Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Mário Sérgio Ribeiro

Proposta de um modelo de maturidade de combate à fraude computacional interna

São Paulo

2010

Mário Sérgio Ribeiro

Proposta de um modelo de maturidade de combate à fraude computacional interna

Mário Sérgio Ribeiro

Proposta de um modelo de maturidade de combate à fraude computacional interna

Dissertação de Mestrado apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo – IPT, como parte dos requisitos para obtenção do título de Mestre em Redes de Computadores

Data da aprovação _____/_____/_____

_____
Prof. Dr. Volnys Bernal (Orientador)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Membros da Banca Examinadora:

Prof. Dr. Volnys Borges Bernal (Orientador)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Prof. Dr. Frank Meylan (Membro)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Prof. Dr. Adilson Guelfi (Membro)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Mário Sérgio Ribeiro

Proposta de um modelo de maturidade de combate à fraude computacional interna

Dissertação de Mestrado apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo – IPT, como parte dos requisitos para obtenção do título de Mestre em Engenharia da Computação

Área de Concentração: Redes de Computadores

Orientador: Prof. Dr. Volnys Borges Bernal

São Paulo
Abril/2010

Ficha Catalográfica
Elaborada pelo Departamento de Acervo e Informação Tecnológica – DAIT
do Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT

R484p Ribeiro, Mário Sérgio
Proposta de um modelo de maturidade de combate à fraude computacional interna. /
Mário Sérgio Ribeiro. São Paulo, 2010.
109p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Volnys Borges Bernal

1. Fraude computacional 2. Empresa 3. ISO 15504:2008 4. COBIT 5. Modelo de maturidade e capacidade de integração 5. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Coordenadoria de Ensino Tecnológico II. Título

10-47 CDU 004.056.2(043)

Dedicatória

Dedico esse trabalho para:

DEUS: que me deu a vida e a oportunidade de ter nascido em um lar, que com sacrifício, mostrou-me que o caminho certo a trilhar era o do estudo.

Meu pai: que enquanto esteve vivo, trabalhou sem parar para que eu pudesse estudar.

Minha mãe: sempre junto em todos os instantes. Na falta cedo do Pai, tomou o seu lugar e cumpriu sua missão. Minha mais reverenciada homenagem a ela, hoje com 90 anos!

Minha esposa: por toda companhia e paciência nessa árdua trajetória que é o Mestrado. É preciso ser muito companheira. Obrigado para sempre!

Todos os professores: gostaria de colocar o nome de cada um deles, desde o primário, mas fica aqui meu agradecimento a todos que me ajudaram a ser o cidadão que sou.

Agradecimento

Uma decisão difícil para quem está fazendo um mestrado é a hora de escolher o seu orientador. Todos comentam sobre essa questão. Confesso que não tive dúvida: prof. Volnys.

Todo e qualquer agradecimento que eu tenha que fazer deve e é dirigido ao prof. Volnys. As qualidades como pessoa e profissionais tornam as coisas mais fáceis para qualquer mestrando. Obrigado Volnys pela paciência e dedicação!

Meus agradecimentos ao IPT na figura do coordenador do mestrado, prof. Mário Miyake. Foi muito bom ter sido aluno de tão prestigiosa instituição.

RESUMO

As perdas médias causadas por fraudes computacionais perpetradas por colaboradores internos (agente de ameaça interna) vêm crescendo ano após ano, com valores anuais da ordem de U$ 78,000 por evento. Isso tem feito com que as organizações pensem sobre a melhor maneira de conter o avanço dessas perdas. Apesar de sua complexidade, o combater a fraude computacional interna passa a ser uma medida imperativa para a maioria das organizações, independente de seu tamanho. Prevenir, detectar, investigar e responder a fraude computacional interna (FCI) são alguns dos domínios que devem ser enxergados e, contemplados com processos que tornem capaz à essas organizações combater a FCI. Para isso, conhecer o grau de maturidade atual em que se encontram esses domínios e processos e buscar as melhorias nos resultados e nas capacidades dos processos que necessitam ser melhorados é um passo importante no combate à FCI. Este trabalho procura contribuir apresentando uma proposta para tratar o problema, de forma a permitir a atuação progressiva, sistemática, monitorada e controlada na melhoria dos resultados e das capacidades dos processos de combate à FCI. Ocorre com o uso de um modelo de maturidade de combate à FCI, utilizando como estrutura para construção do modelo, a norma ABNT ISO 15.504:2008 de avaliação de processos e modelos de maturidade conhecidos pelo mercado como os do CMMI e COBIT. Os componentes desse modelo de maturidade de combate à FCI, são um modelo de processos de combate à FCI, um modelo de avaliação da maturidade dos processos e um modelo de melhoria dos processos de combate à FCI.

Palavras chaves: fraudes computacionais internas, combate à FCI, modelo de maturidade, domínios, processos, ISO 15.504:2008, COBIT, CMMI.

ABSTRACT

Proposal of a maturity model against internal computer fraud

The average loss due to computational frauds committed by internal staff (internal threat agents) has increased yearly. The annual amount loss is around U$ 78,000 each event, leading companies to think about the best way to retain more advances in this figure. Although the complex situation, to struggle the internal computational fraud (ICF) is an imperative measure in most of the organizations, no matter their size. Preventing, detecting, investigating and answering to internal computational frauds are some of the actions to consider and add to processes that will enable the organizations to struggle the ICF. Therefore, it is an important step to know the current maturity stage in which one may find these processes and search for better results in those that need improvement. The aim of this work is to contribute, presenting a proposal to help find the solution to the problem. It will enable the progress action, in a systemic, monitored and controlled way to improve the results and process skills against the ICF. It happens using a maturity model against ICF, according to the ABNT ISO 15.504:2008 standards, in the process valuation and maturity models known in the market as CMMI and COBIT. The components of this maturity model against ICF are: one model of process against ICF, one model of process maturity valuation and one model of process improvement against ICF.

Key word: internal computational frauds, against ICF, maturity model, domains, process, ISO 15.504:2008, COBIT, CMMI.

Lista de Ilustrações

Lista de Tabelas

SUMÁRIO

1 INTRODUÇÃO

1 Introdução

Um preço que vem sendo pago pelos avanços proporcionados pelo uso da computação nas empresas são as ações intencionais praticadas por pessoas que trabalham com sistemas computacionais. Uma dessas ações são as fraudes computacionais internas, uma ameaça capaz de ser perpetrada por funcionários, terceiros e outros que trabalham no interior das organizações.

Pressionado geralmente por questões financeiras e aproveitando-se das oportunidades proporcionadas pela empresa, em face da fragilidade em seus controles internos, esses indivíduos perpetram sua fraude utilizando recursos computacionais.

A KPMG (2005) no Brasil, em uma pesquisa sobre fraudes no Brasil do ano de 2004 “A Fraude no Brasil – Relatório de Pesquisa 2004”, entre tantas conclusões, algumas chamaram a atenção. Dos pesquisados, 45% vêem a fraude como uma séria ameaça; 55% enxergam como tendência futura o crescimento do nível de fraudes no Brasil e 69% alegaram que já tiveram a empresa como vítima de fraude.

A *Association of Certified Fraud Examiners* - ACFE (2008), entre alguns números de seu relatório, apontou que as fraudes cometidas por colaboradores com cargos abaixo de gerentes causam perdas médias de U$ 78.000,00 ao ano, enquanto que as fraudes cometidas por gerentes causam perdas médias de U$ 218.000,00 e executivos e proprietários de U$ 1.000.000,00 ao ano.

O combate às fraudes computacionais é uma atividade sistemática a ser praticada pelas organizações. Uma das formas para mitigar os danos que a fraude possa imputar é entender a situação atual da empresa para com a questão e decidir qual o nível aceitável de gerenciamento e controle se necessita ter. Um método conhecido para ser utilizado nessa questão é a dos Modelos de Maturidade.

Não existem trabalhos diretamente relacionados a modelos de maturidade para combater a fraude computacional interna. Entre os vários trabalhos já publicados sobre o tema, Romney e Steinbart (2006) tratam da fraude computacional interna (FCI) e discutem medidas para a sua prevenção e detecção, sem discutir modelos de maturidade. Schultz e Shumway (2002) têm uma contribuição acerca de uma metodologia em seis etapas para responder a incidentes computacionais, sem citar modelos de maturidade.

Entretanto, um modelo de Governança de TI, que em seu conteúdo tem um modelo de maturidade bem conhecido e utilizado pela área de Tecnologia da Informação, para avaliar a maturidade de processos da TI é o arcabouço conhecido como COBIT (*Control Objectives for Information and related Technology*) – (ISACA, 2007). O modelo de maturidade é aplicado para os trinta e quatro processos listados pelo COBIT. Outros modelos de maturidade que podem ser citados são o CMMI (Capacity Maturity Model Integration) – (SEI, 2007) e o MPS.BR (Melhoria de Processos do Software Brasileiro) (MPS, 2008) .

A *American Institute of Certified Public Accountants* – (AICPA, 2008) em seu documento *Managing the business risk of Fraud: a pratical guide*, recomenda caminhos na qual o conselho de administração, alta administração e auditores internos podem combater a fraude em sua organização.

1.1 Motivação

O combate à fraude computacional interna é realizado pela aplicação de controles que visam minimizar o risco da fraude acontecer. Existem diversas práticas relacionadas aos controles e gestão do risco, entre elas o *Control Objectives for Information and related Technology* (COBIT) – (ISACA,2007) e a família NBR ISO/IEC 27000 – (ABNT,2005), (ABNT,2006) e (ABNT,2008).

Porém, no âmbito de uma organização não é possível avaliar o grau de combate à fraude observando somente os controles. É necessário elevar o nível de atuação para tratar os processos relacionados à FCI. Estes processos

que são responsáveis pela aplicação dos controles necessários ao combate à FCI.

A *Information Systems Audit Control Association* – (ISACA, 2007) em seu documento COBIT versão 4.1, voltado à governança de TI, trata de modelos de maturidade genéricos para os quatro domínios do escopo do arcabouço COBIT (Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte e Monitoramento e Avaliação). Além desses, define também modelos de maturidade específicos para melhoria de cada um dos trinta e quatro processos que compõem os quatro domínios do arcabouço (*framework*).

Porém, não existem modelos de maturidade definidos para aplicação no combate à fraude, de maneira geral. Neste cenário torna-se importante elaborar um modelo de maturidade para combater a FCI e alertar as empresas da necessidade de conhecerem o seu estágio atual de maturidade nos vários processos que compõe a FCI e com isso, poder estabelecer um processo de melhoria estruturado para os
processos da FCI.

1.2 Objetivo

O objetivo principal desse trabalho é propor um modelo de maturidade de combate à fraude computacional interna (CFCI) que possibilite à organização, de qualquer porte, avaliar o seu nível de maturidade baseado em uma visão de processos e não de controles.

A figura 1 ilustra o objetivo proposto:

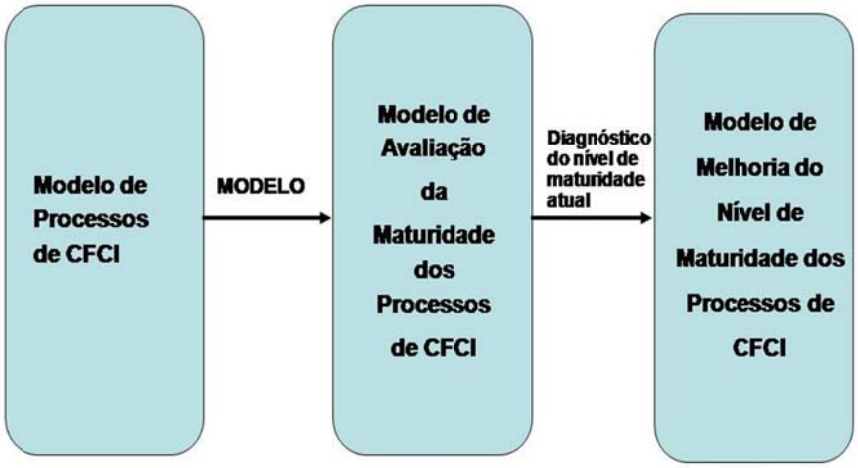

Figura 1 - Modelo de maturidade de CFCI
Fonte: Elaborado pelo autor

1.3 Escopo

O escopo desse trabalho é a proposta de um modelo de maturidade voltado ao combate da fraude computacional interna, estando fora desse escopo as fraudes computacionais externas - realizadas fora das instalações da organização - e as fraudes não computacionais. Também não está incluída no escopo do trabalho a avaliação da proposta, devido à necessidade de aplicação prática do modelo proposto em uma organização, dada a complexidade e extensão do trabalho.

1.4 Método de Trabalho

Tendo em vista o objetivo que se pretende alcançar nessa pesquisa, foram desenvolvidas as seguintes atividades:

a) Estudo dos assuntos relevantes ao trabalho, como fraude, fraude computacional interna (FCI), taxonomia da FCI, processos relacionados ao combate da FCI, modelos de maturidade, agente de ameaça interna e perfil do perpetrador. Referências importantes, Romney e Steinbart (2006), Schultz e Shumway (2002), (ACFE, 2008), (AICPA, 2008), (ISACA, 2007), Vasiu (2004), Carnegie Mellon University (2006), Norma ABNT ISO 15504 (2008), COBIT

(ISACA, 2007), (CMMI, 2007) e MPS.BR (2008) serão estudadas. A finalidade é obter a base para o desenvolvimento e consecução do projeto de pesquisa.

b) Obtenção do conhecimento dos modelos de maturidade do COBIT 4.1 (modelo de maturidade que mede a capacidade dos 34 processos de TI nos quatro domínios do arcabouço), do CMMI (modelo de maturidade para avaliação de processos do ciclo de vida de desenvolvimento de software) CMMI (2007), do MPS.BR (modelo de maturidade que objetiva a melhoria de processo do desenvolvimento do software brasileiro) e da Norma ABNT ISO 15504 (ABNT 2008).

c) Desenvolvimento do modelo de definição dos processos de combate à FCI, por meio da elaboração de um modelo segmentado em domínios e processos, pela definição dos processos e resultados esperados dos processos.

d) Desenvolvimento do modelo de avaliação da maturidade dos processos de combate à fraude computacional interna, por meio da definição do nível de maturidade de combate à fraude computacional interna, através de seus componentes medida dos resultados esperados do propósito do processo e da medida da capacidade dos processos de combate à FCI.

e) Definição do modelo de melhoria da maturidade dos processos de combate à FCI, com a escolha dos domínios e processos para melhoria, a determinação do nível de maturidade desejado para os domínios e processos e a preparação e implementação de um plano de ação.

1.5 Organização do Trabalho

O trabalho está organizado em oito capítulos assim descritos:

O capítulo 2, conceituação, apresenta os principais conceitos e definições que nortearão o trabalho de pesquisa e servirão de base para o seu desenvolvimento.

O capítulo 3, modelos de maturidade, apresenta a ISO 15504, CMMI, MPS.BR e o COBIT 4.1.

O capitulo 4, a proposta do modelo de processos de CFCI, apresentando o propósito (para todos os processos) e os resultados esperados do processo (para quatro deles).

O capitulo 5, a proposta do modelo de avaliação da maturidade dos processos de CFCI, com a estrutura de medição do nível de maturidade de combate à fraude computacional interna e seus componentes.

O capítulo 6, a proposta do modelo de melhoria da maturidade dos processos de CFCI.

O capítulo 7, conclusão, apresenta o resumo dos principais resultados obtidos e a conclusão dos trabalhos, mencionando também a contribuição fornecida pelo projeto de pesquisa ao conhecimento da área e podendo constar sugestões para planos futuros à continuação do trabalho.

Por fim, o capítulo 8, referências, é apresentado a relação dos livros, artigos, pesquisas envolvendo o tema e que foi objeto de estudo para o desenvolvimento do projeto de pesquisa.

7 CONCLUSÃO

Foram algumas motivações que fortaleceram a ideia para o desenvolvimento desse trabalho. A primeira delas é o problema crescente nas organizações das fraudes utilizando sistemas computacionais; os números das pesquisas são contundentes.

A segunda motivação foi a falta de um modelo que não se interessasse apenas pela implementação de controles para combater a fraude computacional interna, mas sim, elevar a atuação pela definição de processos que tratem do tema.

O objetivo do trabalho é a melhoria do combate à fraude computacional interna (CFCI) das organizações através do uso de um modelo de maturidade de CFCI que possibilite à organização, de qualquer porte, avaliar o nível de maturidade de seus processos de CFCI.

Os processos de CFCI foram classificados em cinco domínios a seguir definidos:

- Prevenção (P): é um conjunto de processos que agem de maneira pró-ativa contra a FCI, incluindo as atividades relacionadas à aplicação de controles preventivos com o objetivo de minimizar a ocorrência de fraude.
- Detecção (D): é um conjunto de processos que atuam de forma a detectar uma FCI, nas ocasiões em que os processos preventivos falharem ou para quando os riscos que não foram mitigados ocorrerem.
- Resposta (R): é um conjunto de processos relacionados à contenção, erradicação, recuperação e acompanhamento da fraude computacional interna na organização.
- Investigação (I): é o conjunto de processos relacionados ao esclarecimento do fato (fraude), à determinação da autoria, à determinação da motivação e identificação dos prejuízos.

- Qualidade (Q): é um único processo que tem como finalidade monitorar a qualidade dos outros processos do modelo, por meio de indicadores definidos.

O modelo de maturidade de combate a fraude computacional interna (CFCI), objetivo do trabalho, envolve a composição de três modelos: um modelo de processos de CFCI, um modelo de avaliação da maturidade dos processos de CFCI e um modelo de melhoria do nível de maturidade dos processos de CFCI.

O primeiro dos modelos, o modelo de processos de CFCI tem a finalidade de auxiliar as organizações na prevenção, detecção, investigação e resposta dos processos de combate a fraude computacional interna; o domínio de Qualidade monitora a qualidade dos outros processos do modelo.
Os processos identificados são classificados de acordo com sua atuação e catalogados em um dos cinco domínios. Alguns deles, por seu propósito e característica, estão catalogados em dois domínios, podendo em dado momento atuar em um ou outro domínio.
Neste modelo, além da definição do propósito e atividades que devem compor o processo, em quatro deles foram especificados os resultados esperados do processo.

O modelo de avaliação da maturidade dos processos de combate à fraude computacional interna tem a finalidade de avaliar o nível de maturidade em que se encontra determinado processo ou todos os processos de CFCI.

Esse nível de maturidade de combate à fraude computacional interna (NMcfci) é obtido pela determinação independente de outras duas métricas: a medida de atendimento dos resultados do processo e da capacidade do processo, que tem dois componentes: uma estrutura de medição para a avaliação dos resultados esperados e outra estrutura para a medição para a avaliação da capacidade do processo.

A estrutura de medição dos resultados esperados a partir da definição do propósito do processo tem seis níveis e é baseada nos resultados esperados que o processo alcance, obtendo os produtos esperados para o atingimento do propósito do processo.

Os seis níveis definidos (0-5), com a respectiva definição dos resultados para cada um dos níveis, elencam o que se chama de Medida dos Resultados Esperados para o Propósito do Processo (Mrp).

A estrutura de medição para a avaliação da capacidade do processo tem a finalidade de verificar se a capacidade do processo está presente em uma estrutura bem sucedida do processo. A *capacidade do processo* é definida em uma escala ordinal de seis níveis.

A medição da capacidade de processos foi adaptada da ABNT ISO 15504 e é baseada no conceito de processos tendo atributos comuns. Estes atributos de processo (AP) foram definidos e alocados a níveis de capacidade. Cada um dos atributos de processo define um aspecto particular da capacidade do processo. Em cada um dos níveis definidos, excetuando o nível 0 – Incompleto, existem AP que auxiliam na medição da capacidade do processo.

Os seis níveis definidos (0-5), com a respectiva definição de cada um dos níveis baseados na capacidade do processo e os atributos para cada uma das capacidades, elencam o que chamaremos de Medida da Capacidade dos Processos de Combate à Fraude Computacional Interna (Mcp).

O modelo de melhoria da maturidade dos processos de combate à fraude computacional interna tem a finalidade de propor melhorias para elevar o nível de maturidade do(s) processo(s) avaliado pelo modelo de avaliação.

O modelo foi dividido em sete etapas:

Etapa 1: Escolha das áreas da organização e do(s) processo(s) e/ou domínios para melhoria;

Etapa 2: Avaliação do Nível de Maturidade de Combate à Fraude Computacional Interna;

Etapa 3: Determinação do nível de maturidade desejado para o(s) processo(s) e/ou domínio(s) escolhido(s);

Etapa 4: Análise da diferença entre os níveis de maturidade atual e desejado

Etapa 5: Preparação de um Plano de Ação para alavancagem dos níveis de maturidade

Etapa 6: Implementação do Plano de Ação

Etapa 7: Avaliação dos resultados.

O trabalho teve como partes relevantes a serem destacadas:

a) a contextualização do combate à fraude computacional interna por meio da proposta de um modelo que contemple domínios e processos;
b) a seleção de alguns processos relacionados ao CFCI;
c) o detalhamento de cada um dos processos propostos, contemplando propósitos, atividades e resultados esperados (para quatro deles) que os processos precisem ter;
d) a proposição de um modelo de maturidade que destaca além do nível de capacidade do processo, como CMMI, MPS.BR, o nível de maturidade dos resultados que são esperados dos processos;
e) a proposta de um modelo de melhoria de processos.

Como resumo dos resultados alcançados pelo trabalho destaca-se:

a.) a definição de um modelo de processos, que foi instanciada com cinco domínios e quinze processos de combate à fraude computacional interna;
b.) a proposição de um modelo de avaliação da maturidade de combate à fraude computacional interna, com a estrutura de medição e pontuação de duas medidas: a medida dos resultados esperados do processo (Mrp) e a medida da capacidade do processo (Mcp);

c.) a proposição de um modelo de melhoria do nível de maturidade dos processos de combate à fraude computacional interna em seis etapas, com o objetivo de alavancar o nível de maturidade de CFCI pelo planejamento e implementação de um Plano de Ação.

Foram identificados trabalhos futuros de mestrado ou doutorado. São eles:

a.) No capítulo 4, que trata da proposta do modelo de definição dos processos de combate à fraude computacional interna, pode ser estudada a necessidade de se ampliar o número de processos totais e os processos por cada domínio, além dos resultados esperados dos processos;
b.) No capítulo 5, proposta do modelo de avaliação da maturidade dos processos de combate à fraude computacional interna, pode ser estudada outra proposta que não seja pela combinação de duas medidas (Mrp e Mcp);
c.) No capítulo 6, a proposta do modelo de melhoria do nível de maturidade dos processos de combate à fraude computacional interna, pode ser estudada outra proposta que não tenha como componente principal a determinação de um nível de maturidade alvo a ser atingido.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, ABNT ISO/IEC 15504:2008 – Tecnologia da Informação – Avaliação de Processo – Parte 1-3, Brasil: ABNT, 2008, 89p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, ABNT ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança –Sistemas de Gestão de Segurança da Informação – Requisitos, Brasil: ABNT, 2006, 34p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, ABNT ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão de Segurança da Informação, Brasil: ABNT, 2005, 120p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, ABNT ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação, Brasil: ABNT, 2008, 55p.

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS. ACFE **Report to the Nation on Occupational Fraud&Abuse**. EUA: ACFE, 2006, 64p.

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS (AICPA). **Managing the business risk of fraud: a pratical guide**. EUA: AICPA, 2008, 79p.

CARNEGIE MELLON UNIVERSITY – CyLab. **Common Sense Guide to Prevention and Detection of Insider Threats**. Estados Unidos: 2006, 43p. (Cylab Guideline, 2a. edição, versão 2.1)

COLE, E.; RING, S. **Insider Threat: protecting the enterprise from sabotage, spying, and theft**. Estados Unidos: Syngress Publishing, 2006. 397 p.

Information Technology Technical Committee (ISO/IEC JTC 1). **ISO/IEC 27.005:2008 – Information Technology – Information Security Risk Management**. Suiça: ISO, 2008.

CRESSEY, D. **Other People´s Money**. Estados Unidos: Patterson Smith, 1973.

280 p

DAY, Kevin. **Inside the security mind**. Estados Unidos: Prentice Hall, 2003. 309 p.

DEMING, Edwards W. Qualidade: uma revolução na administração. Brasil: Editora Pioneira, 1995. 350 p.

INFORMATION SYSTEM AUDIT CONTROL ASSOCIATION (ISACA), COBIT, 2007. 195 p.

KENNETH, C., BRANCIK, **Insider Computer Fraud**. Estados Unidos: Auerbach Publications, 2008. 470 p.

KPMG. “A Fraude no Brasil – Relatório de Pesquisa 2004”. Disponível em http://www.kpmg.com.br/publicacoes/forensic/Fraudes2004site.pdf. 2005, 28p.

LANDOLL, D. J. The Security Risk Assessment Handbook. Estados Unidos: Auerbach Publications, 2006. 473 p.

MELHORIA DO PROCESSO DO SOFTWARE BRASILEIRO (MPS.BR). Disponível em http://www.softex.br/mpsbr/_guias/MPS.BR_GUIA_Geral_V1.2.pdf. 2008, 52p.

PELTIER, Thomas R. Information Security Risk Analysis. Estados Unidos: Auerbach Publications, 2005. 281 p.

PORTER, David. **Insider Fraud: Spotting the Wolf Sheep´s cloting**. New York, Computer Fraud & Security Magazine, p. 12-15, abril 2006.

PRICEWATERHOUSECOOPERS. **Information Security a Strategic Guide for Business**. Estados Unidos: PricewaterhouseCoopers Global Technology Centre, 2003. 288 p.

ROMNEY, Marshall B.; Teinbart, Paul J. **Accounting Information Systems**. Estados Unidos: Prentice Hall, 2006. 552 p.

SCHULTZ, E. E.; SHUMWAY, R. **Incidente Response: a strategic guide to handling system and network security breaches**. Estados Unidos: New Riders, 2002. 384 p.

SOFTWARE ENGINEERING INSTITUTE (SEI). CMMI. Disponível em http://www.sei.cmu.edu/pub/documents/07reports/07tr017.pdf. 2007, 441p

STEVENSON, Gordon. **Computer Fraud: Detection and Prevention**. New York, Computer Fraud & Security Magazine, p. 13-15, out 2005.

U.S. Computer Fraud and Abuse Act § 1030, Departamento de Justiça dos EUA, 1996.

VASIU, Lucian; VASIU, Ioana. **Dissecting Computer Fraud: from definitional issues to a taxonomy**. Estados Unidos, IEEE, vol XI, número 4, 2004, 8p.

WELLS, T. Joseph. Corporate Fraud Handbook: prevention and detection. New Jersey:John Wiley, 2004. 280p.

WILDING, Edward. **Information Risk and Security: preventing and investigating workplace computer crime**. Inglaterra: Gower Publishing Limited, 2006. 341 p.