# Utilizando o *Rational Unified Process* para atender a Lei *Sarbanes-Oxley*

**Orlando Ovigli[1], Arthur Gomes[1], Patrícia Kimie[1], Márcia Ito[1,2]**

[1]Gestão e Engenharia de Processos para desenvolvimento de Software – Faculdade de Informática e Administração Paulista (FIAP) – São Paulo, SP – Brasil

[2] Programa de Mestrado – Centro Estadual de Educação Tecnólogica "Paula Souza" (CEETEPS) – São Paulo - Brasil

orlandom@brq.com, agcn84@gmail.com, patrícia_kimie@yahoo.com.br, ito@mind-tech.com.br

***Resumo.*** *O artigo apresenta a proposta de um mapeamento de processo de desenvolvimento de software para atender as exigências da lei "Sarbanes-Oxley" e relaciona as exigências da lei com o processo de desenvolvimento de software "Rational Unified Process". Foi utilizado o CobIT® como diretriz para este mapeamento, que ressalta a necessidade das organizações amadurecerem o gerenciamento dos seus controles internos para fornecer maior transparência das informações e integridade financeira.*

***Abstract.*** *This article proposes a conceptual map of the software development process, "Rational Unified Process", to be compliant with the "Sarbanes Oxley" legal requirements. The map was driven by CobIT® framework which states that management shall improve the internal controls to ensure information transparency and financial integrity.*

## 1. Introdução

Com o avanço da Governança Corporativa e após a falência de empresas conceituadas por motivos de fraude na contabilidade, o governo norte americano decretou a lei *Sarbanes-Oxley* (SOX). Ela é uma lei que obriga todas as empresas de capital aberto a publicarem seus relatórios financeiros para garantir que os processos que dão suporte aos demonstrativos financeiros da empresa possuam controles internos adequados. O controle interno é um processo, desenvolvido para garantir que sejam atingidos os objetivos da empresa. Ele é executado pela Diretoria, pelo Conselho de Administração ou por outras pessoas da companhia que impulsionam o sucesso dos negócios em três categorias: Eficácia e Eficiência das Operações, Confiabilidade dos Relatórios Financeiros e Cumprimento de Leis e Regulamentos Aplicáveis. [ 10 ] [ 4 ]

Uma das ferramentas mais utilizadas para auxiliar o gerenciamento e controle das iniciativas de TI nas empresas é o *Control Objectives for Information and related Technology* (CobIT®). Ele é um guia para a gestão de TI recomendado pelo *Information Systems Audit and Control Association* (ISACA) que contém recursos como mapas de auditoria, ferramentas para a sua implementação e principalmente, um guia com técnicas de gerenciamento [ 2 ].

Na área de TI, os sucessivos fracassos observados nos projetos de software ao longo das últimas décadas [ 1 ], levaram grande parte das organizações a adotarem uma abordagem mais disciplinada para o desenvolvimento do software. O *Rational Unified Process* (RUP) é um processo de engenharia de software que oferece uma abordagem baseada em disciplinas para atribuir tarefas e responsabilidades dentro de uma organização de desenvolvimento, buscando garantir a produção de software de alta qualidade que atenda às necessidades de negócio dentro dos prazos e custos estimados.Por ser um processo de engenharia de software, o RUP é uma tecnologia em camadas, onde a camada do "Processo" é sustentada pelas camadas de "Métodos" e "Ferramentas", podendo ser adaptado para atender as necessidades de cada organização focando na qualidade dos produtos produzidos, tornando-se um instrumento útil para a aplicação de controles e técnicas de gerenciamento. [ 7 ] [ 6 ]

O objetivo deste artigo é relacionar o processo de desenvolvimento de software com a conformidade da lei SOX. Para isso, são utilizados os objetivos de controle do CobIT® como estratégia de governança de TI e o RUP como processo de desenvolvimento de software. O artigo está dividido em três partes principais: Embasamento teórico (Capítulo 2), Mapeamento (Capítulo 3) e Conclusão (Capítulo 4).

## 2. A SOX e a TI

A SOX exige que as organizações evoluam seus processos de negócio a fim de atingir uma maturidade que prevê a integridade financeira e a transparência das informações. Desta forma, para a área de TI a SOX contém duas seções diretamente relacionadas que são: a 302 – Responsabilidades Corporativas para Relatórios Financeiros e a 404 – Gerenciamento de Controles Internos. Apesar da lei não mencionar a área de TI, muitos dos problemas encontrados nas organizações estão relacionados a ela, como as acusações de manipulação de dados, a modificação de programas e a inobservância das políticas de controle para construir relatórios financeiros [ 8 ].

O aspecto chave para o atendimento das exigências da lei SOX é a transparência das atividades de negócio. Por isso, em 2004 foram definidos controles mínimos para duas áreas de TI: Gerência de Mudanças de Aplicações e Segurança de Dados e Aplicações [ 5 ].

É nesse momento que nota-se a importância de ter transparência no desenvolvimento de software e para atingir uma efetiva Gerência de Mudanças e até mesmo Segurança de Dados e Aplicações, é fundamental um processo de desenvolvimento robusto capaz de auxiliar na governança de TI com foco na gerência dos controles internos da organização.

O CobIT®, por sua vez, é um dos métodos adotados para a governança de TI Ele é um conjunto de objetivos de controle que envolvem o Gerenciamento Executivo, os Processos de Negócio e os Serviços de TI. O Gerenciamento Executivo estabiliza e incorpora a estratégia dentro das atividades de negócio. Os Processos de Negócio são os mecanismos da organização para criar e distribuir valores aos envolvidos e os Serviços de TI formalizam as operações e são fornecidos através da organização [ 3 ].

Na perspectiva da SOX, os controles de cada um dos elementos do CobIT® devem ser estabilizados para assegurar que as mudanças de *software* não tenham

impacto na integridade dos dados financeiros. Para isso é necessário que qualquer esforço para o desenvolvimento de software seja realmente justificado, tendo como um dos critérios as reais necessidades do negócio. Desta forma tem-se que um processo de desenvolvimento de software, é essencial para garantir a eficácia dos controles internos da organização e portanto, fazendo-a estar em conformidade com a lei SOX.

## 3. O RUP e a Lei SOX

Dentre as disciplinas do RUP que podem auxiliar a empresa a atender a lei SOX, destacam-se a Gerência de Configuração e Mudança (GCM) e a Gerência de Projetos (GP). A GCM realiza o controle dos diversos produtos gerados durante o desenvolvimento do projeto, a fim de garantir a qualidade desses produtos, além de ajudar na identificação da configuração de um sistema em diferentes pontos no tempo com a finalidade de controlar sistematicamente as mudanças realizadas, mantendo a integridade e rastreabilidade da configuração através do ciclo de vida do sistema. Por sua vez, a GP gerencia riscos e supera obstáculos para liberar com êxito um produto que atenda às necessidades dos clientes e dos usuários. [ 7 ] Estes fatores demonstram que estas disciplinas ajudam a controlar os processos internos da área de TI o qual é uma das exigências da lei SOX.

Para relacionar o RUP com as exigências da SOX, utilizou-se os objetivos de controle do CobIT® já mapeados para a SOX em ITGI 2006 [ 3 ]. Depois é mapeada a equivalência dos objetivos de controle que atendem a SOX com as disciplinas de GP e GCM do RUP, assim como os artefatos resultantes e que permitem contemplar a lei. Os resultados são apresentados a seguir.

O objetivo de controle "**Adquirir e manter software aplicativo (AI2)**" faz com que as aplicações disponíveis estejam alinhadas aos requisitos de negócio, em tempo e custo razoáveis, além disso recomenda um processo padrão para todas as modificações e separa o desenvolvimento, os testes e as atividades operacionais. [ 2 ]. Para evitar que as funcionalidades dos sistemas desenvolvidos não atendam as necessidades de negócio e por conseqüência possam interferir na integridade dos dados e na transparência das informações é necessário um entendimento dos envolvidos do projeto com as reais necessidades de negócio. O ponto inicial desse entendimento são as informações que justificam e estabelecem as restrições econômicas do projeto. Essas informações iniciais que servem como base para a tomada de decisão para a aprovação do projeto é feita no artefato "*Business Case*" e é realizada na tarefa "**Desenvolver caso de negócio**" da disciplina GP [ 7 ]. Por outro lado para atingir as expectativas dos usuários e diminuir a quantidade de defeitos da aplicação é necessário um processo de garantia de qualidade responsável pela verificação das metas de qualidades estabelecidas. Na tarefa "**Desenvolver Plano de Garantia de Qualidade**" da disciplina GP elabora-se o "Plano de Garantia da Qualidade" que apresenta os critérios de garantia para a qualidade do produto, do artefato e do processo [ 7 ]. Ao elaborar o plano pode-se garantir a qualidade do software final e saber se as expectativas dos envolvidos foram atingidas e se a quantidade de defeitos da aplicação está dentro das metas estabelecidas. Para a aceitação do produto existe a tarefa "**Revisar aceitação do projeto**" da disciplina GP que prevê uma revisão formal entre a equipe do projeto e um representante do cliente. Nessa revisão, o cliente verifica se o produto e a documentação de suporte fornecido pelo projeto atendem aos requisitos e objetivos estabelecidos e documentados no início

do projeto. Cada item para aceitação do produto deve ser verificado e se todos forem atendidos é concluído o registro de revisão com o resultado de aprovação [ 7 ]. Ainda neste objetivo de controle é preciso evitar problemas com as informações da organização e estar apto para a auditoria dos controles de mudanças. No RUP, esta processo é feito na tarefa "**Estabelecer processo de controle de mudanças**" da disciplina GCM o qual define o processo de controle de mudança para cada projeto. No processo de controle de mudança a revisão de cada solicitação de mudança garante que todos os aspectos de impacto sejam analisados e documentados para que a tomada de decisão sobre a solicitação esteja resguardada. Essas revisões são passiveis de auditoria para analisar se o controle de mudanças estabelecido foi realizado. A tarefa "**Revisar solicitações de mudança**" da disciplina GCM faz isto ao determinar se cada solicitação deve ser aceita ou recusada. [ 7 ].

O objetivo de controle "**Definir os processos de TI, sua organização e seus relacionamentos (PO4)**" auxilia na agilidade de resposta para as estratégias de negócio enquanto atende os requisitos de governança e provê pontos de contato competentes e definidos, estabelecendo transparência e flexibilidade para as estruturas organizacionais de TI, definindo uma estrutura de processos de TI com papéis e responsabilidades [ 2 ]. Para atender de forma ágil a exigência da área de negócio no que diz respeito à resposta para as suas estratégias é preciso estabelecer um processo para definir como e quais informações são necessárias e quem são os responsáveis por cada tipo de informação. No processo de desenvolvimento RUP, o papel do Gerente de Projeto é responsável por realizar duas tarefas que auxiliam esse objetivo de controle ao mesmo tempo em que os processos e produtos dessas tarefas podem se encaixar aos requisitos de governança estabelecidos para a organização. Assim, a tarefa "**Definir processos de controle e monitoramento**" da disciplina de GP tem por objetivo definir as informações e os processos que são usados para monitorar e controlar o andamento, a qualidade e os riscos do projeto, além de estabelecer indicadores que retratam o andamento do plano de desenvolvimento de software [ 7 ]. A definição desses indicadores é estabelecida de acordo com o orçamento, os objetivos de qualidade e a programação do projeto e são capturadas pela tarefa "**Desenvolver um plano de métricas**" da disciplina de GP. Essa tarefa define metas de gerenciamento, em termos de qualidade, progresso e melhoria, determinando quais informações precisam ser medidas periodicamente para suportar as metas estabelecidas no início do projeto [ 7 ].

O objetivo de controle "**Instalar e acompanhar soluções e mudanças (AI7)**" garante que problemas graves não aconteçam após a instalação das soluções (novas ou alteradas), testando as soluções para verificar se a finalidade da mesma é atendida por meio de uma metodologia de teste, validando o seu resultado com a gerência de negócio e planejando a liberação com execução de relatórios após a instalação [ 2 ]. A garantia da qualidade das aplicações não depende apenas da execução de testes, mas sim de todo o processo utilizado para definir os planos a serem seguidos que garantem que a solução atenda as reais necessidades do negócio. Da perspectiva gerencial, o RUP possui quatro tarefas que definem e executam planos relacionados à garantia da qualidade dos produtos do projeto. A tarefa "**Desenvolver Plano de Garantia de Qualidade**" da disciplina GP estabelece as metas de qualidade que são utilizadas para elaborar um programa de revisões e auditorias que verifica se o processo do projeto definido é seguido corretamente [ 7 ]. Alterações ocorrem durante todo o projeto e para atender

essa demanda, um processo de configuração do projeto precisa ser definido a fim de garantir a revisão e aprovação dos elementos de uma especificação. Outro processo necessário para essas alterações é controlar e monitorar os impactos causados pelas solicitações de mudança. Na tarefa "**Estabelecer políticas e plano de gerência de configuração**" da disciplina GCM a finalidade principal é monitorar e proteger os ativos do projeto, melhorando a comunicação dos membros da equipe durante todo o ciclo de vida de desenvolvimento do software. A documentação das atividades de configuração e do planejamento, implementação, controle e organização dessas atividades faz parte do artefato "Plano de Gerenciamento de Configuração". Além disso, o processo para controle das mudanças que ocorrem durante um projeto é definido na tarefa "**Estabelecer processo de controle de mudanças**" da disciplina GCM que garante a análise e documentação de todas as solicitações de mudanças [ 7 ]. Por fim, a última tarefa identificada para esse objetivo de controle é "**Revisar critérios de avaliação da iteração**" da disciplina GP. Essa tarefa tem o objetivo de revisar e garantir a qualidade dos produtos gerados por cada iteração do projeto, verificando o resultado dos testes realizados e demonstrando à área de negócio que os objetivos da iteração foram atingidos [ 7 ].

O objetivo de controle "**Gerenciar Mudanças (AI6)**" alinha os requisitos de negócio com a estratégia de negócio reduzindo os defeitos e o retrabalho nas soluções e serviços entregues, controlando a avaliação de impacto, reduzindo erros de especificação incompleta, evitando alterações não autorizadas, gerando uma estrutura para captação, priorização e avaliação das solicitações de mudança [ 2 ]. Para gerenciar as mudanças o primeiro passo é a definição desse processo, que é feita na tarefa "**Estabelecer processo de controle de mudanças**" da disciplina GCM [ 7 ]. Com base no processo de controle de mudanças estabelecido, o RUP contém quatro tarefas básicas que são executadas para que o processo garanta a qualidade do produto e por conseqüência atenda esse objetivo de controle atingindo a conformidade com a lei SOX. A primeira tarefa é "**Enviar solicitação de mudança**" da disciplina GCM. Podendo ser executada por qualquer envolvido no projeto, essa tarefa é a formalização de uma solicitação de mudança, contendo a descrição da mudança que pode ser a solicitação de novos recursos, aprimoramentos, correções, requisitos modificados e outros. Por meio do artefato "**Solicitação de Mudança**" gerado nessa tarefa, todo o histórico de mudanças é mantido, incluindo as mudanças de estado, datas e motivos da mudança, além de serem registradas no Sistema de Rastreamento de Solicitações de Mudança. Um administrador do comitê definido para o processo de controle de mudanças ou o proprietário encarregado de uma solicitação de mudança faz atualizações no formulário para indicar o seu estado atual e quaisquer outras informações relevantes. Essa ação trata-se da tarefa "**Atualizar solicitação de mudança**" da disciplina GCM e garante que os envolvidos do projeto acompanhem o estado de cada solicitação e com base nas informações descritas no formulário possam analisar os impactos da mudança. Para todas as solicitações de mudança com estado de Enviadas, a tarefa "**Revisar solicitação de mudança**" da disciplina GCM prevê uma revisão inicial do conteúdo da solicitação para determinar se a mesma é válida. Se for, é decidido se a mudança está dentro ou fora do escopo dos *releases* atuais, de acordo com a prioridade, a programação, os recursos, o nível de esforço, o risco, a gravidade e os outros critérios relevantes definidos pelo processo de controle de mudanças. Se a solicitação de mudança tiver suspeita de

duplicata ou de ser inválida, a tarefa "**Confirmar duplicata ou recusar solicitação de mudança**" da disciplina GCM tem que confirmar o estado da solicitação como Recusada ou Duplicada e obter mais informações do solicitante, quando necessário. Nessa situação, se o solicitante atualizar a solicitação para confirmar que a mesma não é duplicada nem inválida, o estado da solicitação é reenviada, e é analisada novamente pelo comitê definido para o processo de controle de mudanças [ 7 ]. Quando a solicitação de mudança é Aprovada, o papel do Gerente de Projetos do RUP realiza a tarefa "**Programar e atribuir trabalho**" da disciplina GP para acomodar as mudanças aprovadas para produto e processo, que surgem durante uma iteração, entre os membros da equipe de desenvolvimento a fim de garantir o objetivo daquela iteração [ 7 ].

O objetivo de controle "Gerenciar serviços de terceiros (DS2)" provê serviços terceirizados satisfatórios estabelecendo o relacionamento e a responsabilidade dos dois lados, identificando e mitigando os riscos e monitorando e medindo o desempenho do fornecedor [ 2 ]. A Autoridade para Revisão de Projetos (PRA) é uma entidade organizacional responsável pela supervisão do projeto. É extremamente recomendável pelo RUP que uma pessoa seja nomeada para PRA, a qual terá o auxílio, na supervisão do projeto, de um grupo definido de indivíduos seniores da área técnica e de gerenciamento de negócios da organização do projeto, bem como de representantes do cliente no nível executivo [ 7 ]. Com isso, além das tarefas mencionadas nos objetivos de controle, que também auxiliam no processo de monitoração e medição do desempenho do fornecedor, o RUP possui duas tarefas de responsabilidade do Gerente de Projeto que podem ser aperfeiçoadas para controlar os serviços de terceiros. A tarefa "**Iniciar projeto**" da disciplina GP tem por finalidade escalar a equipe que planeja o projeto e define os critérios para medir o êxito dele. Esta tarefa define o PRA e os critérios de aceitação do projeto [ 7 ]. Durante o andamento do projeto, a tarefa "**Revisão do projeto pela PRA**" da disciplina GP realiza uma reunião de *status* em que o andamento, os problemas e os riscos do projeto são revisados pelo PRA [ 7 ].

O objetivo de controle "**Garantir segurança dos sistemas (DS5)**" mantêm a integridade da informação definindo políticas de segurança, monitorando e avaliando a utilização dessas políticas, entendendo e resolvendo os problemas de vulnerabilidade encontrados e realizando testes de segurança regularmente [ 2 ]. Para isto o RUP tem a tarefa "**Desenvolver plano de garantia de qualidade**" que produz o artefato "**Plano de Garantia de Qualidade**". Esse artefato possui uma seção denominada "**Plano de Revisão e Auditoria**" responsável por especificar a programação, os recursos, os métodos e os procedimentos a serem usados na condução de revisões e auditorias do projeto. Ele descreve os vários tipos de revisões e auditorias a serem executados durante o projeto e identifica todas as agências externas que se espera que aprovem ou regulem os artefatos produzidos pelo projeto [ 7 ]. Nessa seção podemos documentar parte das políticas de segurança exigidas pela lei SOX que devem ser revisadas e auditadas durante o desenvolvimento do projeto.

O objetivo de controle "**Gerenciar configuração (DS9)**" define uma estrutura para monitorar e proteger os ativos do projeto, como o suporte para o desenvolvimento dos produtos do projeto, o estabelecimento de um repositório central para os itens de configuração que melhoram a comunicação entre os membros da equipe e facilitam a integração de seus trabalhos [ 2 ]. No RUP a tarefa "**Definir monitoração e controle de**

**processos**" da disciplina GP define como é monitorado e medido o processo de configuração do projeto, para garantir a sua utilização e benefícios. Com base nessa definição, o Gerente de Projeto realiza a tarefa "**Desenvolver um plano de métricas**" da disciplina GP para determinar os atributos que são medidos periodicamente para suportar as metas de gerenciamento no que diz respeito ao controle de configuração do projeto [ 7 ]. Além disso, a lei SOX aponta a necessidade de controle de configuração, assim, no RUP, a tarefa "**Estabelecer políticas e plano de gerência de configuração**" da disciplina GCM tem como objetivo a identificação da configuração o qual permite localizar e identificar de forma rápida e fácil a versão correta de qualquer artefato de projeto. A tarefa "**Configurar ambiente de Gerência de Configuração**" da disciplina GCM estabelece um ambiente em que o produto possa ser desenvolvido e compilado, alocando recursos de máquinas (servidores e espaço em disco) e instalando as ferramentas de gerenciamento de configuração necessárias. Além disso, essa tarefa cria os repositórios, define a estrutura de diretórios do produto e importa todos os arquivos existentes para formar o ambiente de desenvolvimento. Por outro lado a tarefa "**Criar unidade de implantação**" da disciplina GCM serve para criar uma unidade de implantação que seja suficientemente completa para ser entregue. A partir desse momento, onde unidades de implantação começam a ser criadas, um conceito muito importante da gerência de configuração precisa ser utilizado, que é o *baseline*. Ele é definido pelo IEEE [ 9 ] como sendo "uma especificação ou produto que foi formalmente revisto e aprovado e que serve como base para o desenvolvimento futuro, podendo ser modificado apenas através de procedimentos formais de controle de modificação". Esses *baselines* do projeto são criados e promovidos nas tarefas "**Criar *baselines***" e "**Promover *baselines***" da disciplina GCM e garantem a revisão e documentação de cada versão do projeto. Para garantir que o processo de controle de configuração está sendo seguido no desenvolvimento do projeto e atingindo o objetivo de controle em questão, o RUP possui as tarefas "**Relatar o status da configuração**" e "**Realizar auditorias na configuração**" na disciplina GCM que em resumo, são instrumentos para assegurarem que os controles estabelecidos estão sendo cumpridos, além de auxiliar na medição desses controles [ 7 ].

O objetivo de controle "**Gerenciar serviço de atendimento, problemas e incidentes (DS8, DS10)**" permite o uso efetivo dos sistemas de TI para prever soluções e análises para as consultas, perguntas e problemas dos usuários finais, instalando e operando um serviço de atendimento e monitorando e reportando as tendências. Prevê a satisfação dos usuários finais com os serviços e níveis de serviço oferecidos executando análise das causas raízes dos problemas reportados [ 2 ]. Esse controle é realizado para atender os usuários após a instalação dos produtos, no RUP, isto ocorre na fase de transição do projeto, com a tarefa "**Resolver exceções e problemas**" da disciplina GP. Essa tarefa é a avaliação dos problemas e exceções encontrados durante as atividades de revisão e avaliação do andamento do projeto [ 7 ]. Para auxiliar nesse objetivo de controle, essa tarefa pode avaliar as solicitações, perguntas e problemas relatados durante a fase de transição do projeto, onde os usuários começam a utilizar as aplicações desenvolvidas e entram em contato com a área de suporte.

## 4. Conclusão e Discussão

O presente estudo possibilitou analisar que um processo de engenharia de software, o RUP, auxilia a atender a lei SOX, pois descreve as atribuições e responsabilidades de cada envolvido no desenvolvimento de software prevendo que as reais necessidades de negócio sejam alcançadas no prazo e custo estabelecidos para o projeto. Além disso, possui tarefas de gerenciamento que garantem que o processo de desenvolvimento atendem as seguintes exigências da lei SOX: transparência das informações, integridade dos dados e gerenciamento dos controles internos.

Ao analisar os objetivos de controle do CobIT® mapeados para a lei SOX, conclue-se que duas disciplinas do RUP são as que mais atendem as exigências da lei, a Gerência de Projetos e a Gerência de Configuração e Mudança.

Assim, este trabalho ao utilizar como fundamento teórico os objetivos de controle do CobIT® para mapear as exigências da lei SOX com o RUP, evidencia que a utilização e o aperfeiçoamento do RUP pode contribuir para a aplicação dos controles e técnicas de gerenciamento que atendem as exigências da lei SOX.

A continuidade desse trabalho será a adaptação e a aplicação do mapeamento descrito garantindo a conformidade com a lei SOX, mas visando a agilidade do processo de desenvolvimento "RUP".

## Referências


[ **1** ] CHAOS, The Standish Group (1994) "**The Chaos Report**", EUA, Novembro

[ **2** ] ITGI, Governance Institute (2005) "**CobIT® 4.0**", http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27263, último acesso 28/05/2007, EUA

[ **3** ] ITGI, Governance Institute (2006) "**IT Control Objectives for Sarbanes-Oxley**" , 2 ª Edition Exposure Draft, http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27526, EUA, 30 de Abril

[ 4 ] MAYER, F. Eduardo (2004 a) "**SOX e o impacto em TI**", Brasil – São Paulo

[ **5** ] MAYER, F. Eduardo (2004) "**CobIT®: Um kit de ferramentas para excelência na gestão de TI**", Brasil – São Paulo

[ **6** ] PRESSMAN, Roger S. (2002) "**Engenharia de Software**". 5.ed. Rio de Janeiro: Mc GrawHill, Brasil

[ 7 ] RUP, Rational Software Corporation (2003) "**Rational Unified Process**" v6.0, IBM

[ 8 ] SOX. (2002) "**Sarbanes-Oxley Act**". 107º Congresso dos Estados Unidos da América – 2a. Sessão – 23 de Janeiro

[ 9 ] IEEE Std 610.12-1990. **IEEE Standard Glossary of Software Engineering Terminology**. The Institute of Electrical and Electronics Engineers, Inc.: New York, 10017-2394, EUA. 1990.

[10] FERREIRA, L. Alves (2005) **"Entendendo o COSO"**, http://www.auditoriainterna.com.br/coso.htm, Brasil