modelo de Maturidade é composto de critérios de avaliação da maturidade dos processos. Seu objetivo é auxiliar os gestores na tomada de decisão com relação aos processos de TI considerados estratégicos para o negócio da organização. A maturidade deve ser avaliada por processo.

Existem seis níveis de maturidade, de complexidade crescente:

0. Inexistente: falta absoluta de elementos reconhecíveis no processo.

1. Inicial (*ad hoc*): reconhece-se, ainda que caso a caso, o interesse de tratar da necessidade.

2. Repetível: procedimentos similares seguidos por pessoas distintas para o mesmo tipo de atividade.

3. Definido: procedimentos padronizados e documentados comunicados por meio de treinamento.

4. Gerenciado: é possível monitorar e medir a conformidade com os procedimentos.

5. Otimizado: processo automatizado baseado nas melhores práticas.

A aplicação do modelo de maturidade permite que a organização faça o diagnóstico de seus processos, identifique seu estágio atual de desenvolvimento em relação à posição desejável e implemente medidas que assegurem o alcance das metas propostas. Permite, também, que a organização identifique o nível de maturidade em que ela se encontra em comparação com outras organizações da sua categoria e com os padrões internacionais.

5 METODOLOGIA

Para a fundamentação teórica do tema abordado, buscou-se o amparo da literatura, por meio da realização de pesquisa bibliográfica. Dado o objetivo do estudo – *avaliar o nível de maturidade do processo de Avaliação de Riscos de uma empresa que utiliza como estrutura de segurança da informação a NBR ISO/IEC 17799, tendo por base o modelo de maturidade do COBIT* –, realizou-se uma pesquisa de campo junto aos profissionais que integram o Comitê de Segurança da Informação de uma empresa prestadora de serviços na área de tecnologia da informação e comunicação, por meio da utilização de questionário.

A empresa onde a pesquisa foi realizada é uma organização do setor público cuja missão é prover soluções em tecnologia da informação e comunicação para o êxito das finanças públicas e da governança do Estado, em benefício da sociedade. A empresa, alinhada às políticas governamentais, destaca-se por dispor de uma ampla rede de multisserviços, sobressaindo-se no cenário internacional por seu volume, abrangência e infra-estrutura. Tem presença em mais de 1000 municípios do País e sua rede de serviços funciona 24 horas por dia, sete dias por semana.

A amostra de respondentes foi constituída por 24 profissionais especializados em segurança da informação, de um total de 30, que compõem o Comitê de Segurança da Informação. Todos os respondentes pertencem ao quadro de pessoal efetivo da empresa e têm formação universitária, sendo 16 com grau de especialização e 1 de mestrado. Quanto aos cargos que ocupam, 15 deles são analistas, 3 técnicos e 6 gerentes. No que se refere à área de atuação, 9 trabalham com Tecnologia da Informação (*software e hardware*), 5 com Centro de Dados, 1 com Rede, 3 com Negócios e 6 atuam em outras áreas. Com relação ao tempo em que desempenham atividades relacionadas à segurança da informação, 10 trabalham com segurança da informação entre 3 e 5 anos, 8 há mais de 5 anos e 6 entre 1 e 3 anos.

O questionário da pesquisa foi elaborado com base no Guia Gerencial do COBIT, em que as diretrizes relacionadas aos objetivos de controle, fatores críticos de sucesso, indicadores chave de meta e indicadores chave de desempenho do processo PO9 – Avaliação

de Riscos do COBIT foram transformadas em questões. Algumas diretrizes foram desdobradas em mais de uma questão, bem como reformuladas quando verificada a necessidade de melhor adequá-las à realidade da empresa. O questionário, contendo 40 questões, foi dividido em três seções:

Seção 1 – constituída de quatro questões sobre informações pessoais.

Seção 2 – constituída de 26 questões referentes aos objetivos de controle, fatores críticos de sucesso e indicadores chave de meta. Para 24 questões dessa seção, foi adotada uma escala de resposta com as seguintes opções: "discordo", "concordo parcialmente", "concordo totalmente" e "não sei responder". Para as outras duas questões, adotou-se uma escala com intervalos de porcentagens, em que o respondente deveria responder considerando a sua área de atuação e o período de agosto de 2004 a julho de 2005.

Seção 3 – constituída de dez questões referentes aos indicadores chave de desempenho. Para responder as questões dessa seção, o respondente deveria considerar a sua área de atuação e o período de agosto de 2004 a julho de 2005. Foi construída uma escala de resposta com intervalos de números e porcentagens, de acordo com o objetivo de cada questão.

Na Tabela 2, apresenta-se exemplos de questões do questionário referentes a cada uma das diretrizes.

Tabela 2. Exemplos de questões.

Objetivo de controle Na organização existe um gerenciamento periódico dos principais riscos de tecnologia da informação e comunicação que afetam os objetivos do negócio. ( ) Não sei responder ( ) Discordo ( ) Concordo Parcialmente ( ) Concordo Totalmente
Fator crítico de sucesso A estrutura de informações dos riscos é mantida e alimentada pelos relatórios de incidentes. ( ) Não sei responder ( ) Discordo ( ) Concordo Parcialmente ( ) Concordo Totalmente
Indicador chave de meta Houve aumento do grau de consciência da necessidade de avaliação de risco. ( ) Não sei responder ( ) Discordo ( ) Concordo Parcialmente ( ) Concordo Totalmente
Indicador chave de desempenho Qual a porcentagem dos processos de TI documentados de forma completa e formal no período de agosto de 2004 a julho de 2005? ( ) Não sei responder ( ) 0% ( ) 1%-25% ( ) 26%-50% ( ) 51%-75% ( ) 76%-100%

As questões abordadas visaram saber, com base na percepção dos profissionais integrantes do Comitê de Segurança da Informação, se as diretrizes relacionadas aos objetivos de controle, fatores críticos de sucesso, indicadores chave de meta e indicadores chave de desempenho do processo PO9 – Avaliação de Riscos do COBIT estavam alinhadas às aplicações da NBR ISO/IEC 17799 no que se refere ao processo de Avaliação de Riscos da empresa para, então, identificar o nível de maturidade do processo, utilizando-se o modelo de maturidade do COBIT.

A escolha do processo PO9 – Avaliação de Riscos do COBIT, como processo de referência, foi feita a partir da identificação dos processos de TI do COBIT relacionados à segurança da informação, considerados como principais em relação aos Critérios da Informação (confidencialidade, integridade e disponibilidade) e aplicáveis a todos os Recursos de TI (pessoal, sistemas aplicativos, tecnologias, instalações e dados), conforme

apresentado na Tabela 3. A escolha recaiu sobre o processo PO9 – Avaliação de Riscos em razão do seu completo relacionamento com os Critérios da Informação e os Recursos de TI. O processo PO9 – Avaliação de Riscos visa dar suporte às decisões gerenciais para atingir os objetivos de TI; responder às ameaças; identificar os fatores chave de decisão para a organização; analisar os riscos versus os impactos versus a probabilidade de ocorrerem e identificar as medidas que, com custos adequados, possam mitigar os riscos.

Tabela 3. Matriz de relacionamento dos principais processos do COBIT relacionados à Segurança da Informação.

Dimensão	Processos	Critérios da Informação			Recursos de TI				
		C	I	D	P	A	T	I	D
Planejamento & Organização	PO9 Avaliar riscos	p	p	p	v	v	v	v	v
	PO11 Gerenciar qualidade		p		v	v	v	v	
Aquisição & Implementação	AI6 Gerenciar mudanças		p	p	v	v	v	v	v
Suporte & Produção	DS4 Garantir a continuidade dos serviços			p	v	v	v	v	v
	DS5 Garantir a segurança dos sistemas	p	p		v	v	v	v	v
	DS11 Gerenciar dados		p						v
	DS12 Gerenciar instalações		p	p				v	

Legenda: p – principal; v – aplicável em
Critérios da Informação: C – Confidencialidade; I – Integridade; D – Disponibilidade
Recursos de TI: P – Pessoal; A – Aplicações; T – Tecnologia; I – Instalações; D – Dados

6 RESULTADOS

Para uma melhor organização dos resultados, as respostas foram analisadas por bloco de questões, na seguinte seqüência: objetivos de controle, fatores críticos de sucesso, indicadores chave de meta e indicadores chave de desempenho. Analisados os resultados, buscou-se identificar o nível de maturidade do processo utilizando o modelo de maturidade do COBIT.

6.1 Objetivos de Controle

Objetivos de controle são declarações genéricas que definem o que é necessário ser gerenciado em cada processo. Para o processo de Avaliação de Riscos, o sistema de controle deve balancear prevenção, detecção e mensuração do nível aceitável de riscos e elaborar um plano de ação que contemple estratégias para evitar, mitigar ou aceitar os riscos. Para avaliar os objetivos de controle, foram formuladas doze questões. Os resultados das respostas encontram-se demonstrados na Figura 3 e indicam que:

Das doze questões, os respondentes concordam parcialmente com oito: existe um gerenciamento periódico dos principais riscos de tecnologia da informação e comunicação que afetam os objetivos do negócio (75%); a gerência reavalia os riscos e atualiza-os com base nos resultados de auditorias, inspeções e incidentes ocorridos (75%); a análise de riscos identificados resulta em medidas quantitativas e qualitativas, considerando a avaliação do nível aceitável de exposição (50%); o plano de ação de riscos assegura a implantação de controles de custo efetivo e medidas de segurança para reduzir o nível de exposição da área de TI aos riscos e identificar a estratégia de riscos (evitar, mitigar ou aceitar) (54,17%); o enfoque de avaliação de riscos contempla a definição formal da aceitação de riscos residuais

que são compensados com contratação de seguro e responsabilidades contratuais (41,67%); o sistema de controle existente equilibra a prevenção, a detecção, a correção e as medidas de recuperação, priorizando controles que proporcionam melhores retornos aos clientes (58,33%); a gerência monitora a efetividade das medidas de controle (62,5%) e a gerência incentiva a avaliação dos riscos como uma importante ferramenta que proporciona informações para o desenho e implementação de controles internos, a definição do plano estratégico de TI e o monitoramento da segurança (66,67%).

Do total de respondentes, 75% concordam totalmente que existe uma metodologia definida para avaliação de riscos que contempla as responsabilidades e as habilidades para o desempenho da atividade; 58,33% que a gerência, os especialistas de segurança e os especialistas de TI estão envolvidos na identificação, mitigação e controle dos riscos; 58,33% que o enfoque da avaliação de riscos está direcionado para identificar os elementos essenciais que compõem os riscos: ativos tangíveis e intangíveis, ameaças, vulnerabilidades, proteções, conseqüências e probabilidades de ocorrências e 54,17% que a qualificação e a quantificação dos riscos estão associadas à identificação dos riscos (do negócio, regulamentar, legal, tecnológico, humano, terceiro).

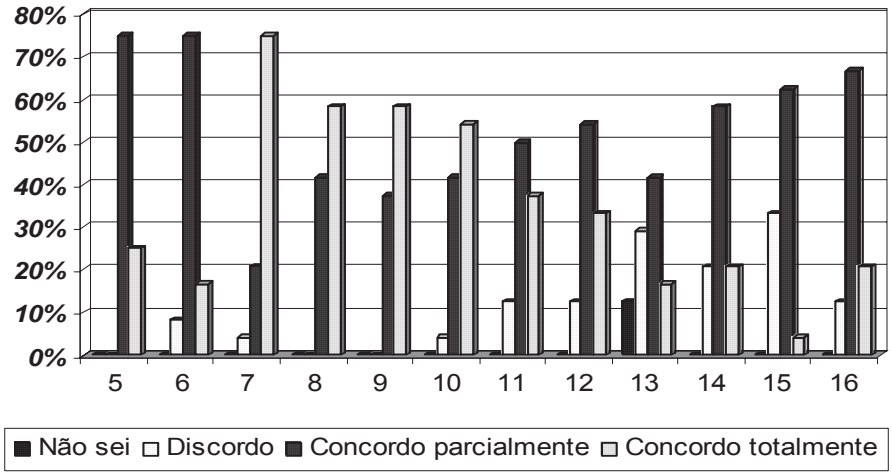

Figura 3. Respostas das questões relativas aos Objetivos de Controle.

6.2 Fatores Críticos de Sucesso

Fatores críticos de sucesso definem as diretrizes mais importantes a serem consideradas pela administração para alcançar o controle com os processos de TI, do ponto de vista estratégico, técnico, organizacional e processual. No contexto da análise de riscos, os fatores críticos de sucesso indicam se as condições essenciais para gerir e mitigar os riscos estão presentes. Na pesquisa, foram aplicadas oito questões para avaliação dessas diretrizes. Os resultados encontram-se demonstrados na Figura 4, onde se depreende que.

Das oito questões, os respondentes concordam parcialmente com quatro: a estrutura de informações dos riscos é mantida e alimentada pelos reportes de incidentes (50%); existe uma política estabelecida para definir os limites e as tolerâncias aos riscos (45,83%); a avaliação de riscos é realizada pela comparação das vulnerabilidades, ameaças e valor dos dados (50%) e existem responsabilidades e procedimentos para a definição, aceitação e investimento de melhorias no gerenciamento de riscos (66,67%).

Do total de respondentes, 58,33% concordam totalmente que o foco primário das avaliações de riscos são as ameaças reais e secundariamente as ameaças teóricas; 50% que são realizadas periodicamente sessões de *brainstorming* e análises das causas que levam à identificação e mitigação dos riscos e 58,33% que existem papéis e responsabilidades definidos para o gerenciamento dos riscos.

Já 50% dos respondentes discordam que é realizada periodicamente uma validação da estratégia de gerenciamento de riscos por terceiros para aumentar a objetividade.

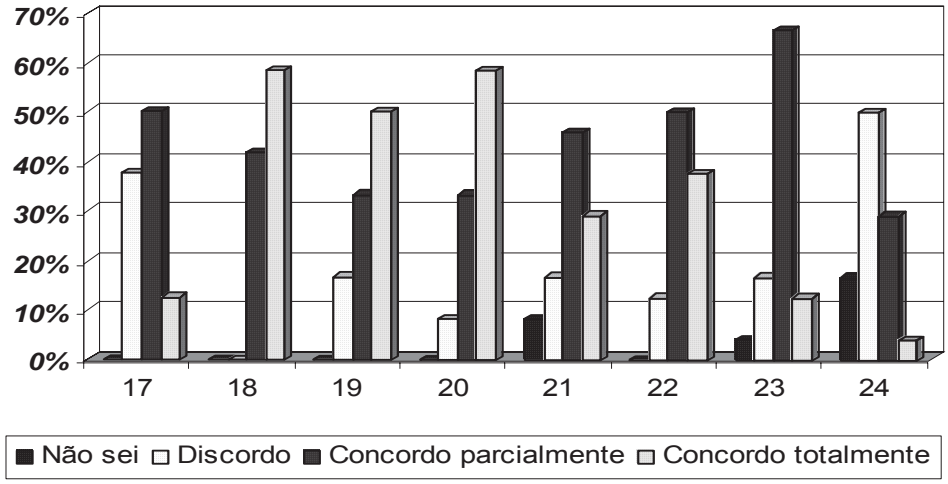

Figura 4. Respostas das questões relativas aos Fatores Críticos de Sucesso.

6.3 Indicadores Chave de Meta

Indicadores chave de meta compreendem as diretrizes a serem consideradas pela administração para medições que indiquem quais processos satisfazem o negócio, considerando a perspectiva financeira, do cliente e dos processos internos. Indicam o cumprimento das metas nos processos de TI relativas à análise de riscos. Para verificar essas diretrizes, foram formuladas seis questões. Os resultados das quatro primeiras questões encontram-se demonstrados na Figura 5 e indicam que:

Das quatro questões, os respondentes concordam parcialmente com duas: houve aumento do grau de consciência da necessidade de avaliação de riscos (50%) e houve diminuição do número de incidentes calculados por riscos já identificados (45,83).

Quando perguntados se houve aumento do número de processos de TI que têm avaliações de riscos, 60,87% dos respondentes concordam totalmente.

Quanto a ter havido aumento de riscos identificados que foram adequadamente mitigados, 37,5 discordam.

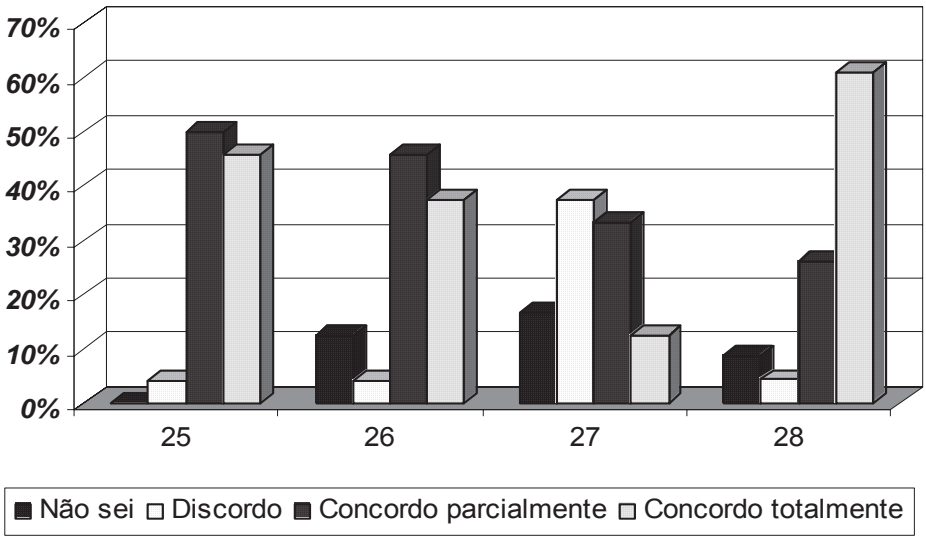

Figura 5. Respostas das questões relativas aos Indicadores Chave de Meta

As duas últimas questões dessa seção objetivaram medir resultados percentuais dos processos de TI documentados de forma completa e formal e dos processos de TI com custo de avaliação de riscos já identificado, considerado o período de doze meses (agosto de 2004 a julho de 2005). Destaca-se que 62,5% e 54,16% dos respondentes, respectivamente, não souberam responder.

6.4 Indicadores Chave de Desempenho

Indicadores chave de desempenho compreendem as diretrizes a serem consideradas pela administração para avaliar o conhecimento de quão bem está se executando o processo frente ao objetivo de controle que se deseja alcançar. Esses indicadores têm afinidade com os indicadores chave de meta quando se olha o desempenho considerando a perspectiva financeira, do cliente e dos processos internos. Buscam monitorar o desempenho dos processos de acordo com as metas estabelecidas. Para atender a essas diretrizes, foram formuladas dez questões com o objetivo de verificar resultados de processos internos de monitoração e mitigação de riscos durante um período de doze meses (agosto de 2004 a julho de 2005). Os resultados mostraram que:

Foram realizados de 1 a 5 treinamentos em gerenciamento de riscos.

Foram realizados de 1 a 5 projetos para o aprimoramento do gerenciamento de riscos.

Foram realizadas de 1 a 3 melhorias no processo de avaliação de riscos.

Foram realizadas de 1 a 3 atualizações das políticas e dos limites de riscos estabelecidos. As atualizações das políticas e dos limites de riscos são realizadas anualmente.

Foram elaborados mais de 10 relatórios de monitoramento de riscos, sendo que 58,33% dos respondentes não souberam responder a freqüência com que os relatórios são elaborados.

Foram treinadas de 1 a 200 pessoas na metodologia de gerenciamento de riscos.

Com relação ao treinamento na metodologia de gerenciamento de riscos, a pesquisa mostrou que 62,5% dos respondentes já participaram de 1 a 5 treinamentos desde que atuam na área de segurança da informação, sendo que apenas 1 deles informou não ter recebido nenhum treinamento.

Quando perguntados sobre o percentual do orçamento de TI alocado para projetos de gerenciamentos de riscos, 83,33% não souberam responder.

6.5 Nível de Maturidade do Processo

O Modelo de Maturidade do Processo PO9 – Avaliação de Riscos do COBIT enfoca o controle do processo em relação às metas do negócio para apoiar o gerenciamento de decisões, a fim de alcançar os objetivos de TI e responder as ameaças por meio da redução da complexidade, aumento da objetividade e identificação dos fatores de decisão importantes.

Com base nos requisitos de maturidade do Modelo de Maturidade do COBIT para o processo PO9 – Avaliação de Riscos e nos resultados da pesquisa, buscou-se verificar o nível de maturidade do processo de Avaliação de Riscos da empresa. Para isso, construiu-se uma escala de valores, com o objetivo de identificar o quanto a empresa atende aos requisitos dos níveis de maturidade estabelecidos pelo COBIT no que se refere ao processo analisado, sendo que:

0% - a organização não atende o requisito

50% - a organização atende parcialmente o requisito

100% - a organização atende totalmente o requisito

Para verificar a conformidade da maturidade do processo de Avaliação de Riscos da empresa com os requisitos de maturidade do processo PO9 – Avaliação de Riscos do COBIT, foi construída a Tabela 4 contemplando:

(i) nível de maturidade;

(ii) descrição dos requisitos por nível de maturidade do processo PO9 – Avaliação de Riscos do COBIT e identificação das questões do questionário relacionadas a cada requisito; e

(iii) percentuais de atendimento dos requisitos – 0%, 50%, 100%

Fazendo-se a correlação das respostas das questões do questionário com os níveis de maturidade do processo PO9 – Avaliação de Riscos, verificou-se que a empresa já atingiu o nível 1 de maturidade do seu processo de Avaliação de Riscos, uma vez que atendeu a 100% dos requisitos desse nível. Merece destaque a posição da empresa nos níveis 2 e 3.

Tabela 4. Conformidade da maturidade do processo de Avaliação de Riscos da empresa com os requisitos de maturidade do processo PO9 – Avaliação de Riscos do COBIT.

Nível	Requisitos de maturidade do processo PO9 – Avaliação de Riscos do COBIT / Identificação das questões do questionário	0%	50%	100%
0	Ocorre a avaliação de riscos associado ao impacto no negócio. (Questões 7 e 28)			X
	A gestão de riscos identifica a solução de TI necessária à entrega do serviço. (Questão 9)			X
1	A organização tem consciência de sua responsabilidade legal, contratual e dos riscos e considera os riscos de TI para definir seus processos e políticas. (Questão 10)			X
	A avaliação de riscos é formal e de acordo com cada projeto. (Questão 7)			X
	A gestão de riscos segue um planejamento para transferir gestões específicas que envolvem cada projeto (Questão 9)			X
	O risco relativo a TI que envolve segurança, avaliação e integridade é considerado por projeto específico. (Questão 28)			X
	Os riscos de TI que afetam o dia-a-dia operacional são freqüentemente discutidos em reuniões e a mitigação é consistente. (Questão 8)			X
2	Existe um entendimento emergente de que os riscos são importantes e necessitam ser considerados. (Questão 25)		X	
	As propostas de avaliação de riscos encontram-se desenvolvidas e implementadas. (Questão 18)			X
	A avaliação de riscos é realizada em todos em níveis e aplicada em todos os projetos. (Questão 9)			X
	A avaliação de riscos é sistematizada. (Questão 7)			X
	A gestão de TI tem procedimentos e descrições de trabalho definidos para tratar a gestão de riscos. (Questão 11)		X	

Nível	Requisitos de maturidade do processo PO9 – Avaliação de Riscos do COBIT / Identificação das questões do questionário	0%	50%	100%
3	A organização tem política de gestão de riscos que define quando e como conduzir a avaliação de riscos. (Questão 21)		X	
	O processo de avaliação de riscos é definido, documentado e disponibilizado (Questão 7)			X
	Decisões de seguir o processo recebem ações de treinamentos. (Questões 29, 33 e 41)			X
	A metodologia é convincente e garante que os riscos do negócio são identificados e que todos os projetos são cobertos ou que as operações em curso são examinadas por risco ou base regular. (Questões 14 e 16)		X	
4	A avaliação de riscos tem procedimentos padrões e os procedimentos são notificados para a gestão de TI. (Questão 23)		X	
	A gestão de riscos é realizada por um gestor sênior. (Questões 15 e16)		X	
	O processo é avançado e o risco é avaliado em nível de projeto individual com o envolvimento de toda operação de TI. (Questões 21 e 28)			X
	A gestão de riscos envolve os efeitos do risco, analise de cenários, para identificar o crescimento das ameaças, tendências e estratégias de TI. (Questões 11, 19 e 22)		X	
	A gestão é capaz de monitorar a posição do risco, para antecipar as decisões e tornar os níveis aceitáveis. (Questões 11, 15 e16)		X	
	O gestor sênior de TI determina os níveis de riscos que a organização poderá tolerar e dispõe de padrões de medição para o risco. (Questões 13 e14)		X	
	A gestão de riscos é institucionalizada. (Questões 5 e 21)		X	
5	A avaliação de riscos foi desenvolvida em estágios diferentes onde a estrutura e os mega-processo são cumpridos e gerenciados. (Questão 24)	X		
	O *brainstorming* de riscos é a raiz da causa da análise e envolve expertise individual e são aplicadas em toda a organização. (Questão 19)			X
	A identificação, análise e reporte da gestão de riscos são altamente automatizados. (Questão17)		X	
	A gestão de riscos é realmente integrada dentro de todos os negócios e operações de TI, e é aceita e extensiva a todos os usuários dos serviços de TI. (Questões 22 e 23)		X	

7 CONCLUSÕES

Constatou-se que o modelo de maturidade do COBIT é um referencial para avaliar o processo de Avaliação de Riscos de uma empresa que utiliza a NBR ISO 17799.

De acordo com o modelo de maturidade do COBIT para o processo PO9 – Avaliação de Riscos, conclui-se que o processo de Avaliação de Riscos da empresa possui nível 1 de maturidade, tendo atingido 100% dos requisitos desse nível. Conclui-se, também, que a empresa dispõe de condições para prover as melhorias necessárias ao aperfeiçoamento do processo podendo, em pouco tempo, alcançar os níveis 2 e 3 de maturidade. O que demonstra que a organização investe na evolução dos controles relacionados à segurança da informação com o objetivo de garantir o sucesso do seu negócio.

Para trabalhos futuros, sugere-se: (i) replicar a metodologia utilizada na pesquisa em outros processos; e (ii) elaborar uma metodologia para avaliação do nível de maturidade dos processos de TI com foco nos controles e requisitos de auditoria do COBIT, que seja referencial de melhores práticas.

Em vista dos resultados da pesquisa, para que a organização alcance maiores níveis de maturidade do processo de Avaliação de Riscos, é recomendável que:

- Incorpore atividades que respondam plenamente ao nível 2, tomando consciência das lacunas do processo ainda presentes nesse nível e buscando os recursos necessários para atingi-los, especialmente no que diz respeito à existência de um entendimento emergente de que os riscos são importantes e necessitam ser considerados e à adoção de procedimentos e descrições de trabalhos definidos para tratar a gestão de risco.

- Envide esforços no sentido de atender plenamente aos requisitos do nível 3 quanto a uma política de gestão de riscos que defina quando e como conduzir a avaliação de riscos e à definição de uma metodologia que garanta que os riscos do negócio sejam identificados, que todos os projetos estejam cobertos e que as operações em curso sejam examinadas por risco.

- Adote um modelo de governança corporativa em que os investimentos em TI relativos aos riscos do negócio sejam controlados e verificados por meio de resultados, por exemplo, quanto custou investir em tecnologia para mitigar os riscos e qual o retorno financeiro para o negócio.

- Adote uma metodologia para avaliar o nível de maturidade dos processos relacionados à segurança da informação.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 17799**: Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

Brandão, Carlos Eduardo. **Conhecendo e implementando políticas de segurança da informação**. Palestra proferida na SUCESU/ES em 06/11/2003. Disponível em http://www.sucesues.org.br/eventos/agenda_passada.asp?cod_evento=124 Acesso em 07 nov 2005.

BSI - British Standards Institution. **BS7799 – *Information Tecnology***: *Code of practice for information security management*, 2000.

BSI - British Standards Institution. **BS7799 – *Information security management* –** *Part 2*: Specification for information security management systems, 2000.

Caruso, A. e Steffen, Fávio D. **Segurança em Informática e de Informações**. São Paulo: Senac, 1999.

Cazemier, Jacques A.; Overbeek, Paul L.; Peters, Louk M.C. ***ITIL***: *Best Practice for Service Management. TSO*, 1999.

CERT.BR – Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas dos incidentes reportados ao CERT.Br**. Disponível em http://www.cert.br/stats/incidentes/. Acesso em 07 nov 2005.

Dhillon, Gurpreet. ***Information Security Management*** – *global challenges in the new millennium*. *Idea Group Publishing*, 2001.

Dias, Sérgio. **A evolução da segurança e os desafios atuais**. Palestra Webcasts Technet, 2004 Disponível em http://www.microsoft.com/brasil/technet/Eventos/EventosDownloadsWebCasts.mspx , acesso em 07 nov 2005.

Fagundes, Eduardo Mayer. **COBIT: Um kit de ferramentas para a excelência na gestão de TI**, 2004. Disponível em: http://www.efagundes.com/Artigos/COBIT.htm. Acesso em: 10 nov 2005.

Fontes, Edison**. Formação de Cultura em Segurança da Informação**. São Paulo: *InfoSec Council for Trustworthy Computing*, 2005. Versão 4.2. Disponível em: http://www.isaca.org.br/eventos/INFOSEC.Formacao.Cultura.V.4.2.pdf. Acesso em 07 nov 2005.

Gherman, Marcelo. **COBIT: Integrando TI aos negócios** – parte I, Módulo Security Magazine, 2005a. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=459&pagenumber=0&idiom=0. Acesso em 07 nov 2005.

Gherman, Marcelo. **COBIT: Integrando TI aos negócios** – parte II, Módulo Security Magazine, 2005b. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=461&pagenumber=0&idiom=0. Acesso em 07 nov 2005.

Humphreys, E J, Moses, R H, Plate, A E. ***Guide to Risk Assessment and Risk Management***. Editor: E J Humphreys. *XiSEC Consultants Ltd. Syntegra Ltd*. GISA, Germany

Höne, Karin e Eloff, J.H.P. ***Information Security Policy*** – *what do international information security standards say?* Elsevier: *Computers & Security*, 21, 402-409, 2002.

ITGI – *IT Governance Institute*. ***COBIT*** – *Control Objectives for Information and Related Technology – Management Guidelines*. 3ª edição, 2000. Disponível em: http://www.itgi.org. Acesso em 21 out 2005.

McGee, James e Prusak, Laurence. **Gerenciamento Estratégico da Informação**. Rio de Janeiro: Campus, 1994.

Menezes, Regina S. e Teixeira, Francisco. **Gestão da Segurança da Informação**: práticas de segurança da informação implementadas em duas organizações que atuam no Estado da Bahia, 2005. Disponível em: http://www.gepicc.ufba.br/enlepicc/pdf/ReginaSáMenezes.pdf. Acesso em 07 nov 2005.

Peltier, Thomas R. ***Information Security Risk Analysis***. *AUERBACH Publications*. USA. 2001. Disponível em: http://www.auerbach-publications.com . Acesso em 07 nov 2005.

Sêmola, Marcos. **Gestão da Segurança da Informação**: uma visão executiva. Editora Campos, 2003.

Solms, Rossouw von. ***The 10 deadly sins of information security mangement***. Elsevier: *Computers & Security*, 23, 371-376, 2004a.

Solms, Rossouw von. ***Information Security Governance***: *COBIT* or ISO 177999 or both? Elsevier: *Computers & Security*, 24, 99-104, 2004b.