**Universidade Federal de Pernambuco**

**CIn - Centro de Informática**

**Graduação em Ciência da Computação**

**Auditoria de Sistemas de Informação e sua inserção nas melhores práticas para a Gestão de TI**

Rubem Salzano Neto

**Trabalho de Graduação**

Recife, 11 de julho de 2012

Universidade Federal de Pernambuco

Centro de Informática

**Auditoria de Sistemas de Informação e sua inserção nas melhores práticas para a Gestão de TI**

Rubem Salzano Neto

Monografia apresentada ao Centro de Informática da Universidade Federal de Pernambuco, como requisito parcial para obtenção do Grau de Bacharel em Ciência da Computação.

Orientador: Ana Carolina Brandão Salgado

Co-Orientador: Décio Fonseca

Recife, 11 de julho de 2012

*“O conhecimento não ocupa espaço”*

**Monteiro Lobato**

Dedico a meus pais, Hermano e Auxiliadora, por seu eterno apoio em minha jornada, ao meu irmão mais novo Rodrigo que está se transformando em um grande homem. Em especial, dedico ao meu avô Rubem Salzano, pela minha grande admiração pessoal e profissional.

**Agradecimentos**

A Deus, por diversas vezes, me dar oportunidades de crescimento profissional e por sempre recompensar meus esforços na medida certa.

A meus pais, Hermano e Auxiliadora, por serem os maiores incentivadores da minha carreira, por serem os que mais acreditam no meu sucesso e por me ensinarem que não se consegue nada sem esforço.

A meu irmão mais novo Rodrigo, que a cada dia me orgulha mais por mostrar que se tornará um grande homem. Agradeço pelo grande aprendizado que tenho em sua companhia, apesar da pouca idade.

Em especial, ao meu avô Rubem Salzano, por admirar o grande profissional e homem que é. Agradeço pelos ricos momentos que passo ao seu lado.

Aos meus tios, Eduardo e Elisa, e as minhas primas, Marcela e Mariana, por saber que sempre poderei contar com eles, apesar da distância.

Aos meus verdadeiros amigos, João Maurício e Carlos Eduardo, pela vida juntos, pelos momentos de descontração, pelo caráter e por serem grandes pessoas.

Aos profissionais do escritório de Recife da PricewaterhouseCoopers, por me mostrarem as qualidades de um profissional de respeito.

Por fim, a todos os profissionais da Universidade Federal de Pernambuco e do Colégio Marista São Luís, que, de alguma forma, contribuíram com meu crescimento profissional.

**Resumo**

O presente estudo aborda um tema constituinte bastante importante dos projetos de auditoria contábil ou auditoria de demonstrações financeiras: a auditoria de sistemas de informação.

Atualmente, os sistemas de informação das empresas vêm suportando dados cada vez mais críticos. Como conseqüência disso, além de sua importância para a gestão estratégica, eles têm sido considerados como ferramentas de alta relevância quando se fala de vulnerabilidade a fraudes. Portanto, os sistemas de informação tem sido alvo constante de trabalhos de auditoria contábil.

Nesse início de segunda década do século XXI, a auditoria de demonstrações financeiras vem adquirindo cada vez mais espaço e importância no mercado financeiro brasileiro e mundial. Seguindo essa tendência, com ambientes tecnológicos cada vez mais complexos nas empresas, a auditoria de sistemas de informação também vem ganhando destaque nesse cenário.

Com isso em mente, o trabalho analisa a inserção da auditoria de sistemas em um dos mais relevantes *frameworks* de melhores práticas para a gestão de TI: o CobiT. Adicionalmente, esse estudo ainda expõe um estudo de caso de uma auditoria de sistemas para uma empresa fictícia. Nesse estudo de caso, são expostos elementos de uma auditoria de sistemas fundamentada nas melhores práticas abordadas e nas normas internacionais.

Com a imersão no estudo apresentado, se perceberá a alto valor agregado da auditoria de sistemas para a área de Tecnologia da Informação de uma empresa. É dever da auditoria alertar gestores sobre riscos de fraudes ou continuidade do negócio que uma organização pode estar correndo sem perceber.

Palavras-chave: Gestão de TI, Auditoria de sistemas, CobiT.

**Abstract**

This study addresses a very important constituent theme of accounting audit projects or audit of financial statements, the audit of information systems.

Nowadays, the information systems of the companies are supporting too much critical data than ever before. As a result of this aspect, in addition of the importance of the information systems for the strategic management of a company, they have been considered as a tool of great importance when we talk about things like vulnerability and fraud. It’s easy to see why information systems has been an constant subject in audit projects.

In this second decade of the century XXI, the audit of financial statements is acquiring more importance than ever before in Brazil and around the world. Following this trend, due to the complex technological environments in the companies, the audit of information systems is obtaining a lot of importance too.

Keeping these aspects in mind, this document analyzes the audit of information systems in one of the most important frameworks of best practices for IT management (CobiT). Additionally, this study also presents a study case of an audit of information systems for a fictional company. In this study case, are exposed elements of an audit of information systems based on best practices addressed before and on international rules.

After the immersion in the study presented, it will be easy to realize the importance of the audit of the information systems for the Information Technology area. It’s an obligation of an information systems auditor to open the eyes of an organization to risks of fraud and business continuity which the company can be handling without a greater perception.

Keywords: IT Management, Audit of information systems, CobiT.

**Sumário**

[**1.** **Introdução** 1](#_Toc327982702)

[**2.** **Auditoria de Demonstrações Financeiras** 2](#_Toc327982703)

[**2.1** **História da Auditoria de Demonstrações Financeiras** 2](#_Toc327982704)

[**2.2** **Definição da Auditoria de Demonstrações Financeiras** 3](#_Toc327982705)

[**2.3** **Motivação para a Contratação de Serviços de Auditoria de Demonstrações Financeiras** 3](#_Toc327982706)

[**2.4** **Órgãos Reguladores da Prática de Auditoria de Demonstrações Financeiras** 4](#_Toc327982707)

[**2.5** **Metodologia da Auditoria de Demonstrações Financeiras e Necessidade da Auditoria de Sistemas** 5](#_Toc327982708)

[**2.6** **Considerações Sobre a Auditoria de Demonstrações Financeiras** 6](#_Toc327982709)

[**3.** **Auditoria de Sistemas de Informação** 7](#_Toc327982710)

[**3.1** **Definição e Objetivos da Auditoria de Sistemas de Informação** 7](#_Toc327982711)

[**3.2** **Dimensões da Auditoria de Sistemas de Informação** 8](#_Toc327982712)

[**3.3** **Segurança da Informação e Auditoria de Sistemas de Informação Aliada à Gestão de TI**  9](#_Toc327982713)

[**3.4** **Considerações Sobre a Auditoria de Sistemas de Informação** 10](#_Toc327982714)

[**4.** **Auditoria de Sistemas de Informação e sua Inserção nas Melhores Práticas** 12](#_Toc327982715)

[**4.1** **Conceitos Básicos do CobiT** 12](#_Toc327982716)

[**4.2** **Estrutura do CobiT** 13](#_Toc327982717)

[**4.3** **Conclusões Gerais Sobre o CobiT e sua Aplicabilidade** 16](#_Toc327982718)

[**4.4** **CobiT e Auditoria de Demonstrações Financeiras** 17](#_Toc327982719)

[**4.5** **Considerações Sobre a Inserção da Auditoria de Sistemas de Informação nas Melhores Práticas** 19](#_Toc327982720)

[**5.** **Estudo de Caso** 20](#_Toc327982721)

[**5.1** **Definição dos Testes Aplicados na Empresa Fictícia** 20](#_Toc327982722)

[**5.2** **Resultados dos Testes Aplicados na Empresa Fictícia** 29](#_Toc327982723)

[**5.3** **Considerações Sobre o Estudo de Caso Apresentado** 40](#_Toc327982724)

[**6** **Conclusão e Trabalhos Futuros** 42](#_Toc327982725)

[**6.2** **Conclusão** 42](#_Toc327982726)

[**6.3** **Trabalhos Futuros** 42](#_Toc327982727)

**Lista de Figuras**

[**Figura 1 - Controles de TI 9**](#_Toc327983328)

[**Figura 2 - Relação entre os Domínos do CobiT 14**](#_Toc327983329)

[**Figura 3 - Organização dos Processos do CobiT 14**](#_Toc327983330)

**Lista de Tabelas**

[**Tabela 1 - Relação dos Processos CobiT com Domínios ISA 18**](file:///D:\My%20Documents\Salzano\Faculdade\TG\Monografia\monografia%20vf%20%2013.docx#_Toc330731437)

[**Tabela 2 - Divisão dos Controles a serem Testados entre os Domínios do ISA 21**](file:///D:\My%20Documents\Salzano\Faculdade\TG\Monografia\monografia%20vf%20%2013.docx#_Toc330731438)

[**Tabela 3 - Análise dos Controles não Efetivos Divididos entre os Domínios do ISA 40**](file:///D:\My%20Documents\Salzano\Faculdade\TG\Monografia\monografia%20vf%20%2013.docx#_Toc330731439)

1. **Introdução**

Desde o marco da revolução industrial ocorrida no século XVIII, com o constante aumento das atividades empresariais, medidas rígidas vêm sendo adotadas com o intuito de se regular o mercado financeiro. Essas medidas têm como causa a grande influência que as atividades empresariais exercem sobre a vida particular das pessoas e sobre a soberania do Estado. Desde o dito acontecimento do século XVIII, vários episódios de fraudes, corrupção e atividades antiéticas que geraram grandes crises comprovaram a necessidade dessas medidas.

Atualmente, em pleno século XXI, a atuação da CVM (Comissão de Valores Mobiliários), no Brasil, dentre outros fatores, fortalece os projetos de auditoria de demonstrações financeiras. Aliado a essa tendência, com ambientes tecnológicos cada vez mais complexos e com sistemas de informação cada vez mais integrados entre as diversas áreas de uma organização, não se pode falar de auditoria contábil sem mencionar o termo tecnologia da informação (TI). Atualmente, os processos das empresas estão cada vez mais restritos aos seus sistemas.

A equipe de auditoria foca bastante seu trabalho nos sistemas da empresa (auditoria de sistemas de informação). Isso porque são neles que estão todos os dados relevantes para a demonstração do resultado da entidade. Qualquer erro durante o ciclo de vida desses dados no sistema impactará diretamente a demonstração do resultado da organização e, conseqüentemente, também impactará o trabalho da auditoria contábil.

Aliado a essa perspectiva, o trabalho que se segue começará introduzindo conhecimentos básicos de auditoria de demonstrações financeiras (como história, definição, importância, órgãos reguladores, estratégias entre outros conceitos) para, em seu terceiro Capítulo, mostrar toda a importância e os aspectos mais importantes da auditoria de sistemas de informação (parte importantíssima da auditoria contábil).

No terceiro Capítulo, esse documento mostrará como uma auditoria de sistemas de informação se encaixa dentro do CobiT, que é um dos mais importantes *frameworks* de melhores práticas para a gestão de TI.

Em seu quinto Capítulo, o trabalho irá expor um estudo de caso de uma auditoria de sistemas de informação fictícia fundamentada nas melhores práticas e nas normas internacionais de auditoria.

Por fim, o trabalho se encerra realizando uma visão geral sobre as conclusões obtidas e propondo temáticas para trabalhos futuros.

1. **Auditoria de Demonstrações Financeiras**

O Capítulo que se segue introduzirá conceitos básicos de auditoria contábil. Esse Capítulo explorará o surgimento do termo auditoria, definirá o conceito de auditoria contábil, discorrerá sobre os diversos motivos de se contratar serviços de auditoria e também falará sobre a regulamentação dessa área.

Por fim, esse Capítulo mostrará a moderna forma de se auditar os demonstrativos financeiros de uma empresa através, dentre outros meios, dos sistemas de informação da organização.

* 1. **História da Auditoria de Demonstrações Financeiras**

Muito se discute nos dias de hoje sobre a real origem da atividade de auditoria contábil.

Alguns estudiosos sentem-se confortáveis em dizer que as primeiras práticas de auditoria estão relacionadas com as primeiras atividades contábeis. Para essas atividades, considera-se que elas tiveram início com a necessidade de se realizar registros de comércio e de se cobrar impostos sobre esses registros. Dessa forma, há indícios de que os primeiros contadores da história seriam os escribas Egípcios, por volta do ano de 2000 antes de Cristo.

No entanto, outros historiadores preferem afirmar que a atividade de auditoria contábil apenas efetivamente começou a ser desempenhada com a criação do cargo de auditor na Inglaterra (berço das atuais grandes empresas de auditoria). Na história, os registros desse fato datam do ano de 1314, porém apenas durante a revolução industrial do fim do século XVIII há registros da criação das primeiras empresas de auditoria com o advindo da legislação britânica.

No Brasil, há registros da fundação de um escritório da extinta empresa de auditoria Arthur Andersen no Rio de Janeiro no ano de 1909 e da ainda atuante firma PriceWaterhouseCoopers no ano de 1915, ambas no Rio de Janeiro. Em contrapartida à chegada dessas empresas estrangeiras ao país, a auditoria só foi efetivamente efetivada no país no ano de 1968 quando o Banco Central aprovou normas e procedimentos criados pelo Instituto dos Auditores Independentes do Brasil – IAIB (atualmente denominado IBRACON – Instituto dos Auditores Independentes do Brasil). Após esse marco na história da auditoria contábil brasileira, esse campo de atuação não parou mais de crescer, principalmente após a instituição da lei das Sociedades por Ações e da criação da CVM (Comissão de Valores Mobiliários) em 1976 [1].

* 1. **Definição da Auditoria de Demonstrações Financeiras**

Define-se que a atividade de auditoria contábil é uma ramificação da Contabilidade que permite ao profissional de auditoria emitir um parecer à administração da empresa ou acionistas sobre a integridade de suas demonstrações financeiras. Para isso, as equipes de auditoria podem realizar testes na empresa na forma de indagação de funcionários, observação de procedimentos, inspeção de documentos ou recálculo de valores.

Ao contrário do que pensam muitas pessoas, a auditoria contábil não é destinada especificadamente a desvendar fraudes ou erros, que no decorrer dos trabalhos podem ou não surgir. Porém, tais fatos podem ser de tamanha grandeza, que estejam interferindo significativamente a posição patrimonial e financeira da empresa em exame. Dessa maneira, esses casos podem ser incluídos no relatório final de auditoria.

No relatório de auditoria, além do chamado balanço patrimonial resultante do trabalho e das demais demonstrações financeiras, outro material que também deve ser incluído é o que se chama de carta de controles internos. Essa carta, que é obrigatória a toda atividade de auditoria contábil, resulta de possíveis deficiências nos controles internos da empresa identificadas durante o trabalho. A carta de controles internos oferece aos acionistas ou administradores da empresa sugestões de melhorias nos processos da entidade, para que o risco de se afetar as demonstrações financeiras com as deficiências identificadas seja mitigado.

Por fim, um relatório de auditoria também deve conter ressalvas do auditor responsável às informações apresentadas no documento. Por exemplo, no relatório deve ser explicitado que as informações apresentadas foram representadas através de informações passadas pelos funcionários da empresa em exame. Dessa forma, o auditor não se responsabiliza por informações passadas falsamente ou por documentos obtidos não fidedignos à realidade da empresa [2].

* 1. **Motivação para a Contratação de Serviços de Auditoria de Demonstrações Financeiras**

São inúmeros os motivos que podem levar uma organização a contratar serviços de auditoria contábil independente.

Primeiramente, para as empresas que negociam suas ações em bolsas de valores (as chamadas de capital aberto e que devem ser inscritas na CVM), é mandatório que essas tenham suas demonstrações financeiras auditadas por auditores independentes devidamente cadastrados na CVM. Vale salientar que a CVM (Comissão de Valores Mobiliários) é uma autarquia vinculada ao Ministério da Fazenda do Brasil e tem poderes para disciplinar, normalizar e fiscalizar a atuação dos diversos integrantes do mercado de valores mobiliários [3].

Em segundo lugar, as chamadas instituições financeiras (bancos, seguradoras, consórcios, corretoras de títulos e valores) também necessitam ter seus balanços contábeis auditados de forma independente. Essa regulamentação se dá devido à forte fiscalização do BC ou BACEN (Banco Central) e da SUSEP (Superintendência de Seguros Privados). O BC é uma autarquia federal integrante do Sistema Financeiro Nacional, sendo vinculado ao Ministério da Fazenda. A SUSEP é uma entidade da Administração Pública Indireta Federal brasileira, com sede no Rio de Janeiro responsável pela autorização, controle e fiscalização dos mercados de seguros [4, 5].

Em terceiro lugar, as empresas que fornecem planos de saúde também devem possuir seus balanços contábeis auditados de acordo com regulamentação da ANS (Agência Nacional de Saúde Suplementar). A ANS é a agência reguladora vinculada ao Ministério da Saúde responsável pelo setor de planos de saúde no Brasil [6].

As sociedades sem fins lucrativos que arrecadam mais do que 2,4 milhões por ano são outro tipo de organização que também devem possuir suas demonstrações contábeis auditadas [7].

Por fim, por trazer maior segurança aos resultados apresentados, muitas são as razões para se contratar serviços de auditoria contábil sem relação com órgãos reguladores. Muitos acionistas que não participam diretamente no processo de administração da empresa muitas vezes solicitam serviços desse tipo (fundos de investimentos na maioria das vezes), muitos bancos solicitam esse tipo de trabalho para liberar empréstimos e financiamentos, e a necessidade de uma auditoria contábil pode surgir através da controladoria de uma empresa para evitar fraudes ou participar de licitações do Governo [8].

* 1. **Órgãos Reguladores da Prática de Auditoria de Demonstrações Financeiras**

Atualmente, não estão claramente definidas em nossa legislação civil, penal, comercial e profissional as responsabilidades legais de um auditor. Considera-se essa profissão como técnica ou como uma simples aplicação do conhecimento contábil. Dessa forma, sanções disciplinares podem ser aplicadas ao profissional pelo CFC (Conselho Federal de Contabilidade).

As atividades de escritórios de auditoria independente são regidas pela NBC (Norma Brasileira de Contabilidade), em seção específica que trata de auditoria independente. Essas normas, por sua vez, são baseadas nas normas internacionais de auditoria: ISA (International Standards on Auditing). A seção que trata de auditoria independente da NBC é uma ação conjunta do CFC, da CVM, do IBRACON e do Banco Central. A ISA é produto do trabalho do Comitê de Auditoria Internacional (International Auditing and Assurance Standards Board) da Federação Internacional dos Contadores (International Federation of Accountants) [9].

* 1. **Metodologia da Auditoria de Demonstrações Financeiras e Necessidade da Auditoria de Sistemas**

Muito se fala no ramo da auditoria contábil do termo *Big Four.* Essa expressão se refere às quatro maiores empresas de auditoria contábil do mundo: PriceWaterhouseCoopers, Deloitte Touche Tohmatsu, KPMG e Ernst & Young. Essas corporações possuem alcance global e praticamente dominam todo o mercado de auditoria independente. Quase metade dos investidores de empresas dizem que chegariam a deixar de investir ou, ao menos, repensar o investimento em uma empresa, caso ela contratasse um escritório de auditoria não pertencente ao grupo denominado de *Big Four.*

Devido ao alcance global dessas firmas e à tendência de convergência das normas de contabilidade ao redor do mundo ao padrão global de demonstrações de resultados IFRS (International Financial Reporting Standards), esse grupo de empresas prefere possuir metodologias de auditorias próprias e baseadas no ISA. Portanto, ao aceitar um trabalho de auditoria independente, pode-se perceber que essas empresas não atuam integralmente conforme normas brasileiras, mas conforme normas internacionais (onde as normas brasileiras se baseiam).

Segundo a seção 315 do ISA (*Understanding the entity and its environment and assessing the risks of material misstatement*), nas estratégias de auditoria, pode-se, algumas vezes, se economizar trabalho confiando-se em controles internos. Nessa seção, quando se fala genericamente em economizar trabalho confiando-se em controles internos, fala-se em não praticar testes substantivos (inspeção de notas fiscais, verificação de assinaturas, contagem de itens entre outras atividades) devido à confiabilidade do ambiente de processos da empresa. Portanto, para a estratégia da auditoria e para a redução de pagamento de honorários das empresas, é muito bom que a área de TI da entidade seja bem estruturada [10].

Pode-se falar que os controles de TI são os mais importantes dentro da estrutura de controles internos de uma organização, porque esses controles são ditos como pervasivos. Ou seja, estando uma organização toda fundamentada em seu sistema, qualquer falta de atenção pode ocasionar grandes danos para todas as áreas da empresa. São nos sistemas de informação de uma empresa que estão todos os dados relevantes para a demonstração do resultado da entidade. Qualquer erro durante o ciclo de vida desses dados no sistema impactará diretamente a demonstração do resultado da organização e, conseqüentemente, também impactará o trabalho da auditoria contábil [11].

Em conseqüência da relevância dos controles de tecnologia da informação das empresas, há não muito tempo atrás, resolveu-se implementar no ISA seções específicas do que se chama de auditoria de sistemas de informação.

* 1. **Considerações Sobre a Auditoria de Demonstrações Financeiras**

Sem dúvida alguma, a prática de auditoria de demonstrações financeiras, já há algum tempo, fez com que empresas que vendem esses serviços se tornassem grandes corporações. Essas empresas, atualmente, empregam inúmeras pessoas, ditam tendências de mercado, são primordiais para a economia de qualquer país, geram importantes pesquisas monetárias, concentram um grande número de profissionais formadores de opinião e são necessárias para o crescimento estruturado de qualquer organização.

Mais recentemente, com a constante atualização dessa prática, as empresas de auditoria contábil independente começaram a possuir um corpo de funcionários multidisciplinar. Isso se deve, principalmente, aos vários tipos de trabalhos diferentes que um trabalho de auditoria contábil moderno exige. Dentre esses novos trabalhos, destaca-se o trabalho de auditoria voltado aos sistemas de informação das empresas.

Cientistas e engenheiros da computação desempenham tarefas cada vez mais relevantes dentro de um projeto de auditoria de demonstrações financeiras. Dentre essas tarefas, destaca-se a auditoria de sistemas de informação.

1. **Auditoria de Sistemas de Informação**

O Capítulo que se segue, primeiramente, definirá o termo de auditoria de sistemas de informação no âmbito de parte integrante dos trabalhos de auditoria de demonstrações financeiras. Ela, dessa forma, definirá quais são seus objetivos, explicará sua divisão genérica e fará uma relação dessa atividade com o processo de gestão de uma empresa.

* 1. **Definição e Objetivos da Auditoria de Sistemas de Informação**

O termo auditoria de sistemas de informação, ou simplesmente auditoria de sistemas é muito amplo. O pesquisador Ron Weber define o termo como um processo de recolhimento e avaliação de evidência para determinar se um sistema computadorizado salvaguarda os bens, mantém a integridade dos dados, permite atingir os objetivos da organização de forma eficaz e utiliza os recursos de forma eficiente [12].

Como se pode perceber na definição do termo, não há definição de qual o real objetivo de uma auditoria de sistemas. Da mesma maneira, também não há regras gerais da forma de se conduzir um trabalho desse tipo. Esses dois aspectos (objetivos e metodologia) vão depender de onde partiu a necessidade de se instaurar um processo de auditoria de sistemas.

Um processo de auditoria de sistemas pode ser requisitado por diversos motivos. Primeiramente, esse processo pode ser requisitado como parte dos trabalhos de auditoria contábil ou auditoria de demonstrações financeiras. Um projeto desse tipo também pode acontecer como parte de um trabalho de auditoria de controles internos (auditoria da lei *Sarbanes Oxley* por exemplo). Além disso, uma auditoria de sistemas também pode ser solicitada como uma tentativa de verificar pontos de melhoria nos controles de tecnologia da informação (projeto geralmente realizado pela área de auditoria interna da empresa). Por fim, a própria área de TI pode realizar trabalhos desse tipo com um enfoque maior na segurança dos dados e na eficiência dos recursos [13].

Nesse documento, daremos maior enfoque no tema de auditoria de sistemas de informação como parte dos trabalhos de auditoria contábil.

A seção 315 do ISA não realiza uma definição clara e objetiva do que é um trabalho de auditoria de sistemas dentro de um projeto de auditoria contábil. Essa seção apenas define riscos de inconsistências nas demonstrações financeiras que devem ser observados pela empresa em exame para a equipe de auditoria obter o chamado conforto nos controles de TI (discutido na Seção 2.5 desse documento) [10].

* 1. **Dimensões da Auditoria de Sistemas de Informação**

A seção 315 do ISA divide os riscos de TI para a equipe de auditoria em quatro dimensões: Acesso a programas e dados, Mudanças de programas, Operações computadorizadas e Desenvolvimento de programas.

Para a dimensão de Acesso a programas e dados o ISA define 3 riscos:

* O acesso não autorizado a dados pode resultar em sua destruição ou alteração indevida, incluindo o registro de transações não autorizadas. Quando vários usuários acessam um banco de dados comum, riscos específicos podem surgir;
* A possibilidade de o pessoal de TI ganhar privilégios de acesso além dos necessários para executar suas funções apresenta risco para a auditoria e descaracteriza a segregação de funções;
* Intervenções manuais inadequadas nos processos de TI geram riscos para a auditoria.

Para a dimensão de Mudanças de programas o ISA define 3 riscos:

* Mudanças sem autorização nos “arquivos mestre”;
* Mudanças sem autorização nos sistemas ou programas;
* Falha em fazer mudanças necessárias nos sistemas ou programas.

Para a dimensão de Operações computadorizadas o ISA define apenas um risco:

* Potencial perda dos dados ou impossibilidade de acessá-los.

Para a dimensão de Desenvolvimento de programas o ISA define 2 riscos:

* Mudanças sem autorização em sistemas ou programas;
* Falha em fazer mudanças necessárias nos sistemas ou programas.

Note que os riscos da dimensão de Desenvolvimento de programas estão incluídos nos da dimensão de Mudanças de programas. Dessa forma, mesmo para empresas que não possuem área de desenvolvimento interno, a equipe de auditoria pode confiar, dependendo do caso, nos controle de TI [10].

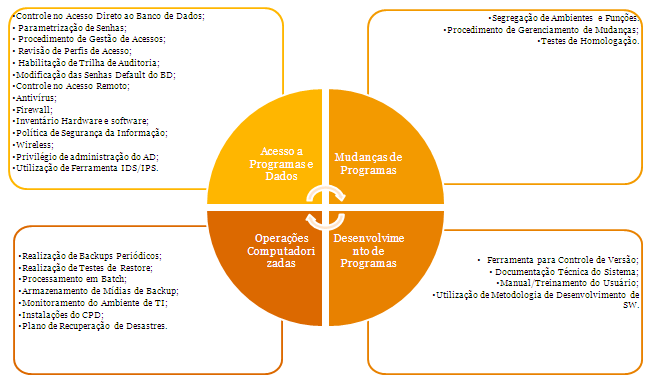
As áreas de tecnologia da informação das empresas costumam já apresentar controles que mitigam alguns dos riscos apresentados. Dessa forma, o objetivo do auditor de sistemas é verificar se esses controles funcionam de forma adequada e se estão em bom número. Os controles de TI mais comuns estão apresentados na Figura 1:

Figura - Controles de TI

Material extraído de SAT\_ITGC\_vFinal2.pptx, de posse da PriceWaterhouseCoopers Auditores Independentes

Mais à frente nesse documento, mais especificamente no Capítulo 5, explicaremos como testar a eficácia de cada um desses controles durante um trabalho de auditoria de sistemas de informação.

* 1. **Segurança da Informação e Auditoria de Sistemas de Informação Aliada à Gestão de TI**

A informação, na visão de Rezende e Abreu (2000), é o dado com uma interpretação lógica ou natural agregada pelo usuário. A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegida (NBR ISSO/IEC 17799, 2003). Como salienta Dias (2000), a informação é o principal patrimônio da empresa e está sob constante risco.

Como se verifica a alta relevância da informação e sabe-se da sua indispensabilidade no processo de gestão de uma empresa, para suportar as decisões, os gerentes de TI modernos, ou CIO’s (*Chief Information Officer*) ou CISO’s (*Chief Information Security Officer*) estão constantemente preocupados com os controles de TI [14].

Para ajudar os gestores a monitorar os controles de TI e para propor melhorias nesses controles existe a auditoria de sistemas. Para nosso caso específico de auditoria de sistemas como parte integrante da auditoria contábil, essa atividade também auxilia os gestores de TI. Isso porque na carta de controles internos que é enviada no relatório de auditoria (para mais informações vide Seção 2.2) estarão todos os pontos identificados pelos auditores de sistemas para serem reportados à administração.

Sem dúvida alguma uma auditoria de sistemas auxilia e muito os gestores de TI a aprimorar os controles da área. Em contrapartida, para isso acontecer, um trabalho desse tipo, para possuir respaldo frente aos gestores da área, deve ser embasado nas melhores práticas de governança de TI. Isso acontece, pois muitas vezes é papel do auditor criticar a forma como os controles estão sendo efetuados e, para isso, o auditor precisa ter conhecimento do que seria o cenário ideal.

Devido à qualidade do trabalho de auditoria de sistemas ser muito atrelada a sua inserção nas melhores práticas, muitas empresas de auditoria possuem suas metodologias (vide Seção 2.5) para a área de TI baseadas em alguns *frameworks*, além do ISA. Como o ISA 315 apenas define riscos para a área de TI (vide Seção 3.2) e não controles, cada empresa de auditoria tem a liberdade de auditar essa área como quiser, desde que seus testes avaliem a cobertura dos riscos mencionados no ISA. Por outro lado, é evidente que a prática de um teste embasado nas melhores práticas mundiais dá muito mais credibilidade aos resultados obtidos.

* 1. **Considerações Sobre a Auditoria de Sistemas de Informação**

Por si só, um trabalho de auditoria de demonstrações financeiras já agrega muito valor para a controladoria, para a contabilidade, para os acionistas e para diversos outros *stakeholders* de uma organização. Além desses usuais beneficiados, dentre os vários tipos de auditoria de sistemas de informação, sem dúvida alguma, uma auditoria de sistemas de informação como parte de um trabalho de auditoria contábil agrega muito valor também para a área de TI de uma organização.

Uma auditoria de sistemas como parte integrante de um trabalho de auditoria contábil, além de reduzir os honorários de um projeto desse tipo, consegue fornecer para a empresa em exame, anualmente, um panorama dos controles de TI da empresa. Como qualquer empresa bem estruturada deseja sempre estar no nível mais alto de padrões de governança, isso é um valor agregado que não pode ser dispensado.

Em trabalhos de auditoria de sistemas desse tipo, costuma-se recomendar para a empresa em exame, em carta de controles internos (vide Seção 2.2) os pontos de melhorias identificados segundo as melhores práticas do mercado. Como empresas de auditoria geralmente possuem um alto grau de conhecimento do que se melhor pratica pelas empresas, entre outras pessoas, gestores de TI devem ficar atentos aos pontos por elas identificados. Esse é um privilégio que os gestores de TI possuem anualmente, toda vez que recebem visitas de auditores de sistemas.

Portanto, pode-se perceber facilmente que a inserção dos trabalhos de auditoria de sistemas nas melhores práticas é fator determinante para, além do respaldo das recomendações reportadas, para a valorização do trabalho da auditoria contábil como um todo e para o crescimento organizacional estruturado das empresas contratantes.

1. **Auditoria de Sistemas de Informação e sua Inserção nas Melhores Práticas**

Como discutido no Capítulo anterior, é muito importante que um auditor de sistemas tenha pleno conhecimento de vários *frameworks* de melhores práticas para realizar boas recomendações em seu trabalho.

Entre vários outros *frameworks* que enriquecem o auditor de sistemas e o possibilita de realizar boas recomendações (PMBoK, ITIL, ISO17799, CMMI entre outros), nesse Capítulo defenderemos o porquê do CobiT ser um dos principais modelos agregadores de valor à base de conhecimentos de um auditor.

O Capítulo que se segue, portanto, irá mostrar a relação entre o *framework* CobiT e as recomendações de possíveis testes de auditoria de sistemas [15].

Para isso, esse Capítulo se inicia introduzindo (conceitos básicos, estrutura, conclusões gerais e aplicabilidade) esse *framework* de alta relevância no atual mercado de TI de forma básica. Após essa etapa inicial, realizaremos então a relação do conteúdo do CobiT com as recomendações de uma auditoria de sistemas.

* 1. **Conceitos Básicos do CobiT**

O CobiT (*Control Objectives for Information and related Technology*) é um modelo para governança e gestão de TI desenvolvido pela ISACA (*Information Systems Audit and Control Association*).

A ISACA, organização que teve sua fundação em 1996, é uma organização líder de profissionais de controle em TI. Ela é uma entidade privada e voluntária que possui mais de 86.000 membros ao redor do mundo e é reconhecida como entidade líder global em governança de TI. A ISACA possui mais de 185 capítulos (sedes) em aproximadamente 75 países. O foco da associação é na área de auditoria de sistemas, controles de TI e questões de segurança da informação.

Com a criação do CobiT (seu principal produto), a ISACA definiu seus objetivos. Em sua criação, ficou acertado que o objetivo do CobiT seria fornecer ao gerenciamento dos processos de negócio, um modelo de governança em TI, desenhado para ajudar no entendimento e gerenciamento dos riscos associados. Também se tornou objetivo do CobiT o fato dele ser orientado ao negócio, ou seja, o fato dele direcionar a governança de TI e seus recursos para as estratégias de negócio.

Atualmente, o CobiT está em sua 5ª edição (lançada no início de 2012) e é dividido em agrupamento de afinidades dos principais processos e atividades de TI. Ele provê boas práticas através de sua estrutura que distribui controles através de uma estrutura lógica e gerenciável [16].

* 1. **Estrutura do CobiT**

O CobiT, em sua recente versão 5, possui, ao todo, 37 processos descritos de acordo com as melhores práticas do mercado de TI. *O framework,* nessa recente versão, começa a separar os seus processos entre atividades de governança de TI e atividades de administração de TI. Dentro dessas duas perspectivas, o CobiT possui os seguintes domínios:

Governança de TI (5 processos pertencentes ao conjunto dos três domínios - EDM):

* Avaliar (*Evaluate*)
* Direcionar (*Direct*)
* Monitorar (*Monitor*)

Administração de TI:

* Alinhar, Planejar e Organizar (13 processos)

(APO – *Align, Plan and Organise*)

* Construir, Adquirir e Implementar (10 processos)

(BAI – *Build, Acquire and Implement*)

* Entregar, Serviço e Suporte (6 processos)

(DSS – *Deliver, Service and Support*)

* Monitorar, Avaliar e Medir (3 processos)

(MEA – *Monitor, Evaluate and Assess*)

Esses domínios interagem entre si de acordo com a relação da figura 2.

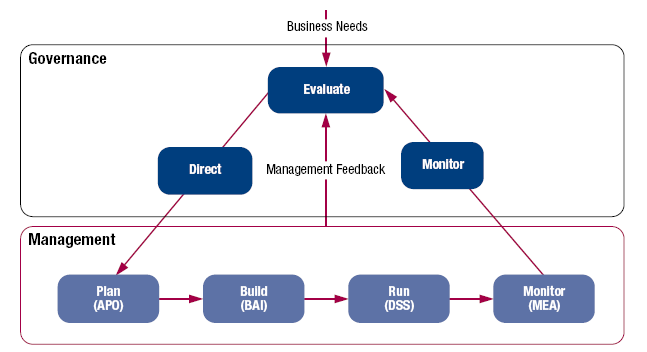


Figura - Relação entre os Domínos do CobiT [15]

A listagem completa dos 37 processos do CobiT, bem como uma melhor visualização de sua organização entre os domínios do *framework,* pode ser visualizada na figura 3:

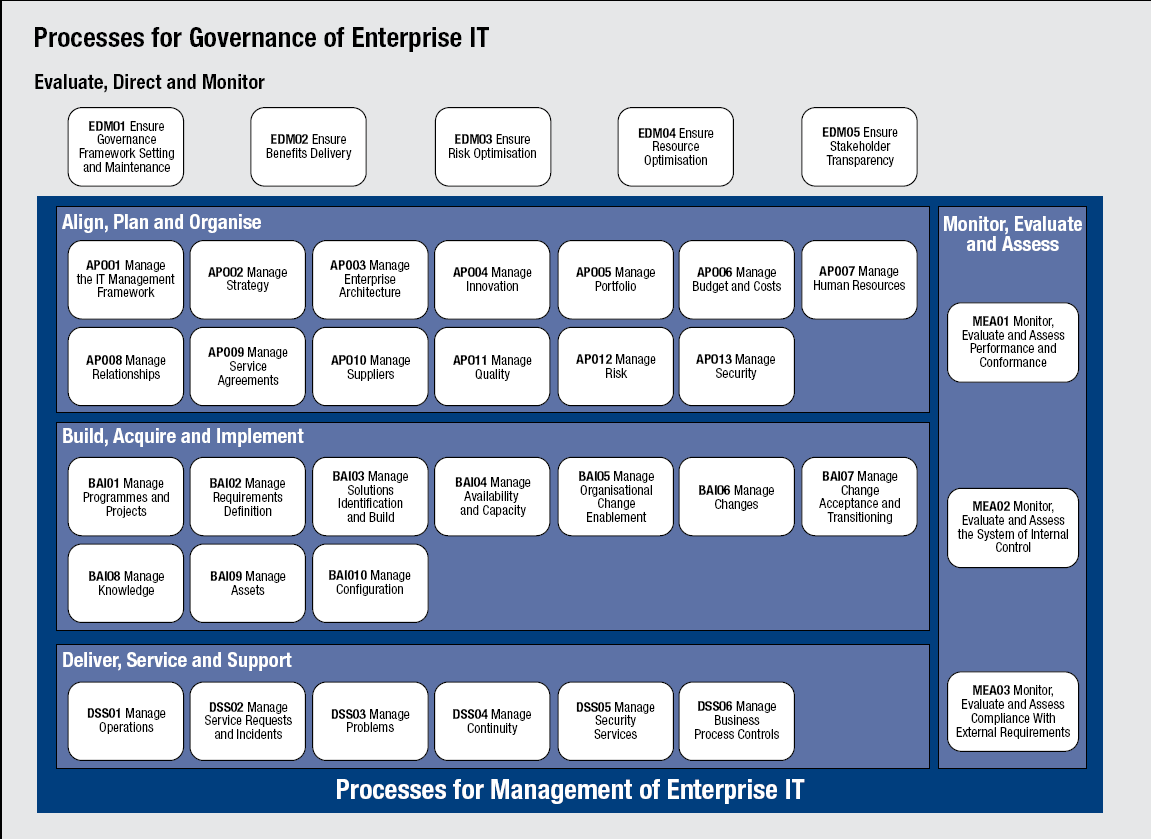


Figura - Organização dos Processos do CobiT [15]

* APO01 – Administrar o *Framework* de Administração de TI (*Manage the IT Management Framework*)
* APO02 – Administrar a Estratégia (*Manage Strategy*)
* APO03 – Administrar a Arquitetura Corporativa (Manage Enterprise Architecture)
* APO04 – Administrar a Inovação (*Manage Innovation*)
* APO05 – Administrar o *Portfólio* (*Manage portfolio*)
* APO06 – Administrar o *Budget* e os Custos (*Manage Budget and Costs*)
* APO07 – Administrar os Recursos Humanos (*Manage Human Resources*)
* APO08 – Administrar as Relações (*Manage Relationships*)
* APO09 – Administrar os Acordos de Serviço (*Manage Service Agreements*)
* APO10 – Administrar os Fornecedores (*Manage Suppliers*)
* APO11 – Administrar a Qualidade (*Manage Quality*)
* APO12 – Administrar os Riscos (*Manage Risk*)
* APO13 – Administrar a Segurança (*Manage Security*)
* BAI01 – Administrar os Programas e os Projetos (*Manage Programmes and Projects*)
* BAI02 – Administrar a Definição de Requisitos (*Manage Requirements Definitions*)
* BAI03 – Administrar a Identificação de Soluções e Construir (*Manage Solutions Identification and Build*)
* BAI04 – Administrar a Disponibilidade e a Capacidade (*Manage Availability and Capacity*)
* BAI05 – Administrar a Capacidade de Realizar Mudanças Organizacionais (*Manage Organisational Change Enablement*)
* BAI06 – Administrar as Mudanças (*Manage Changes*)
* BAI07 – Administrar a Transição e Aceitação de Mudanças (*Manage Change Acceptance and Transitioning*)
* BAI08 – Administrar o Conhecimento (*Manage Knowledge*)
* BAI09 – Administrar os Ativos (*Manage Assets*)
* BAI10 – Administrar as Configurações (*Manage Configuration*)
* DSS01 – Administrar as Operações (*Manage Operations*)
* DSS02 – Administrar a Requisição de Serviços e Incidentes (*Manage Service Requests and Incidents*)
* DSS03 – Administrar os Problemas (*Manage Problems*)
* DSS04 – Administrar a Continuidade (*Manage Continuity*)
* DSS05 – Administrar os Serviços de Segurança (*Manage Security Services*)
* DSS06 – Administrar os Controles de Processo de Negócio (*Manage Business Process Controls*)
* MEA01 – Monitorar, Avaliar e Medir o Desempenho e a Conformidade (*Monitor, Evaluate and Assess Performance and Conformance*)
* MEA02 – Monitorar, Avaliar e Medir o Sistema de Controles Internos (*Monitor, Evaluate and Assess the System of Internal Control*)
* MEA03 – Monitorar, Avaliar e Medir a Observância com Requerimentos Externos (*Monitor, Evaluate and Assess Compliance with External Requirements*)
* EDM01 – Assegurar a Fixação e a Manutenção do Framework de Governança (*Ensure Governance Framework Setting and Maintenance*)
* EDM02 – Assegurar a Entrega dos Benefícios (*Ensure Benefits Delivery*)
* EDM03 – Assegurar a Otimização dos Riscos (*Ensure Risk Optimisation*)
* EDM04 – Assegurar a Otimização dos Recursos (Ensure Resource Optimization)
* EDM05 – Assegurar a Transparência para os *Stakeholders* (*Ensure Stakeholder Transparency*)
  1. **Conclusões Gerais Sobre o CobiT e sua Aplicabilidade**

O CobiT é um produto aplicado para diversos tipos de *stakeholders*. Ele é aplicável para o comitê executivo de uma empresa, para os gestores de negócio, para o gerente de TI, para o gerente de projetos, para os desenvolvedores, para a área de operações, para os usuários da área de TI, para o *Chief Information Security Officer* e para auditores de sistemas.

De todos esses possíveis envolvidos com a aplicação do CobiT, seu principal público-alvo são os gerentes de TI, os usuários da área de TI e os auditores de sistemas.

Os gerentes de TI precisam do *framework* para avaliar as decisões de investimento em TI, para balancear riscos e controles de investimentos em TI que geralmente são imprevisíveis e para fazer comparações com ambientes de TI atuais e futuros.

Os usuários dos sistemas providos pela área de TI de uma empresa precisam do CobiT para obter garantia na segurança e controle de produtos e serviços fornecidos internamente e por terceiros.

Por fim, os auditores de sistemas devem possuir um alto embasamento sobre esse modelo de melhores práticas para substanciar as opiniões para a gerência de controles internos e para conseguir entender quais são os controles mínimos necessários para cada negócio [17].

* 1. **CobiT e Auditoria de Demonstrações Financeiras**

Como discutido anteriormente na Seção 3.2, o ISA define alguns riscos de distorções nas demonstrações financeiras de uma empresa que devem ser cobertos por controles de TI. Ainda naquela mesma Seção, verificamos que existem 28 controles (divididos em 4 domínios) de TI ditos como mais comuns nos ambientes de informática das empresas brasileiras que procuram mitigar o efeito desses riscos.

Como um trabalho de um auditor de sistemas é avaliar a eficácia dos controles de TI e em seu trabalho agrega muito embasá-lo nas melhores práticas, pode-se visualizar na Tabela 1 uma relação entre a auditoria de sistemas e o *framework* de melhores práticas do mercado trabalhado nesse documento. Essa tabela relaciona os processos do CobiT de maior relevância para auditoria de sistemas com os domínios do ISA descritos na Seção 3.2.

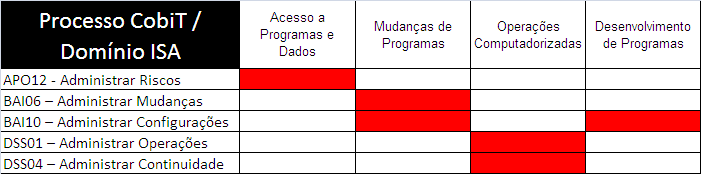


Tabela - Relação dos Processos CobiT com Domínios ISA

Pode-se falar da alta relevância do processo APO12, pois ele discursa sobre os mesmos princípios do domínio de Acesso a Programas e Dados. Esse processo fala sobre a garantia que apenas acessos autorizados sejam concedidos para os recursos de informação. Dessa maneira, pode-se garantir a integridade dos dados.

Da mesma maneira, pode-se falar da alta relevância do processo BAI06, pois ele discursa sobre os mesmos princípios do domínio de Mudanças de Programas. Esse processo, com auxílio de outros, prega que as alterações em programas e componentes de infra-estrutura relacionados sejam solicitadas, autorizadas, executadas, testadas e adequadamente implementadas.

Da tabela, pode-se verificar que o processo BAI10 abrange tanto o domínio de Mudanças de Programas quanto o de Desenvolvimento de Programas. Isso acontece, pois uma boa Gerência de Configuração é imprescindível para um ambiente de Controles de TI estruturado e, dessa forma, deve ser alvo freqüente de auditoria de sistemas.

Pode-se verificar também da tabela, que o domínio de Operações Computadorizadas possui dois processos que caracterizam muito bem sua essência: garantir o adequado funcionamento dos componentes de tecnologia da empresa. Atualmente, nesse domínio, as grandes empresas tem se preocupado bastante com planos de contingência e de recuperação de desastres.

Por fim, Mesmo considerando esses processos aqueles com maior relação com os controles descritos na Seção 3.2, para um auditor de sistemas competente é necessário conhecer todos os processos do CobiT. Isso porque cada processo, mesmo que minimamente, tem alguma coisa a contribuir com um trabalho de auditoria de sistemas. Além disso, existem outros *frameworks* que podem contribuir para o embasamento dos testes de auditoria de sistemas. Restringir o cenário ideal do ambiente tecnológico da empresa em exame a apenas um framework não torna o trabalho suficientemente consistente.

* 1. **Considerações Sobre a Inserção da Auditoria de Sistemas de Informação nas Melhores Práticas**

É muito fácil perceber a grande dimensão de aplicações que o modelo de governança/gestão de TI que o CobiT propõe abrange. Nesse Capítulo vimos mais especificamente que, dentre vários outros conjuntos de melhores práticas citados, o CobiT tem enorme importância para a auditoria de sistemas.

Um auditor de sistemas, em suas recomendações, não consegue se basear em apenas um modelo pré-formatado. Ele muitas vezes, nem necessariamente segue algum modelo, mas sim o bom senso ou sua experiência acumulada em outros trabalhos. No próximo Capítulo, poderá se verificar a tamanha complexidade desse caso.

Por outro lado, conhecer metodologias enriquece muito a base de conhecimentos de um auditor para que ele possa sugerir as mais bem elaboradas melhorias identificadas em seus clientes. Dentre várias metodologias que um auditor deve conhecer, nesse Capítulo defendemos o conhecimento do CobiT, pois consideramos essa a mais importante.

Podemos concluir do Capítulo passado que o um auditor de sistemas necessita de uma boa leitura no CobiT, pois nele há seções que sintetizam quase que inteiramente domínios definidos no ISA 315 (vide Seção 4.4). Acabamos de mostrar que toda a idéia inicial da auditoria de sistemas e sua segurança da informação está contida na essência de alguns processos do CobiT. Dessa forma, conhecer esses bem esses processos e também os demais pode ajudar e muito um auditor de sistemas. Para comprovar isso, basta analisarmos o conteúdo do próximo Capítulo.

1. **Estudo de Caso**

O Capítulo que se segue demonstrará uma formalização real de testes de auditoria de sistemas de informação como suporte para um projeto de auditoria contábil. Essa auditoria de sistemas está, como vimos em capítulos anteriores, fundamentada nas melhores práticas abordadas no mercado.

Serão expostos testes para 19 controles previamente identificados com a adição de uma conclusão geral do trabalho. Primeiramente, na Seção 1, se explicará os métodos utilizados em cada teste para, na Seção 2, expormos o resultado obtido em cada um dos 19 testes aplicados em nossa empresa fictícia.

As formalizações que se seguem, não contemplarão nomes de pessoas ou ferramentas específicas, datas, documentos (evidências) externos, com o intuito de preservar a identidade dos envolvidos.

* 1. **Definição dos Testes Aplicados na Empresa Fictícia**

Como visto na Seção 3.3, o ISA 315 apenas define riscos para a área de TI (vide Seção 3.2) e não controles, cada empresa de auditoria tem a liberdade de auditar essa área como quiser, desde que seus testes avaliem a cobertura dos riscos mencionados no ISA. Dessa forma, foram previamente selecionados para esse trabalho, com uma visão macro do ambiente computacional da empresa fictícia, os 19 controles expostos na Tabela 2. Esses controles foram escolhidos devido a sua relevância dentro do ambiente computacional da empresa em exame e devido a sua cobertura aos riscos descritos no ISA 315.

Na Tabela 2, os controles selecionados para teste, estão divididos em 3 domínios ISA: Acesso a Programas e Dados, Mudanças de Programas e Operações Computadorizadas. Não foram definidos controles a serem testados para o domínio de Desenvolvimento de Programas, pois foi identificado que, nessa empresa fictícia, não há desenvolvimento interno de sistemas aplicativos.

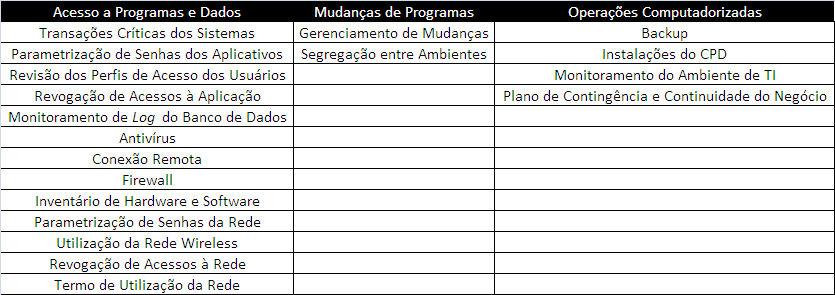


Tabela - Divisão dos Controles a serem Testados entre os Domínios do ISA

O intuito do nosso trabalho é verificar a eficácia de cada um desses 19 controles de TI. Para verificar esse desempenho, como não existem práticas definidas no ISA 315, relacionaremos as estratégias definidas nas próximas 19 Seções.

* + 1. **Transações Críticas dos Sistemas**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, busca detectar a realização de transações críticas de um sistema aplicativo por pessoas não autorizadas. Dessa forma, espera-se que em um ambiente tecnológico complexo, pessoas sejam responsáveis por, periodicamente, verificar se uma série de transações consideradas críticas pela gerência da empresa só estejam sendo desempenhadas pelas pessoas a elas determinadas.

Por exemplo, para uma transação de “aprovação de baixa manual de títulos a pagar”, deve-se verificar, periodicamente, se essa transação só está sendo processada por gestores da área financeira da empresa.

Para testarmos a eficácia desse controle em nossa empresa fictícia, basta indagarmos pessoas responsáveis pelo sistema aplicativo sobre a realização dessa atividade. Nessa indagação, primeiramente temos que verificar se o sistema permite esse monitoramento através do que chamamos de *log* (textos que registram o processamento do sistema). Depois, temos que questionar os responsáveis se esses *logs* são utilizados para o monitoramento (com evidência de sua realização).

* + 1. **Parametrização de Senhas dos Aplicativos**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, busca dificultar, ao máximo, a possibilidade que sistemas sejam acessados por pessoas não autorizadas. Como muitos usuários costumam escolher senhas muito simples, há, nos sistemas modernos, como restringir a complexidade de suas senhas através de alguns parâmetros.

Por exemplo, limitar o tamanho mínimo da senha, fazer com que o usuários sempre estejam mudando suas senhas para novos conjuntos de caracteres, bloquear usuários com tentativas repetidas de acesso sem sucesso e definir a complexidade das senhas (uso de maiúsculas, números e caracteres especiais) são alguns parâmetros de senha que podem ser configurados nos sistemas de informação.

Para testarmos a eficácia de um controle desse tipo, basta verificar a tela de opções do sistema em questão e relacionarmos a política de senhas da empresa.

* + 1. **Revisão dos Perfis de Acesso dos Usuários**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, busca garantir que os acessos dos usuários no sistema de informação utilizado sejam revisados. É bastante claro que usuários de um sistema de informação complexo e integrador de diferentes áreas não devem ter acesso a todas as transações possíveis do sistema.

Por exemplo, não faz sentido que a própria pessoa que realizou uma transação de solicitação de reembolso no sistema a aprove. Devido a concessão de acessos a transações nas empresas ser bastante dinâmica e mutável, recomenda-se como uma boa prática de mercado estar sempre revisando os acessos dos usuários.

Para testarmos a eficácia desse controle basta, em conversa com a área de TI da empresa em exame, entender se existe algum processo periódico desse tipo, obtendo evidências da realização.

* + 1. **Revogação de Acessos à Aplicação**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, busca que não existam no sistema de informação usuários genéricos (usuários utilizados por mais de uma pessoa), usuários desconhecidos da empresa, usuários duplicados e usuários que já foram desligados da empresa.

As melhores práticas do mercado dizem que a existência desses usuários acarreta riscos de processamentos cujos autores não podem ser identificados pela empresa em exame.

Para testarmos a eficácia desse controle, podemos obter uma listagem de funcionários ativos e desligados da empresa em exame e realizarmos uma análise dos usuários do sistema de informação em planilha eletrônica.

* + 1. **Monitoramento de *Log* do Banco de Dados**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, funciona de maneira bastante semelhante e possui os mesmos princípios do controle descrito na Seção 5.1.1. A única diferença entre os dois é que o primeiro funciona no nível da aplicação e esse funciona no nível da base de dados, se considerarmos uma arquitetura de sistemas de informação tradicional.

Como nos sistemas de informação, muitos usuários possuem acesso para editar informações diretamente na base de dados, temos que nos precaver que isso não acontece por pessoas não autorizadas. Por causa disso deve existir um forte monitoramento dessa atividade.

Como no primeiro controle, para testarmos a eficácia desse controle em nossa empresa fictícia, basta indagarmos pessoas responsáveis pelo banco de dados sobre a realização dessa atividade. Nessa indagação, primeiramente temos que verificar se o SGBD (Sistema de Gerenciamento de Banco de Dados) permite esse monitoramento através do que chamamos de *log* (textos que registram o processamento do sistema). Depois, temos que questionar os responsáveis se esses *logs* são utilizados para o monitoramento (com evidência de sua realização).

* + 1. **Antivírus**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, tem como objetivo a proteção do ambiente computacional da empresa em exame. Essa proteção tem tanto como finalidade a continuidade do negócio da empresa quanto à proteção de seus dados críticos.

Dependendo do tipo de negócio desempenhado pela empresa em exame, esse controle deve ser mais ou menos rigoroso. Por exemplo, empresas que guardam dados de clientes devem preservar ao máximo o sigilo de suas informações.

Para testarmos a eficácia desse controles devemos, antes de tudo, identificar se a empresa em questão utiliza alguma ferramenta com amplo respaldo do mercado. Em segundo lugar, devemos identificar se os funcionários utilizam a ferramenta de forma adequada com todas suas possibilidades e a atualizam.

* + 1. **Conexão Remota**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, busca controlar os acessos à rede da empresa por seus funcionários quando eles estão fora de seus domínios físicos. Dessa maneira, uma empresa com alta maturidade em controles não deve liberar esse tipo de acesso a qualquer funcionário. As empresas devem institucionalizar uma gestão de concessão de acessos eficiente para casos como esse.

Para testarmos a eficácia desse controle, precisamos entender, junto aos funcionários da área de TI, como os colaboradores da empresa realizam acesso remoto aos sistemas. Além disso, precisamos entender como ocorre a concessão de novos acessos a essa funcionalidade.

* + 1. **Firewall**

Esse controle, também pertencente ao domínio de Acesso a Programas e Dados, possui objetivos semelhantes ao do controle da Seção 5.1.6. Esse controle busca a proteção do ambiente computacional da empresa através de ferramentas que controlam o tráfego de dados entre o ambiente interno e externo.

Para testarmos a eficácia desse controle, precisamos verificar se a empresa utiliza uma ferramenta de *Firewall* de respaldo do mercado. Além disso, temos que verificar também se essa ferramenta é utilizada de maneira eficaz com, dentre outras finalidades, o bloqueio de sites considerados perigosos para a empresa. Como muitas ferramentas de *Firewall* já vêm acopladas com ferramentas de IDS (*Intrusion Detection System*), nesse teste, verificamos também se a empresa utiliza uma ferramenta desse tipo para prevenir a intrusão da rede interna.

* + 1. **Inventário de Hardware e Software**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, tem dois objetivos principais.

O primeiro é que a empresa controle, de forma estruturada (através de alguma ferramenta do mercado), a quantidade de equipamentos de hardware e licenças de software que possui.

Seu segundo objetivo é que a empresa coíba a instalação de softwares não autorizados por sua administração. Prevenindo, portanto, a instalação de softwares perigosos ao ambiente computacional.

Para testarmos a eficácia desse controle, devemos, primeiramente, entender se a empresa possui alguma ferramenta, mesmo que simplória, que controle seus ativos de TI. Depois disso, podemos tentar realizar a instalação de um programa qualquer em uma máquina aleatória da empresa. Com essa tentativa, identificaremos se a empresa está bloqueando a instalação de *softwares* não autorizados.

* + 1. **Parametrização de Senhas da Rede**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, possui os mesmos princípios do controle da Seção 5.1.2. A diferença entre esses dois controles é que o primeiro funciona no nível da aplicação e esse funciona no nível da rede da empresa.

Da mesma forma que para o controle da Seção 5.1.2, para testarmos a eficácia desse controle, devemos verificar quais parâmetros de complexidade de senha estão configurados para acesso à rede da empresa. Para a grande maioria das empresas, que utilizam sistemas operacionais *Windows*, a gestão da rede da empresa se dá através da ferramenta *Active Directory.*

* + 1. **Utilização da Rede Wireless**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, tem como finalidade garantir que o acesso à rede sem fio da empresa seja adequado. Seu principal ponto de atenção é a garantia de que o acesso à rede sem fio para visitantes seja diferenciado do acesso à rede sem fio para funcionários. Isso garante que arquivos confidenciais não sejam acessados por pessoas não autorizadas, por exemplo.

Para testarmos a eficácia desse controle, devemos entender como está montada a topografia da rede sem fio da empresa. Isso visa a garantir essa segregação entre rede de visitantes e rede de funcionários.

* + 1. **Revogação de Acessos à Rede**

Esse controle, pertencente ao domínio de Acesso a Programas e Dados, busca princípios parecidos ao do controle da Seção 5.1.4. A diferença entre esses dois controles é que o primeiro funciona no nível da aplicação e esse a nível da rede da empresa.

Da mesma forma que para o primeiro controle, este busca que não existam na rede da empresa usuários genéricos (usuários utilizados por mais de uma pessoa), usuários desconhecidos da empresa, usuários duplicados e usuários que já foram desligados da empresa.

Para testarmos a eficácia desse controle, podemos obter uma listagem de funcionários ativos e desligados da empresa em exame e realizarmos uma análise dos usuários da rede em planilha eletrônica.

* + 1. **Termo de Utilização da Rede**

Esse controle, último pertencente ao domínio de Acesso a Programas e Dados, busca que os funcionários da empresa estejam cientes de suas responsabilidades no uso da rede da empresa e seus equipamentos. Para isso, muitas empresas se utilizam de termos que devem ser assinados por seus funcionários.

Para testarmos a eficácia desse controle, podemos conseguir uma lista dos novos funcionários da empresa e selecionarmos aleatoriamente alguns deles. Após essa etapa, basta solicitarmos à área que fica de posse desses documentos os mesmos para verificarmos se eles estão devidamente assinados.

* + 1. **Gerenciamento de Mudanças**

Esse controle, pertencente ao domínio de Mudanças de Programas, tem como objetivo que a empresa em exame possua um adequado procedimento formalizado para o gerenciamento das mudanças realizadas em seu sistema. Além disso, a empresa deve possuir em seu procedimento fases como testes e requisição de usuário. Por fim, não se pode falar em gerenciamento de mudanças sem uma ferramenta de controle de versão adequada.

Para testarmos a eficácia desse controle, primeiramente, devemos entender se a empresa em questão possui um procedimento desse tipo e se ele está formalizado. Após essa etapa, se a empresa possuir uma ferramenta de controle de versão adequada, podemos solicitar evidências da realização das fases descritas para algumas mudanças realizadas.

* + 1. **Segregação entre Ambientes**

Esse controle, pertencente ao domínio de Mudanças de Programas, tem como objetivo a separação entre os ambientes onde as diferentes versões do sistema estão instaladas. É importante que a empresa possua ambientes de desenvolvimento, de teste e de produção. Além disso, as boas práticas dizem que não deve ser de responsabilidade dos desenvolvedores a migração da mudança para o ambiente de desenvolvimento.

Para testarmos a eficácia desse controle, deve-se procurar entender como está a disposição das diferentes versões do sistema nos servidores. Além disso, devemos entender também como ocorre a migração das mudanças desenvolvidas para o ambiente de produção. Nessa última etapa, deve-se atentar se a ferramenta utilizada para essa finalidade é amplamente utilizada no mercado.

* + 1. **Backup**

Esse controle, pertencente ao domínio de Operações Computadorizadas, tem como objetivo garantir que a empresa possa salvaguarda de seus dados no caso de problemas que visem à continuidade de seus negócios. Para isso, quase todas as empresas possuem algum procedimento de armazenamento externo de seus dados, o que se chama popularmente de *backup*.

As empresas geralmente utilizam alguma ferramenta para realizar esse procedimento de forma automática, armazenam suas fitas de *backup* em lugares seguros, realizam testes de *restore* (reinserir os dados armazenados no sistema) entre outros procedimentos. Em empresas mais estruturadas, todos os procedimentos relativos a esse controle constam em políticas amplamente disseminadas entre os funcionários da área de TI.

Para evidenciarmos a realização desse controle em todos os seus aspectos, devemos realizar profundo entendimento da área junto aos funcionários de TI.

* + 1. **Instalações do CPD**

Esse controle, pertencente ao domínio de Operações Computadorizadas, procura fazer com que o ambiente físico onde estão instalados os servidores da empresa seja o melhor possível. Esse ambiente, segundo as melhores práticas, deve possuir controles de temperatura, umidade, combate a incêndios, entre outros artifícios para proteger ao máximo os dados da empresa.

Para testarmos a eficácia desse controle, uma simples visita à sala onde estão localizados os servidores da empresa resolve nossa questão. Contudo, nessa visita, devemos estar atentos a todos os aspectos da sala.

* + 1. **Monitoramento do Ambiente de TI**

Esse controle, pertencente ao domínio de Operações Computadorizadas, tem como objetivo o constante monitoramento da ocorrência de possíveis problemas na estrutura do ambiente de TI da empresa (baixa capacidade de processamento, falta de espaço em disco, entre outros problemas). Para esse constante monitoramento, as melhores práticas recomendam o uso de *softwares*.

Para evidenciarmos o adequado monitoramento do ambiente de TI basta entendermos se a empresa utiliza alguma ferramenta do mercado para esse fim e como ela é utilizada.

* + 1. **Plano de Contingência e Continuidade do Negócio**

Esse controle, pertencente ao domínio de Operações Computadorizadas, busca que a empresa esteja prevenida para quaisquer eventuais catástrofes não esperadas como incêndios, alagamentos e outros desastres naturais. Para isso, com o intuito de garantir sua continuidade do negócio, muitas empresas desenvolvem planos de ação para casos como esses.

Para testarmos a utilização desse controle, devemos indagar se a empresa possui algum plano desse tipo formalizado. Além disso, um plano desse tipo deve ser amplamente divulgado entre os funcionários da área de TI e deve haver treinamentos para casos como os descritos.

* 1. **Resultados dos Testes Aplicados na Empresa Fictícia**

A seguir, serão expostos os testes que verificam o desempenho dos 19 controles previamente identificados que estão relacionados na Seção 5.1. Os testes expostos apresentam conformidade com as estratégias definidas também na Seção 5.1.

Para seguir um padrão para cada item, pode-se verificar que cada formalização do trabalho está dividida em entendimento, teste e conclusão. Poderá se observar que, em algumas vezes, apenas o entendimento se faz necessário para se chegar a alguma conclusão específica. Esse modelo foi escolhido por ser o mais intuitivo na opinião da equipe que executou o trabalho. Contudo, mais uma vez, sabe-se que o trabalho poderia ser executado de maneira diferente.

Como também não é definido no ISA 315 a forma de se descrever os testes executados, fica a cargo da equipe de auditoria essa definição.

* + 1. **Transações Críticas dos Sistemas**

**Entendimento:** Verificamos, junto ao Sr. Coordenador de Desenvolvimento, que todas as transações realizadas no ambiente de produção do sistema possuem *log* habilitado, identificando o usuário que executou a transação e a data de execução. Ele nos informou que está em processo de implantação um procedimento de monitoramento periódico desses *logs.*

**Teste:** N/A.

**Conclusão:** Controle não efetivo. Recomendamos que se instaure, de forma estruturada, um procedimento formal de monitoramento dos *logs* de acesso às transações críticas. Adicionalmente, recomendamos que sejam mantidas evidências das transações monitoradas, dos responsáveis pelo monitoramento e das ações corretivas tomadas ao serem identificadas exceções.

* + 1. **Parametrização de Senhas dos Aplicativos**

**Entendimento:** Através de entendimento realizado com o Sr. Coordenador de Desenvolvimento verificamos que os seguintes parâmetros de senha estão configurados para o sistema:

- Tamanho mínimo da senha de 8 caracteres;

- Histórico de 2 senhas memorizadas;

- Máximo de 4 tentativas de acesso até o bloqueio da senha;

- Tempo máximo de vida de 60 dias.

Entretanto, os critérios de complexidade de senha estão desativados (parâmetro “máscara da senha”).

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle não efetivo. Recomendamos que o parâmetro de complexidade de senha seja configurado no sistema, com o objetivo de aumentar a segurança dos acessos ao sistema aplicativo.

* + 1. **Revisão dos Perfis de Acesso dos Usuários**

**Entendimento:** Verificamos, juntamente ao Sr. Coordenador de Desenvolvimento, que os usuários do sistema possuem uma estrutura de perfil de acesso de acordo com o cargo ocupado e com as funções desenvolvidas em sua área, com base no projeto de Reformulação de Menu de Acesso do sistema, implementado no início do ano passado.

Consideramos o procedimento adequado, no sentido de estruturar os perfis de acesso de acordo com o cargo ocupado e com as funções desenvolvidas pelos colaboradores de cada área.

Contudo, nos foi informado pelo Sr. Coordenador que nesse ano não houve uma revisão ou sequer uma atualização do projeto realizado no ano passado.

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle não efetivo. Recomendamos que as revisões nos perfis de acesso dos usuários sejam realizadas periodicamente (ex: semestral ou anualmente), com o objetivo de adequar os acessos às funções exercidas pelos funcionários, bem como garantir a adequada segregação de funções nos acessos ao sistema.

* + 1. **Revogação de Acessos à Aplicação**

**Entendimento:** Vide procedimento de teste.

T**este:** Obtivemos com o Sr. Coordenador de Desenvolvimento, a listagem de usuários com acesso ao sistema. Adicionalmente obtivemos junto a Sra. Coordenadora de RH (Recursos Humanos), listagem dos funcionários e estagiários ativos e desligados da empresa, com o intuito de identificar usuários desligados que ainda possuam acesso à aplicação e usuários desconhecidos. Confrontamos os arquivos recebidos e verificamos que dos 454 usuários habilitados:

- Identificamos 3 usuários genéricos;

- Identificamos 8 usuários desligados com acesso;

- Não Identificamos usuários duplicados;

- Não identificamos usuários desconhecidos.

**Conclusão:** Controle não efetivo. Recomendamos que seja realizada a substituição de usuários genéricos por usuários pessoais para cada funcionário para que, dessa forma, seja mantida a trilha de auditoria. Adicionalmente, recomendaremos o bloqueio tempestivo dos usuários pertencentes a funcionários desligados.

* + 1. **Monitoramento de *Log* do Banco de Dados**

**Entendimento:** Fomos informados pelo Sr. Coordenador de Desenvolvimento, que o banco de dados do sistema disponibiliza *log* dos acessos realizados no banco. Entretanto, a empresa não possui um procedimento periódico de monitoramento desses log. Os *logs* são utilizados apenas quando necessário.

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle não efetivo. Recomendamos que seja implantado um controle de monitoramento periódico do *log* de acesso direto ao banco de dados do sistema, com o objetivo de verificar se todos os acessos foram devidos e autorizados pela administração.

* + 1. **Antivírus**

**Entendimento:** Realizamos entendimento junto ao Sr.Analista de Suporte, e verificamos que a ferramenta utilizada para proteger os servidores e estações de trabalho contra vírus e ameaças é o *Forefront Endpoint Protection* (FEP), fornecida pela Microsoft. Verificamos que o FEP está programado para realizar o *scan* nas estações de trabalho às quartas-feiras a partir das 12:15h e nos servidores aos sábados a partir das 3h. As atualizações nas máquinas ocorrem automaticamente a cada 8 horas, tanto para os servidores quanto para as estações de trabalho, identificando quando forem lançados novos *updates* divulgados no site da Microsoft. Verificamos ainda que a ferramenta disponibiliza o envio de alertas para o administrador da rede por email. Por fim, verificamos que a ferramenta disponibiliza relatórios de monitoramento para acompanhamento da área de Suporte, identificando o nível de atualização das máquinas e contaminação por vírus. Contudo, verificamos que essa opção ainda não estava configurada na ferramenta. Segundo informações da área, este recurso ainda não está em uso devido à recente aquisição da ferramenta.

**Testes:** Vide procedimento de entendimento.

**Conclusão:** Controle efetivo. Sem exceções a reportar.

* + 1. **Conexão Remota**

**Entendimento:** Verificamos juntamente com o Sr. Analista de Suporte, que o acesso remoto à rede interna da empresa é realizado através da ferramenta *Citrix*. A concessão desses acessos é realizada através de abertura de chamado na ferramenta específica da empresa. Esse tipo de chamado é aprovado, na maioria das vezes, pelo Sr. Gerente de TI. Verificamos que para acessar a rede remotamente, é necessário que o funcionário possua usuário e senha de rede e que o acesso seja liberado no *Active Directory* pelo administrador da rede. Os acessos à rede via *Active Directory* foram testados através do controle de “Revogação de Acessos à Rede”.

**Testes:** Vide procedimento de entendimento.

**Conclusão:** Controle efetivo. Sem exceções a reportar.

* + 1. **Firewall**

**Entendimento:** Através de entendimento realizado junto ao Sr. Analista de Suporte, verificamos que a ferramenta utilizada para controlar o tráfego de dados entre a rede interna e a internet é o *Threat Management Gateway* 2010 (TMG). Adicionalmente, verificamos que o firewall está configurado para bloquear sites considerados pela empresa como indevidos (sites de download, pornografia, fofocas, etc.), assim como todos os acessos externos divergentes daqueles configurados como liberados. Por fim, fomos informados que a empresa não disponibiliza da ferramenta IDS para detecção e tratamento das tentativas de intrusão à rede interna da empresa de forma estruturada.

**Testes:** Vide procedimento de entendimento.

**Conclusão:** Controle não efetivo. Recomendamos a adoção de ferramenta IDS para detecção e tratamento das tentativas de intrusão à rede interna da empresa de forma estruturada.

* + 1. **Inventário de Hardware e Software**

**Entendimento:** Através de entendimento junto ao Sr. Analista de Suporte verificamos que a ferramenta *System Center* é utilizada na realização de inventário de hardware e software pela empresa. Contudo, fomos informados pelo Sr. Analista de Suporte que não é realizado um controle periódico de *softwares* instalados versus licenças adquiridas pela empresa, com o objetivo de coibir instalações de *softwares* irregulares e/ou não-autorizados pela administração. Adicionalmente, fomos informados pelo Sr. Analista de Suporte que as contas utilizadas pelos funcionários são de usuários comuns e não de administradores. Desta forma não é possível instalar *softwares* irregulares e/ou não autorizados pela administração.

**Testes:** Com o intuito de verificar a autenticidade do bloqueio, realizamos teste na máquina da Sra. Assistente Administrativo (Depto. Marketing), tentando instalar um software juntamente com o Sr. Analista de Suporte. Verificamos que a instalação não foi concluída devido à insuficiência de privilégios, pois a usuária não é administradora local da estação de trabalho.

**Conclusão:** Controle não efetivo. Recomendamos que seja implantado um controle periódico e estruturado para comparar a quantidade de softwares instalados versus licenças adquiridas, com o objetivo de se identificar a instalação de softwares irregulares e/ou não-autorizados pela administração.

* + 1. **Parametrização de Senhas da Rede**

**Entendimento:** Obtivemos com o Sr. Analista de Suporte, os parâmetros de configuração de senhas da rede da empresa (*Active Directory*). Verificamos que os seguintes parâmetros de senha estão configurados de forma adequada:

- Comprimento mínimo da senha: 8 caracteres;

- Histórico de senhas: 2 senhas memorizadas;

- Tempo de vida máximo da senha: 60 dias;

- Tempo de inatividade: 5 minutos;

- Limite de bloqueio de conta: 5 tentativas inválidas de *logon*;

- Zerar contador de bloqueios de conta: após 5 minutos.

Entretanto, verificamos que alguns parâmetros poderiam ser melhorados:

- A senha deve satisfazer a requisitos de complexidade: Desativada

- Tempo de vida mínimo da senha: 0 dias

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle não efetivo. Recomendamos configuração dos seguintes parâmetros de senha, de forma a conferir maior segurança dos acessos à rede da empresa:

- Ativação do parâmetro de complexidade de senha;

- Tempo de vida mínimo da senha: 5 dias (com o objetivo de coibir a troca seqüencial e repetitiva de senhas).

* + 1. **Utilização da Rede Wireless**

**Entendimento:** Através de entendimento com o Sr. Analista de Suporte, verificamos que existem 10 *access points* ativos na empresa, os quais atendem a rede de visitantes, rede dos funcionários e a rede de telefone. Adicionalmente, verificamos que os *access points* apresentam protocolo de criptografia ativada (WEP 104*bits*). Para os acessos à rede de visitantes, que se utiliza de um *link* específico para essa finalidade, é necessária a criação de um usuário e senha para concretização do acesso (durante nossa visita foram criados dois destes usuários para acessarmos à rede de visitantes).

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle efetivo. Consideramos a configuração adequada para coibir o acesso não autorizado à rede interna da empresa.

* + 1. **Revogação de Acessos à Rede**

**Entendimento:** Vide procedimento de teste.

**Teste:** Obtivemos com o Sr. Analista de Suporte, a listagem de usuários com acesso ao *Active Directory*. Adicionalmente, obtivemos junto a Sra. Coordenadora de RH, a listagem dos funcionários e estagiários ativos na empresa e a listagem de funcionários e estagiários desligados no ano em exame, com o intuito de avaliar a consistência dos acessos à rede. Confrontamos os arquivos recebidos e verificamos que, dos 838 usuários ativos:

- 79 casos se tratavam de usuários genéricos;

- Não havia casos de usuários duplicados;

- Identificamos 5 usuários desligados com acesso.

Adicionalmente, analisando o trabalho feito no ano anterior, identificamos 5 usuários desligados que ainda possuem acesso.

Inicialmente, não conseguimos realizar a análise de usuários desconhecidos devido à inexistência de uma chave entre a lista de usuários e a lista de funcionários ativos na folha de pagamento. Em contrapartida, conseguimos gerar manualmente uma lista com 158 usuários com possibilidade de serem desconhecidos. Verificamos na nossa metodologia de auditoria que para uma quantidade de itens entre 100 e 200, deveríamos gerar uma amostra de, no mínimo, 20 itens. Com o intuito de obter maior conforto sobre nossa amostra, geramos uma amostra de 40 usuários no software ACL e realizamos análise junto ao Sr. Analista de Suporte. Durante análise, não foram identificados usuários desconhecidos.

**Conclusão:** Controle não efetivo. Recomendamos o bloqueio dos usuários pertencentes a funcionários, estagiários e prestadores de serviços desvinculados da empresa. Adicionalmente, recomendamos que seja realizada análise visando a substituição de usuários genéricos por usuários pessoais para cada funcionário para que, dessa forma, seja mantida a trilha de auditoria.

* + 1. **Termo de Utilização da Rede**

**Entendimento:** Fomos informados pelo Sr. Gerente de TI, que a Política de Utilização da Rede é assinada pelos funcionários no momento da admissão e ficam sob a posse do RH (Recursos Humanos). Obtivemos com o Sr. Assistente Administrativo, a política de utilização da rede assinada por um funcionário. Verificamos que na política constam as práticas que devem ser seguidas pelos usuários em relação à utilização de rede, email, impressoras e acesso à internet.

**Teste:** Obtivemos com o Sr. Analista de Suporte a listagem de usuários com acesso à rede, com data de criação da conta. Filtramos os usuários que foram criados durante o ano em exame, gerando um arquivo com 311 usuários. Com base na nossa metodologia de auditoria, selecionamos uma amostra de 25 itens (risco baixo), com o intuito de confirmar o conhecimento das políticas pelos funcionários. Levando em conta que na amostra inicial selecionada obtivemos 6 usuários genéricos, selecionamos, aleatoriamente, 6 outros usuários para substituir os genéricos inicialmente selecionados. Obtivemos do Sr. Assistente Administrativo, as políticas de Utilização da Rede solicitadas. Da amostra inicialmente selecionada (25 casos), verificamos que:

- Em 10 casos, as políticas estavam devidamente assinadas;

- Em 2 casos, os usuários eram funcionários terceirizados e o RH não estava de posse das políticas nem conseguiu localizá-las;

- Em 1 caso, o funcionário estava desligado da empresa e não conseguimos obter o documento.

- Para os outros 12 casos também não conseguimos obter a Política de utilização da rede.

**Conclusão:** Controle não efetivo. Recomendamos maior controle no arquivamento e gerenciamento das políticas de utilização da rede dos funcionários da empresa.

* + 1. **Gerenciamento de Mudanças**

**Entendimento:** Fomos informados pelo Sr. Coordenador de Desenvolvimento que a empresa não possui uma política de mudanças de programas formalizada, na qual sejam especificados os papéis e responsabilidades em cada etapa do processo (solicitação do usuário, autorização da implementação, especificação do programa, implementação, testes, validação do usuário, autorização para migrar, migração para o ambiente de produção). Adicionalmente, verificamos que as solicitações de mudanças do sistema são realizadas através de chamados na ferramenta específica.

As alterações são analisadas pelo Coordenador de Desenvolvimento, que solicita via ferramenta ao usuário solicitante mais detalhes sobre a demanda (caso necessário) e, em seguida, direciona o chamado para um dos desenvolvedores. Os desenvolvedores visualizam o chamado e acessam diretórios próprios, onde atualizam as versões antes de iniciar a etapa de programação. Eles utilizam a ferramenta de desenvolvimento para alteração das fontes e, em seguida, enviam as mudanças para um diretório utilizado como "quarentena". Apenas o Coordenador de Desenvolvimento, acessa este diretório para analisar a alteração com auxílio da ferramenta *Subversion*. Após análise, o Sr. Coordenador de Desenvolvimento envia as alterações para o ambiente de produção.

Adicionalmente, fomos informados que as etapas de aprovação pela gerência impactada pela mudança; aprovação pela gerência de TI; especificação; priorização das alterações e teste de homologação não são formalizadas.

**Teste:** Obtivemos com Sr. Coordenador de Sistemas a relação de programas alterados no software Sub-version no nosso período em exame, contendo 1211 customizações. Geramos uma amostra de 25 ocorrências de acordo com nossa metodologia de auditoria e solicitamos ao Sr. Coordenador de Sistemas evidências das etapas de (a) solicitação do usuário e (b) documentação da mudança no aplicativo Sub-version.

Verificamos que das 25 ocorrências analisadas:

(a) apenas 6 casos possuíam evidência da solicitação da customização através de chamado na ferramenta específica. Para as outras 19 mudanças, verificamos que a solicitação não foi formalizada através da ferramenta específica (segundo a equipe de TI, não havia chamado porque a solicitação foi elaborada pelo Gerente de TI);

(b) 25 apresentaram documentação da mudança no software Sub-version.

Como exceção, consideramos os 19 casos de mudanças realizadas sem a formalização da solicitação do usuário através do específica.

**Conclusão** Controle não efetivo. Recomendamos formalização de um Procedimento de Mudanças de Programas do sistema, na qual sejam especificados os papéis e responsabilidades em cada etapa do processo (solicitação do usuário, autorização da implementação, especificação do programa, implementação, testes, validação do usuário, autorização para migrar, migração para o ambiente de produção) e que sejam mantidas evidências das etapas de solicitação do usuário, aprovação pela gerência impactada pela mudança; aprovação pela gerência de TI; especificação e priorização das alterações.

Adicionalmente, recomendamos que os testes de homologação e a sua documentação sejam pré-requisitos para migração das mudanças para o ambiente de produção e que as pessoas impactadas pelas mudanças sejam comunicadas. Para as alterações de maior relevância, recomendamos que sejam promovidos treinamentos formais ou que sejam disponibilizados manuais acerca das novas funcionalidades do sistema.

* + 1. **Segregação entre Ambientes**

**Entendimento:** Verificamos juntamente com o Sr. Coordenador de Desenvolvimento, a segregação do sistema em dois ambientes: (1) desenvolvimento/ teste; e (2) produção. Verificamos que o ambiente de produção está no servidor 9 e que o ambiente de desenvolvimento/ teste está no servidor 19, estando os dois ambientes devidamente segregados. Adicionalmente, verificamos que o pessoal de desenvolvimento não possui acesso direto ao ambiente de produção. Contudo, o Sr. Coordenador de Desenvolvimento é o responsável por efetuar as migrações do ambiente de desenvolvimento para o ambiente de produção. Para tanto, este se utiliza da ferramenta *TortoiseSVN*, que foi configurada para executar as migrações por meio de usuário administrador. Consideramos que não há deficiências relacionadas a segregação de funções entre desenvolvimento e migração para produção, uma vez que o Coordenador de Desenvolvimento é o único responsável por migrar as customizações para o ambiente de produção via ferramenta configurada para esta finalidade.

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle efetivo. Sem exceções a reportar.

* + 1. **Backup**

**Entendimento:** Obtivemos com o Sr. Analista de Suporte a política de *backup* da empresa. Verificamos que esta política compreende, de forma geral, os seguintes aspectos: abrangência do *backup*, periodicidade do procedimento e meio de armazenamento das informações. Entretanto, verificamos que a política de *backup* não define os responsáveis pelo procedimento.

Adicionalmente, através de entendimento junto ao Sr. Analista de Suporte, verificamos que os *backups* são realizados diariamente, de segunda à sexta, de forma “*full*”, a partir das 23:50h, através da ferramenta *ARCServe* R15, para todos os servidores da empresa, incluindo arquivos de rede, dados da aplicação do sistema e do banco de dados. São utilizadas diariamente 2 mídias LTO5 de 3 Tera *Bytes* de capacidade, utilizando-se um total de 10 mídias por semana. Este mesmo procedimento também é realizado em caráter mensal no último dia do mês e em caráter semanal aos sábados. Adicionalmente, são realizados *backups* *full* semanalmente e mensalmente.

O ARCserve disponibiliza os *logs* dos *backups* diários, permitindo a identificação do status do *backup*. Obtivemos com o Sr. Analista de Suporte o *log* do *backup* semanal de um dia aleatório e verificamos que este ocorreu de forma adequada.

Quanto ao armazenamento dos *backups*, fomos informados que as mídias de *backup* semanais, mensais e algumas diárias (*backups* da terça-feira e quinta-feira) são armazenadas em cofre anti-chamas em outro escritório da empresa (localizado na rua ao lado).

Para os outros *backups* diários (da segunda-feira, quarta-feira e sexta-feira), observamos que existe o armazenamento das mídias em cofre anti-chamas localizado dentro da própria sala de suporte da área de TI da empresa.

Fomos informados pelo Sr. Analista de Suporte que não existe procedimento periódico de teste de *restore*. A recuperação é realizada apenas quando necessário. Contudo, segundo o Sr. Analista de Suporte, surgem demandas freqüentes do pessoal da empresa para recuperar as informações / dados, o que justificaria a ausência de um procedimento periódico de *restore*. Verificamos que a ferramenta ARCserve apresenta *logs* dos *restores* efetuados.

Adicionalmente, segundo informações do Sr. Analista de Suporte, o banco de dados do ERP contém dados desde a implantação do sistema na empresa, isto é, qualquer mídia com *backup* *full* seria capaz de recuperar todas as informações necessárias à plena recuperação das funções de TI.

Levando em conta os controles identificados, bem como a ausência de histórico de problemas com backup na empresa, consideraremos o controle efetivo e não reportaremos exceções.

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle efetivo. Sem exceções a reportar.

* + 1. **Instalações do CPD**

**Entendimento:** Através de visita à sala dos servidores realizada junto ao Sr. Gerente de TI, verificamos que a sala dos servidores apresenta controle de acesso biométrico e apenas três pessoas estão autorizadas a entrar no local, são elas: o Gerente de TI e dois Analistas de Suporte.

A sala apresenta piso suspenso, os servidores estão armazenados em *racks* adequados, existe controle de temperatura e umidade automatizado e interligado com a Ronda Segurança, que direciona alertas para o gerente de TI via SMS e ligações telefônicas.

Verificamos também que a sala possui um sistema automatizado de combate à incêndio, que, caso ocorra algum incidente, se utiliza de gás nitrogênio para conter qualquer dano aos equipamentos.

Existe câmera de monitoramento na sala, cujas imagens estão disponíveis apenas para o setor de TI, sendo possível a visualização via acesso remoto para o gerente de TI.

Em casos de pane elétrica, a sala dispõe de dois *no-breaks* de 20kva, capazes de suportar 45 minutos sem energia. Além disso, a equipe de TI fechou um contrato com o condomínio do Empresarial para se utilizar do gerador do prédio em caso de pane elétrica mais longa (apenas para manter a sala de servidores em atividade).

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle efetivo. Sem exceções a reportar.

* + 1. **Monitoramento do Ambiente de TI**

**Entendimento:** Realizamos reunião junto ao Sr. Analista de Suporte, e verificamos que a empresa utiliza a ferramenta *System Center Operation Manager* para o monitoramento da capacidade de processamento dos servidores, espaço em disco, dentre outros aspectos. Verificamos que a ferramenta disponibiliza o aviso de alerta das irregularidades via email, o qual está habilitado para ser enviado ao gerente da área e aos analistas de suporte.

**Teste:** Vide procedimento de entendimento.

**Conclusão:** Controle efetivo. Sem exceções a reportar.

* + 1. **Plano de Contingência e Continuidade do Negócio**

**Entendimento:** Fomos informados pelo Sr. Gerente de TI que, no momento, a empresa não possui um Plano de Contingência ou Plano de Continuidade de Negócios formalmente documentado. Por outro lado, também nos foi informado que existe um projeto em fase de aprovação da diretoria, que contemplará várias atividades referentes à recuperação de desastres como, por exemplo, réplica de servidores em outra localidade.

**Teste:** N/A

**Conclusão:** Controle não efetivo. Recomendamos que seja elaborado um plano de recuperação de desastres ou plano de contingência para os recursos computacionais críticos da empresa (ex: servidores de aplicação e banco de dados do sistema), descrevendo em detalhes quem seriam os responsáveis, quanto tempo seria necessário e como seria o procedimento de re-estabelecimento dos serviços em caso de falhas ou desastres significativos no ambiente de TI.

* + 1. **Conclusão da Auditoria de Sistemas**

O ISA em sua seção 315 indica que: "*If the audit team intends to place continuous reliance on automated controls or to assume a controls reliance strategy in the financial statement audit, the team must assess the potential impact of all known automated controls weaknesses on the integrity of each underlying application control that the automated controls were designed to protect****.****"*

Dessa forma, a equipe de suporte à auditoria aconselha à equipe de auditoria a realização de uma “Análise de Mudanças nos Controles Automatizados” com o intuito de obter conforto nos controles automáticos devido às deficiências no domínio de “Mudanças de Programas”.

Para as demais deficiências da auditoria de sistemas, chegamos à conclusão que há, no planejamento de auditoria, procedimentos substantivos (revisões analíticas substantivas e testes de detalhes) suficientes para endereçar os possíveis impactos relacionados em nível relevante para as demonstrações financeiras. Ou seja, iremos conviver com as deficiências identificadas, porém reportando-as na carta de controles internos.

* 1. **Considerações Sobre o Estudo de Caso Apresentado**

Dos 19 testes aplicados aos controles, da empresa fictícia em exame, previamente identificados, que poderiam suprir os riscos descritos no ISA 315, podemos verificar que 12 deles não foram efetivos, segundo Tabela 3.

Da Tabela 3, pode-se verificar que aqueles em vermelho não foram efetivos.



Tabela - Análise dos Controles não Efetivos Divididos entre os Domínios do ISA

Da conclusão do estudo de caso, na Seção 5.2.20, entende-se que a equipe da auditoria de sistemas, junto à equipe de auditoria contábil, considerou os seguintes resultados para cada um dos domínios do ISA:

* Para o domínio de Acesso a Programas e Dados, os auditores consideraram que poderiam conviver com os riscos identificados mesmo se confiando em controles automatizados. Contudo, iriam reportar as deficiências identificadas em carta de controles internos (para mais informações sobre carta de controles internos vide Seção 2.2)
* Para o domínio de Mudanças de Programas, a equipe de auditores considerou a deficiência encontrada como bastante significativa. Dessa forma, foi sugerido à equipe de auditoria contábil que, toda vez que fosse se confiar em controles automatizados, que se fizesse uma análise das mudanças consideráveis realizadas naquele processo.
* Para o domínio de Operações Computadorizadas, os auditores consideraram a única deficiência encontrada como imaterial dentro da análise de todo o domínio. Dessa forma, considerou-se que se poderia conviver com o risco identificado, porém sendo reportado em carta de controles internos.

Dessa maneira, portanto, foi concluído o trabalho da auditoria de sistemas e seus resultados foram enviados à equipe da auditoria contábil para que as documentações fossem devidamente incorporadas ao trabalho como um todo.

1. **Conclusão e Trabalhos Futuros**
   1. **Conclusão**

Não restam dúvidas da relevância de trabalhos de auditoria de demonstrações financeiras no atual mercado financeiro brasileiro e mundial. Nesse sentido, a prática de auditoria de sistemas de informação como parte integrante desses trabalhos vem ganhando cada vez mais espaço. Atualmente, vem crescendo o número de profissionais de diversas áreas que exercem esse tipo de atividade.

Por outro lado, um projeto de auditoria de sistemas de informação não pode ser considerado uma atividade trivial. Um projeto desse tipo necessita de profissionais com características multidisciplinares. Um auditor de sistemas deve ter a capacidade de discutir sobre riscos contábeis com a equipe de auditoria contábil, deve conseguir dialogar sobre termos técnicos com gerentes de TI e, entender sobre processos e controles internos. Ou seja, um auditor de sistemas deve possuir habilidades das áreas de Ciências Contábeis, Tecnologia da Informação e Administração de Empresas.

Considerando o aspecto da TI, os testes realizados na empresa em exame com o intuito de verificar a eficácia de controles devem possuir embasamento teórico. Para isso, muitas empresas de auditoria possuem metodologias baseadas em *frameworks* como o CobiT. Dessa forma, conhecer vários conjuntos de melhores práticas para a área de TI engrandece o trabalho de um auditor de sistemas. Isso acontece quando a forte fundamentação teórica dá respaldo às recomendações de melhoria efetuadas.

Com a esperança de apoiar trabalhos de auditoria contábil mais eficientes, evitando, dessa forma, riscos de fraudes e erros, espera-se que a qualidade das auditorias de sistemas só faça crescer nos próximos anos. Portanto, espera-se o contínuo aprimoramento das melhores práticas para a Tecnologia da Informação e uma maior inserção das metodologias de auditoria nessas práticas.

* 1. **Trabalhos Futuros**

Um trabalho de auditoria contábil é, ao mesmo tempo que bastante solicitado, no atual mercado financeiro, bastante complexo e demanda a participação de várias pessoas com formações diferentes. Nesse documento, avaliamos a inserção e a importância da Tecnologia da Informação nesses projetos com a atuação da auditoria de sistemas.

Por outro lado, profissionais com formação em cursos de Tecnologia não limitam sua participação nas auditorias de demonstrações financeiras a somente essas atividades. Existem também outras atividades praticadas por esses profissionais que se denominam de TAAC’s (Técnicas de Auditoria Auxiliadas por Computador). Essas atividades são essencialmente o teste da confiabilidade de grandes bases de dados com o auxílio de *softwares*. Além disso, cientistas e engenheiros da computação devem conhecer os mais diversos ERP’s (*Enterprise Resource Planning*) do mercado para auxiliar os demais membros da equipe de auditores a extrair quaisquer informações do sistema de informação em uso com confiabilidade [21, 22].

Por fim, apenas para demonstrar mais um pouco a grande abrangência de novos estudos que poderíamos realizar, poderíamos também realizar novos trabalhos com enfoque em outros tipos de auditoria de sistemas de informação. Como mencionado na Seção 3.1, nesse documento demos ênfase a auditoria de sistemas de informação como parte integrante de um projeto de auditoria contábil. Contudo, poderíamos abordar mais aspectos da atividade de auditoria de sistemas de informação se considerássemos essa atividade como parte de um trabalho de auditoria de controles internos (auditoria da lei *Sarbanes Oxley* por exemplo). Além disso, relembrando a Seção 3.1, uma auditoria de sistemas também pode ser solicitada como uma tentativa de verificar pontos de melhoria nos controles de tecnologia da informação (projeto geralmente realizado pela área de auditoria interna da empresa) e a própria área de TI pode realizar trabalhos desse tipo com um enfoque maior na segurança dos dados, e na eficiência dos recursos. Dessa forma, qualquer estudo sobre auditoria de sistemas de informação sob esses diferentes enfoques teria muitas questões a serem discutidas [13].

**Referências Bibliográficas**

**[1] SOARES PACHECO, MARCELA; RENATO DE OLIVEIRA, DENIS; LA GAMBA, FABRÍCIO. A História da Auditoria e suas novas tendências: um enfoque sobre Governança Corporativa** – Online, acesso em 21/05/2012 na url <http://www.ead.fea.usp.br/semead/10semead/sistema/resultado/trabalhosPDF/204.pdf>

**[2] MARINHO DE M. MENEGUSSI, ELIRES; AUGUSTO LANESKO, JOSÉ. A importância da Auditoria Contábil na prevenção e combate aos erros e às fraudes nas organizações** – Online, acesso em 13/03/2012 na url <http://web03.unicentro.br/especializacao/Revista_Pos/P%C3%A1ginas/6%20Edi%C3%A7%C3%A3o/Aplicadas/PDF/1-Ed6_CS-ImpAu.pdf>

**[3] Comissão de Valores Mobiliários** – Online, acesso em 21/05/2012 na url <http://www.cvm.gov.br/>

**[4] Banco Central do Brasil** – Online, acesso em 21/05/2012 na url <http://www.bc.gov.br/>

**[5] Superintendência de Seguros Privados** – Online, acesso em 21/05/2012 na url <http://www.susep.gov.br/>

**[6] Agência Nacional de Saúde Suplementar** – Online, acesso em 21/05/2012 na url <http://www.ans.gov.br/>

**[7] AUDIBRAS AUDITORES E CONSULTORES. Alteração na lei das entidades sem fins lucrativos** – Online, acesso em 21/05/2012 na url <http://audibras.blogspot.com.br/2010/01/alteracao-na-lei-das-entidades-sem-fins.html>

**[8] HENRIQUE TEIXEIRA, PAULO. Profissão: Auditor Independente** – Online, acesso em 21/05/2012 na url <http://www.portaldecontabilidade.com.br/tematicas/auditor.htm>

**[9] ALVES DE CRISTO, CÉLIA; LOPES DA SILVA, ELMY. A função ética e a responsabilidade social do auditor na análise das demonstrações contábeis** – Online, acesso em 23/05/2012 na url <http://www.contabeis.com.br/artigos/34/a-funcao-etica-e-a-responsabilidade-social-do-auditor-na-analise-das-demonstracoes-contabeis/>

**[10] International Standard on Auditing (UK and Ireland) 315 –** Online, acesso em 13/03/2012 na url <http://www.frc.org.uk/images/uploaded/documents/ACF15D.pdf>

**[11] Governança de TI** – Online, acesso em 23/05/2012 na url <http://www.codix.com.br/blog/governanca-de-ti.html>

**[12] Método de auditoria a Sistemas de Informação** – Online, acesso em 24/05/2012 na url <http://recursos.wook.pt/recurso?&id=184404>

**[13] FALCÃO DE BITTENCOURT, DÊNIA; BASTOS, VIVIANE. Auditoria de Sistemas Informatizados** – Online, acesso em 24/05/2012 na url <http://www.profallan.com/profallan.com/asi.pdf>

**[14] RAFAEL V. SIMCH, MAICOM; SQUINZANI TONETTO, TIAGO. Auditoria dos Sistemas de Informação Aliada à Gestão Empresarial –** Online, acesso em 13/03/2012 na url <http://w3.ufsm.br/revistacontabeis/anterior/artigos/vIVn02/t005.pdf>

**[15]** ISACA (INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION). CobiT 5, 2012

**[16] ISACA (Information Systems Audit and Control Association) São Paulo Chapter** – Online, acesso em 24/05/2012 na url <http://www.isaca.org.br/novoportal/>

**[17]** ITGI (IT Governance Institute), CobiT 4.1, 2007

**[18] CASSOL PICADA, RODRIGO; CARLOS G. MAÇADA, ANTONIO; RAMOS RIOS, LEONARDO; MORAES DOS SANTOS, ANDRÉ. Governança de Tecnologia de Informação baseado na Metodologia COBIT: O caso de um banco privado brasileiro** – Online, acesso em 02/05/2012 na url <http://www.ea.ufrgs.br/professores/acgmacada/pubs/Governanca%20TI%20macada%20rodrigo%20leonardo%20guilherme%20enegep%202007.pdf>

**[19]** DO PATROCÍNIO, Cosme Leandro; FONSECA, Décio. **IT Governance: a challenge for Internal Auditor.** Universidade Federal de Pernambuco, 2007

**[20]** El Comité Directivo de CobiT; La Information Systems Audit and Control Foundation. **CobiT – Directrices de Auditoria.** 1998

**[21] Computer Assisted Audit Techniques (CAATs)** – Online, acesso em 29/05/2012 na url <http://220.227.161.86/10857p730-737.pdf>

**[22] O ERP é uma ferramenta tecnológica de gestão empresarial, utilizada por empresas do mundo todo** – Online, acesso em 29/05/2012 na url <http://www.cigam.com.br/erp/>