CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas

UM ESTUDO DA AUDITORIA DE SISTEMAS DE INFORMAÇÃO E AS FERRAMENTAS EMPREGADAS NESTE PROCESSO

SIDNEI JOSÉ VICENTE

Americana, SP
2013

CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas

UM ESTUDO DA AUDITORIA DE SISTEMAS DE INFORMAÇÃO E AS FERRAMENTAS EMPREGADAS NESTE PROCESSO

SIDNEI JOSÉ VICENTE
sidnei.1984@yahoo.com.br

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas da Fatec-Americana, sob orientação do Prof. Dr. Moacir Degasperi Junior.

Área: Tecnologia em Análise e Desenvolvimento de Sistemas

Americana, SP
2013

BANCA EXAMINADORA

Professor Dr.: Moacir Degasperi Junior (Orientador)

Professor Esp.: Fernando José Ignácio

Professor Esp.: Rogério Nunes de Freitas

SIDNEI JOSÉ VICENTE

UM ESTUDO DA AUDITORIA DE SISTEMAS DE INFORMAÇÃO E AS FERRAMENTAS EMPREGADAS NESTE PROCESSO

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas da Faculdade de Tecnologia de Americana.

Aprovado: 17 de junho de 2013

_____ _____

Prof. Esp.: Fernando José Ignácio **Prof. Esp.: Rogério Nunes Freitas**

_____

Prof. Dr.: Moacir Degasperi Junior

Americana, SP
2013

AGRADECIMENTOS

Primeiramente a Deus por toda a saúde, vitalidade para estudar e conseguir sempre superar as dificuldades e que pelo sangue de Cristo Nosso Senhor, está presente mesmo diante de minhas rebeldias, aliviando meu fardo em momentos difíceis.

A minha esposa e meu filho que compartilharam o tempo dividido pelo estudo e dedicação, pelas batalhas ganhas e perdidas, por me apoiarem mesmo quando me sentia abalado e sem paciência, ou quando perdia a coragem de enfrentar os desafios da vida.

A quem não está comigo, embora desejasse muito sua presença (em memória de Dolcídio, meu querido pai), e a quem devo a honra de receber a primeira educação e os primeiros princípios de minha formação, minha mãe, Jovelina, que sempre se esforçou para me ver onde estou agora, e que sempre confiou em minha capacidade e me ensinou a confiar em Deus e muitos outros valores preciosos.

A meus mestres que tiveram a dedicação e paciência de me ensinar, sem que pudessem ganhar muito em troca, além da satisfação em exercer a função grandiosa de ministrar aquilo que sabem e, em especial, ao Prof. Moacir que me orientou na construção desta obra.

A meus amigos de curso e trabalho, principalmente Bruno e Ana. Não poderia deixar de agradecê-los por me ajudarem nessa carreira de conhecimento, pela paciência e pelo esforço em equipe.

DEDICATÓRIA

Dedico este trabalho ao Senhor Deus, a minha querida esposa Janaina e ao meu querido filho Estevam, aos meus pais, aos meus mestres pelo apoio e paciência e aos meus amigos de faculdade que estarão em minhas lembranças.

RESUMO

Os sistemas de informação e a tecnologia de informação são extremamente importantes para o desenvolvimento das organizações empresariais que procuram sempre inovar em diversas perspectivas de negócio e padrões tecnológicos. A importância do estudo dos sistemas de informação possibilita esclarecer outros assuntos importantes como as vantagens de manter os sistemas seguros a partir de técnicas de sistemas de gerenciamento de segurança da informação que agregam valor ao negócio e confiança nos investidores, entretanto, empresas que fazem uso da tecnologia precisam sempre atualizar-se mediante o surgimento de novas tendências de mercado e proteger-se contra fraudes. São fornecidos, nesta obra, os conceitos básicos de auditoria de sistemas de informação, a partir de um estudo bibliográfico, que mostram os passos necessários para a execução dos trabalhos de auditoria dos sistemas de informação. É abordada a necessidade das empresas que esperam um alinhamento da tecnologia da informação com a estratégia da organização, ou seja, um requisito avaliado pela auditoria de sistemas de informação com a intenção de buscar a conformidade deste alinhamento, detectando fraudes e riscos, avaliando e acompanhando as soluções se necessário. São necessários pré-requisitos para o desenvolvimento da carreira de auditor de sistemas de informação, análise de níveis de conhecimento, hierarquia organizacional e plano de carreira, e estes pré-requisitos são, aqui, analisados. Este estudo procura descrever algumas das ferramentas de auditoria ou programas de computadores que o auditor poderá utilizar nos processos de auditoria, para que o leitor/auditor consiga observar a ferramenta mais apropriada para a empresa e até mesmo tirar conclusões para desenvolver uma ferramenta personalizada que será utilizada por ele ou por sua equipe de auditoria.

Palavras Chave: Sistemas de informação; Auditoria de sistemas de informação; Ferramentas de auditoria.

ABSTRACT

Information systems and information technology are extremely important for the development of business organizations that are always looking to innovate in different business perspectives and technological standards. The importance of the study of information systems allows us to clarify other important issues such as the advantages of keeping systems secure through technical systems security management of information that add value to business and investor confidence, however, companies that use technology must always update themselves through the emergence of new market trends and protect themselves against fraud. It is provided in this work basic concepts of information systems auditing through a bibliographical study which shows the steps needed to execute the information systems audit. It is discussed the need for companies to expect an information technology alignment with the organization's strategy, in order words, a requirement assessed by the information systems audit with the goal of looking for a compliance of this alignment detecting fraud and risks, assessing and monitoring solutions. Prerequisites are necessary for the development of information systems auditor career, examining knowledge levels, organizational hierarchy and career plan, therefore these prerequisites are here analyzed. This study aims to describe some of the audit tools or computer programs that may be used by the auditor in auditing procedures, so the reader/ auditor can observe the most appropriate tool for the company and even make their own conclusions to develop a custom one that will be used by their audit team.

Keywords: Information systems; information systems audit; audit tools.

LISTA DE ABREVIATURAS/SÍMBOLOS

TI ..... Tecnologia da Informação
SI ..... Sistemas de Informação
SGSI ..... Sistema de Gerenciamento de Segurança de Informação
SA .....Sociedade Anônima
SGBD .....Sistema de Gerenciamento de Banco de Dados
ISACA ..... Associação dos Auditores de Sistemas e Controle
CISA .....*Certified Information Systems Auditor*
© ..... *Copyright*
CASE .....Computer-Aided Software Engineering
SOx .....Sarbanes-Oxley
® ..... Registrado
MS .....Microsoft
IDEA .....Interactive Data Extraction & Analisys
ACL .....Audit Command Language
SE .....SOFTEXPERT
GRC ..... Governance, Risk and Compliance
TAAC ..... Técnicas de Auditoria Assistidas por Computador
RH ..... Recursos Humanos

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

O surgimento da auditoria é relatado desde a Idade Média. Sua principal função era ouvir os responsáveis pelos ativos e pelos patrimônios, descrevendo e documentando com o desígnio de apontar ou prever possíveis falhas contábeis na gestão deste patrimônio e nos demais componentes do império ou organização, sendo ainda testemunha destas para com os soberanos e responsáveis pela equipe de auditoria.

Com o surgimento do capitalismo e da Revolução Industrial, a auditoria se adaptou para atingir os novos setores e controles organizacionais que surgiram. Muitos deles, sistemas contábeis e outros sistemas da organização. A auditoria se tornou requisito necessário para os líderes da organização e governo que procuravam controlar o capital e obter investimentos externos. São muitos os benefícios que a auditoria traz para uma organização ou governo descentralizado, que controla os setores industriais e comerciais em outros países (GOMES; ARAÚJO; BARBOSA *apud* SÁ, 1998, p. 21).

Como as organizações precisavam investir no Novo Mundo, um continente emergente e dependente capitalista, a auditoria tão breve acompanhou este investimento seguindo as multinacionais que vinham para o Brasil e se instalaram, procurando novos rumos de negócio, e foram divulgando também suas técnicas e experiências para as organizações de auditoria brasileiras que se formavam com base nas organizações de auditoria estrangeiras (GOMES; ARAÚJO; BARBOSA *apud* MOTTA, 1992).

Com o surgimento da era computacional, por volta da década de 1950, mais uma vez ocorreram mudanças na gestão dos negócios. As empresas se transformavam principalmente na área de infraestrutura de tecnologia da informação (TI), para apoiar na gestão e na governança corporativa, e demais setores empresariais tentando diminuir a complexidade e a demora dos processos de envio de dados e da informação aumentando a interação entre os módulos que se distanciavam (IMONIANA, 2008).

Os métodos de processamento de dados, de gestão de pessoas e máquinas existentes junto com os sistemas de controle já não eram tão competentes para a demanda de trabalho. Houve a necessidade de rápida expansão e de novos recursos competitivos, precisando de um gerenciamento mais preciso, de mais máquinas para auxílio e a evolução das que já existiam para atenderem o sistema de gerenciamento da informação que evoluía (IMONIANA, 2013).

Para atender estas necessidades surgiu uma intensa demanda de gerenciamento sobre os dados processados e junto deste gerenciamento, profissionais especializados, como os auditores, que são responsáveis por analisar a complexidade deste sistema e emitir suas opiniões e soluções para o combate e prevenção às falhas nos sistemas da organização.

Foram criadas empresas de auditoria compostas por auditores que conhecem detalhadamente os sistemas da organização, como finanças, contabilidade, recursos humanos e TI.

A auditoria pode ser dividida em auditoria interna e auditoria externa. A auditoria interna geralmente é controlada pelos gestores da organização que se preocupam com a análise dos sistemas e com os rumos estratégicos da organização. Geralmente confiam em um grupo de auditoria mais reservado.

A auditoria externa ou independente é executada sob interesse de acionistas ou organizações governamentais, sem que este grupo de auditores possua nenhum vínculo com a empresa auditada, e mantém o foco na auditoria detectando e evitando os prejuízos causados com informações incorretas (fraudes), paralisias e perdas (IMONIANA, 2008).

O estudo se **justifica** pela necessidade de analisar o processamento de dados através dos sistemas de informação (SI) nas organizações privadas ou governamentais que, depois de amplamente desenvolvida, necessita de um controle/gerenciamento mais sensível e de precisão evitando assim possíveis falhas e fraudes.

Para monitorar os sistemas com precisão e controle surge o profissional auditor de sistemas de informação que utiliza as informações e os processos antes disponíveis somente em papel, e que atualmente são transmitidas e guardadas nos computadores e distribuídas entre os subsistemas através de redes de comunicação, mídias digitais, etc., utilizando diversas técnicas de abordagens ao auditado buscando como auxílio a TI (IMONIANA, 2008).

O estudo analisa minuciosamente parte das ferramentas e técnicas de auditoria no mercado de trabalho. Aborda as tecnologias existentes em cada uma delas, para posteriormente o auditor fazer uso nos processos de auditoria nas empresas. Busca detalhes e conformidades com as normas e políticas organizacionais da empresa e os requisitos e a demanda de trabalho.

Já o **problema** foi: falta de comitês e padrões que especializam a carreira do auditor de sistemas, já que, os processos de auditoria de sistemas são confundidos com outros processos de auditoria, por participar de uma auditoria generalista, é confundido com outros processos de auditoria, tornando difícil a regulamentação do trabalho do auditor de sistemas de informação (IMONIANA, 2008).

A **pergunta** que se buscou responder: O auditor de SI enfrentaria dificuldades para escolher ou desenvolver a melhor ferramenta (programa de computador) de auxílio empresarial e como ele é determinado a escolher uma ferramenta existente no mercado de trabalho ou desenvolver uma ferramenta condizente com as técnicas necessárias da auditoria de sistemas de informação na organização?

As **hipóteses** encontradas foram: a) sim, poderia encontrar dificuldades se a auditoria fosse realizada fora dos padrões estabelecidos pela Associação de Auditores de Sistemas e Controle (ISACA) e outras associações, se não estudasse previamente a necessidade da organização pela auditoria dos sistemas de informação (IMONIANA, 2008); b) não, pois se o auditor de SI entender as necessidades da organização e como montar um planejamento para a auditoria, observando certificações importantes como a ABNT NBR 19011:2012, facilitaria para o auditor escolher uma ferramenta específica ou generalista de acordo com a ocasião e a organização auditada (ABNT NBR19011, 2012) e, c) talvez não

superasse as necessidades da empresa em ocasião, por escolher a ferramenta mais generalista e o sistema auditado precisar de uma ferramenta que analise mais profundamente um módulo do sistema, porém, o auditor deverá estudar todas as ocasiões possíveis como a cultura organizacional da corporação e praticar atividades de acompanhamento, adquirindo e avaliando informações apropriadas e aprimorando o seu conhecimento relativo aos avanços da tecnologia empregada e conceitos inovadores (IMONIANA, 2008).

O **objetivo geral** consistiu em: conhecer e analisar os princípios dos sistemas de informação nas empresas, princípios de segurança da informação, valores que os gestores das empresas e acionistas esperam que a auditoria identifique e análise a partir de toda a complexidade dos SI, compreender a função de auditoria de sistemas de informação e uso de ferramentas especialistas e generalistas, para auxiliar o auditor que, por sua vez, auxilia os gestores e acionistas da organização no processamento de dados, buscando a confiabilidade dos investimentos, a analisar e aperfeiçoar uma segurança mais eficiente, a combater as fraudes não calculadas e evitar uma paralisia por diversos problemas técnicos e operacionais como, incompatibilidade de programas ou máquinas, quedas nos sistemas de vendas pela Internet, falhas na segurança como falta de controle de acesso a ambientes que necessitam segurança, sendo eles físicos ou lógicos, sempre apontando deficiências no sistema e sugerindo medidas de correção e prevenção.

Os **objetivos específicos** foram: a) fazer um levantamento bibliográfico dos principais problemas relacionados à segurança de um SI e seus subsistemas devido à constante fraude dos dados processados, das pessoas envolvidas, das informações e documentos no subsistema social e, dos meios automatizados (computadores e redes de comunicação) que interligam os elementos do subsistema automatizado; b) estudar os processos de auditoria de SI, sua aplicação de forma correta, sua mutação e atualização e sua importância para a organização que atinge uma expansão sem precedentes procurando atender a necessidade dos fundadores e gestores da organização, com a intenção de confirmar se todos os controles existem e funcionam de forma efetiva (IMONIANA, 2008); c) fazer um levantamento de técnicas de auditoria mediante os comitês de padrões e associações, certificações e desenvolvimento de equipes de auditoria para o auxílio e

planejamento completo do auditor, evitando gastos desnecessários para as empresas que investem pesadamente no controle dos SI e, descrever uma ampla variedade de ferramentas para auxílio de auditoria, não as comparando, mas, expondo em contraste com sua aplicação mediante os diversos problemas que podem ocorrer nos principais processamentos de dados, acrescentando uma visão para decisões precisas para a organização e para a equipe de auditoria (ABNT NBR19011, 2012).

Como **metodologia** para o desenvolvimento deste trabalho, foi utilizada a pesquisa exploratória envolvendo um levantamento bibliográfico e documental para o estudo do tema abordado e dos problemas relatados buscando exemplos para estimular a associação de opiniões e melhorar a compreensão do leitor com a pesquisa construindo um estudo detalhado da auditoria de sistemas e das ferramentas usadas para auxílio do auditor, de maneira que espalhe o conhecimento através do estudo de caso (SILVA; MENEZES, 2001).

O trabalho foi estruturado em três capítulos, sendo que, o **primeiro** capítulo explica conceitos sobre os sistemas de informação, sua classificação em sistemas abertos e fechados, as diferenças em relação à tecnologia da informação, além de, conceituar a segurança e as vulnerabilidades dos sistemas de informação e os pilares que sustentam a implantação da segurança nas organizações.

O **segundo** capítulo traz os conceitos relacionados à auditoria dos sistemas de informação, com os princípios básicos para a execução, seus padrões e normas, procedimentos teóricos de realização e quais são os requisitos básicos para se tornar um profissional auditor de sistemas de informação.

O **terceiro** capítulo descreve as técnicas gerais de auditoria e o uso das ferramentas generalistas e especialistas para auxilio no processo da auditoria de sistemas de informação com um aprofundamento no estudo das ferramentas generalistas, mais fáceis de serem encontradas e implantadas na organização.

Com base nas informações alcançadas a partir dos estudos realizados nos capítulos anteriores, o quarto capítulo se reserva às Considerações Finais.

2. SISTEMAS DE INFORMAÇÃO

Com a expansão dos sistemas computacionais e a expansão da Internet, nas organizações empresariais, as informações digitais também se expandiram ultrapassando fronteiras e continentes. As empresas necessitam tratar corretamente as informações, pois o mercado tornou-se globalizado e as estratégias são planejadas numa velocidade surpreendente.

A valorização da informação aumentou, cresceu a concorrência entre as empresas e junto a ela também aumentou a necessidade da segurança nas transações da informação, que percorre o mundo através de meios guiados e não guiados devido o deslocamento de unidades empresariais, como as multinacionais (DEGASPERI JUNIOR, 2006).

Neste capítulo estudamos conceitos detalhados dos sistemas de informação das empresas, abordaremos conceitos sobre sistemas abertos e fechados, as diferenças entre o SI e a TI e as necessidades de investimento para a implantação da TI. Também citamos os pilares que sustentam a segurança da informação e os processos que podem ser usados para a normatização da segurança da informação.

2.1. Conceitos sobre SI

Um sistema é um conjunto de módulos ou setores dependentes da organização interna e externa entre eles, que interagem formando um supersistema unitário e complexo com o objetivo de ser funcional, dinâmico e que se atualize em relação as suas finalidades e ambientes (DEGASPERI JUNIOR, 2010).

Os SI são utilizados para manter as operações das empresas. Eles são relacionados por fatores humanos e tecnológicos, para que funcione com bom desempenho é necessário um ambiente controlado e seguro.

A princípio, os SI eram somente usados no piso operacional das empresas, ajudando na redução de custos com mão de obra e auxiliando no aumento da produção, mas atualmente os sistemas migraram para todos os níveis da

organização auxiliando também no desenvolvimento tático e estratégico (DEGASPERI JUNIOR, 2006).

O engenheiro de sistemas é o profissional responsável pelo sistema que tem a função de perceber as funcionalidades do sistema na organização, as leis e as normas da organização em que são baseadas e seguem, e as interações do sistema junto aos ambientes internos e externos da empresa para um processamento exato. O engenheiro de software precisa entender o sistema para que consiga projetar e/ou desenvolver um programa que siga todos os padrões e decisões da engenharia de sistemas (SOMMERVILLE, 2004).

Os sistemas obedecem quase sempre a uma hierarquia na organização e dependendo de sua complexidade ele se divide e se transforma em um módulo mais especialista, como está representado na figura abaixo:

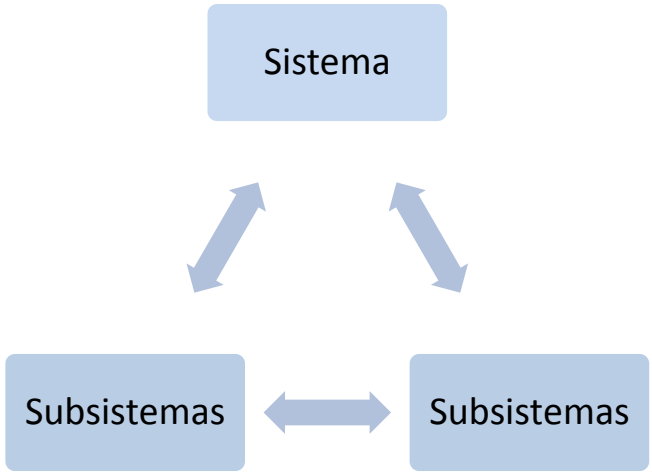

Figura 1 – Ecossistema de uma organização. Fonte: (LAUDON: LAUDON, 2006).

Observando a figura acima podemos fazer uma analogia e citar como exemplo um supersistema financeiro que pode ter como topo na hierarquia organizacional o módulo de administração financeira e se subdividir em subsistemas, com os departamentos de crédito e o departamento de finanças, sendo este último especializado em dois módulos: tesouraria e análise e controle (SOMMERVILLE, 2004).

As relações entre sistemas no ambiente da empresa sejam eles, interno ou externo, os fazem pertencer a um todo, ou seja, a um supersistema ou ecossistema onde todos são dependentes do ambiente organizacional (LAUDON: LAUDON, 2006).

Mesmo existindo estes subsistemas divididos e dependentes do sistema pai, eles ainda podem operar de forma independente e serem requisitados por outros sistemas operantes diferentes (DEGASPERI JUNIOR, 2010).

2.2. Sistemas abertos e fechados

Os sistemas podem ser classificados em abertos e fechados. Os sistemas abertos são classificados por realizarem transações transparentes para com os outros setores de negócios. Para que isso aconteça, todos os setores da empresa serão envolvidos, respeitando todas as normas e padrões estabelecidos pela engenharia de sistemas.

Os sistemas abertos podem ser analisados como uma gestão moderna de TI e estão vinculados a um modelo de gestão participativa que foca mudanças e adaptações internas (BARROS, 2011).

Já os modelos de sistemas fechados evitam a transparência com as transações externas, se tornando um sistema indiferente ou relativo, o que frequentemente estão vinculados a um modelo de gestão autoritário como o sistema de departamento pessoal (RH) e o sistema de almoxarifado obedecendo a paradigmas autoritários de administração.

Estes modelos de sistemas estão evoluindo, juntamente com as redes de computadores e com a evolução dos softwares. Os sistemas empresariais que em totalidade eram sistemas fechados e isolados, ou seja, mais fáceis para as organizações manterem o controle total, estão se modificando para sistemas abertos e distribuídos dificultando o monitoramento total das transações que ocorrem entre eles e os controles necessários para a segurança e a integridade (IMONIANA, 2013).

2.3. A diferença entre SI e a TI e o investimento aplicado em TI nas organizações

Existe uma estreita diferença entre SI e TI. Os módulos dos sistemas de informação necessitam dos componentes da TI, tais como, os computadores e seus programas e as redes de comunicações entre eles e demais dispositivos de transmissão e armazenamento de dados, para transformar os módulos dos sistemas operacionais e eficientes (DEGASPERI JUNIOR, 2006).

O investimento em TI nas organizações é um grande gerador de custo para os gestores das empresas que, sempre enxergam este investimento com pouco retorno em valor tangível. Sem dúvida, este investimento se não for bem planejado, poderá se tornar um fracasso de retorno em lucratividade para a organização.

Para alcançar resultados positivos, devem ser analisados fatores importantes para o sucesso como a compatibilidade e as funcionalidades que este novo sistema trará, e se este investimento em TI segue os padrões de estratégia e governança da corporação. Por exemplo, podemos citar aquela empresa que investe em tecnologia atualizada, mas não investe na eficiência e no entendimento do uso, como os treinamentos necessários para operar estes equipamentos.

A forma mais eficaz de investimento deve acontecer de forma correlacionada e não por motivos intuitivos ou sem prévio planejamento, evitando assim a perda dos recursos aplicados em ambos, TI e SI (DAWEL, 2005).

Cada sistema empresarial é diferente, o que funciona em uma organização pode não funcionar em outra. É sensato que um sistema antes de ser implantado, deve ser alinhado à cultura organizacional da empresa e analisado pela engenharia de sistemas, responsável por aprovar ou reprovar um investimento em TI que apresenta ou não concordância com as necessidades da organização (DEGASPERI JUNIOR, 2006).

É necessário que o nível gerencial ou executivo esteja envolvido por meio de reuniões e simulações construtivas no planejamento de investimento em TI, para analisar as contribuições da TI para a organização. Analisar se o gerenciamento da TI está devidamente alinhado à estratégia da organização, pois, antes da

autorização de um investimento como este, será necessária uma boa compreensão e visibilidade estratégica das necessidades encontradas (MARCUSSO, 2013).

2.4. A segurança e as vulnerabilidades dos sistemas de informação

Para que haja segurança em uma organização é necessário ministrar um entendimento do risco e da segurança preventiva para a perspectiva empresarial, propondo uma reflexão sobre a segurança da informação como um investimento ativo, além do investimento necessário com a TI.

A segurança existe quando o bem assegurado, ativo ou patrimônio, tangível ou intangível, está livre de ameaças de qualquer tipo. Sejam elas físicas como informações valiosas jogadas no lixo, escutas telefônicas, papéis ou relatórios deixados sobre a mesa ou visíveis no computador.

São diversos os tipos de ataques que aproveitam a falta de controle de acesso a sistemas críticos como, a sala onde ficam os servidores ou ameaças que atingem a psique do usuário do sistema, que por motivos de confiança ou credibilidade oferece o empréstimo de uma senha ou favores a pessoas não autorizadas (DAWEL, 2005).

Os dados que alimentam o sistema organizacional e a informação precisam estar seguros contra espionagem ou ataques. Como estes dados e informações são manipuladas por pessoas que trabalham na empresa, e na maioria dos casos, estes dados são armazenados nos computadores, eles podem vazar ou serem acessados por pessoas não autorizadas (IMONIANA, 2013).

Sistemas que apresentam vulnerabilidade em segurança sofrem acesso de diversas pessoas, algumas delas não autorizadas e com péssimas intenções, ou de pessoas de outros setores não integrados da empresa. Estes sistemas também podem sofrer ameaças vindas de fora da organização por meio da Internet, que se for usada incorretamente, pode ocasionar para a empresa prejuízos incalculáveis fazendo com que ela feche as portas (DAWEL, 2005).

Ao trocar ou acessar informações internas e externas ao sistema da organização, que seja observada a importância da utilização de técnicas de

criptografia. Com o uso destas técnicas, as informações que precisam ser transmitidas através de redes de informação inseguras, trazem junto dela uma chave de segurança que inibe o acesso do invasor, onde somente o destinatário possa receber a informação para ter acesso à mensagem (DAWEL, 2005).

Compreendendo o risco dos sistemas vulneráveis, é comprovada a extraordinária necessidade que o auditor tem de identificar estes riscos, podendo adquirir a ajuda de um profissional especialista na segurança da informação ou se especializar nos estudos e nas técnicas aplicadas.

Uma das principais funções do profissional auditor é analisar e avaliar os riscos, fazer um levantamento de ameaças e vulnerabilidades dos sistemas, elaborando relatórios de prevenção que apontem possíveis falhas que possam causar danos irreparáveis nos ativos da organização (IMONIANA, 2013).

Os desafios que os profissionais de auditoria e segurança da informação enfrentam devido o surgimento desenfreado de pragas cibernéticas (os famosos vírus de computador) e meios de conduzir fraudes e espionagem de documentos fazem desta profissão, uma necessidade de valor para a organização, uma vez que trabalham de forma sensível no acompanhamento e na manutenção dos sistemas (DAWEL, 2005).

2.5. Os pilares de sustentação da segurança da informação

A segurança da informação é o conhecimento e o estudo adicional da auditoria de sistemas, já que suas funções são levantar requisitos de usos de segurança nos sistemas e controles de uma organização, examinando as operações e identificando conformidades com os padrões exigidos pela organização auditada. Estes controles internos para a organização são essenciais e o foco baseado da auditoria esta na integridade e autenticidade destes controles (FERREIRA, 2013).

Existem quatro pilares fundamentais que regem a segurança da Informação. Falaremos brevemente sobre eles (DAWEL, 2005):

I. Confidencialidade: onde somente pessoas autorizadas poderão ter acesso às informações confidenciais dentro da organização e em ambientes

externos da organização o acesso a estas informações deverão ficar restritas a nenhum ou a um grupo restrito de responsáveis;

II. Autenticidade: a confirmação da verdade das informações, como uma análise de remetente válido de e-mail numa caixa de correio eletrônico;

III. Integridade: analisar se a informação não foi corrompida ou modificada por aqueles (vírus ou pessoas) que a manipulam;

IV. Disponibilidade: a informação esteja disponível somente para os que precisem dela.

Quando falamos da disponibilidade da informação e citamos também os riscos, não podemos esquecer um fato importante: os danos podem atingir um objeto de valor calculável, como um computador ou algo mais abstrato e incalculável, como a confiança de um cliente que não se sente seguro em acessar a página da empresa para efetuar compras online.

Podemos analisar determinada gravidade do dano causado em uma empresa pensando sobre o valor de cada hora de indisponibilidade de acesso à rede, ou a página de Internet, em uma empresa de comércio eletrônico que depende do fechamento de negócios e vendas pela Internet, e teve sua página desfigurada por um *cracker*[1] (DAWEL, 2005).

É importante ressaltar nesta seção as certificações que os níveis gerenciais podem se apoiar para auxílio nos controles e nos processos como, a implantação de um Sistema de Gerenciamento de Segurança da Informação (SGSI), de acordo com as necessidades da corporação, com a intenção de identificar ou detectar os riscos, analisar, avaliar e apresentar soluções para mitigar os riscos existentes (ABNT NBR ISO/IEC: 27001, 2006).

Mediante esta avaliação fica evidente a importância de um bom auxílio do profissional de auditoria detectando falhas na segurança ou na integridade dos dados e informações avaliadas.

[1] Termo usado para programadores avançados com intuito de danificar determinado software, derrubar ou desfigurar uma página na Internet ou roubar informações confidenciais para uso em benefício próprio (AMARIZ, 2008).

Vale lembrar e ressaltar que o auditor de sistemas necessita de um treinamento e conhecimento prévio da segurança envolvida na TI. Necessita também trabalhar em conjunto com profissionais da área de segurança da informação para uma boa avaliação e detecção dos riscos envolvidos (IMONIANA, 2008).

3. AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Para aprofundar os conhecimentos sobre este assunto se faz necessário conhecer também os campos de atuação da auditoria e do profissional auditor. Assim é possível direcionar o foco da auditoria para uma possível organização pública ou privada que necessita dos processos da auditoria.

Para que as avaliações da auditoria sejam concluídas de forma eficiente, é necessário um bom gerenciamento do tempo e de outros recursos para a aplicação dos processos de auditoria. A equipe de auditoria esculpe um escopo de auditoria, estuda a natureza da organização e demonstra estar confiante e decisiva para o início dos trabalhos (NETO; SOLONCA, 2007).

A organização que será auditada espera que a auditoria siga alguns princípios para exercer esta função com profissionalismo e confiança. Neste capítulo veremos os conceitos da auditoria de SI, alguns dos padrões e códigos de ética que o profissional auditor deverá seguir como guia, as dificuldades encontradas e como desenvolver uma equipe de auditoria com um estudo sobre o nível de aprendizado e sua respectiva função do profissional auditor.

3.1. Conceitos de auditoria e princípios básicos para sua execução

Para a melhoria dos processos e as atividades da organização, sempre houve a necessidade de guardar as informações em papel. Atualmente estas informações, em sua grande parte, estão sendo digitais ou digitalizados, porque houve um grande aumento da quantidade de informações devido o distanciamento dos negócios e dos módulos da organização e a facilidade de armazenamento e transferência.

A informação digitalizada traz de certa forma comodidade e organização de espaço e trabalho, para a busca e armazenamento em arquivos de grande porte. Com a ocorrência destes avanços nos sistemas de informação, existe a necessidade de auditar os processamentos que envolvem a criação da informação e dos e sistemas de gerenciamento de banco de dados (SGBD) que acumulam e armazenam os dados e as informações digitalizados, com foco na confiabilidade dos dados digitais prevenindo o desvio de informações (IMONIANA, 2013).

A auditoria é dividida em interna e externa. A primeira é conduzida pela própria organização auditada, para intenções particulares desta, como analisar mais detalhadamente determinados módulos que precisam demonstrar eficiência ou aperfeiçoamento.

A externa é conduzida por auditores que objetivam o interesse direto e impactante para a organização. Como aquelas empresas de capital aberto (SA), precisam mostrar o máximo de transparência em seus valores e planos estratégicos ou por organizações governamentais que controlam a regulamentação ou para conseguir uma certificação em associações (ABNT NBR ISO 9000, 2005).

Outro assunto importante a ser relatado nesta obra são os princípios básicos para a execução da auditoria. Os princípios que ajudam o auditor a conseguir credibilidade e confiança por parte do auditado.

Começaremos com o princípio da integridade. O auditor realiza sua função com honestidade e em conformidade com as leis demonstrando assim sua competência. Outro princípio importante a segundo é o da apresentação justa, que exige do auditor demonstrar seu trabalho com precisão e exatidão.

O cuidado profissional é outro princípio que dever ser observado pelo auditor. Ele deve apresentar-se ou intervir em julgamentos de auditoria com devida cautela, comprovando as suas ações e seus argumentos. O princípio da confidencialidade alerta o auditor a usar e armazenar de forma correta e em local seguro os dados confidenciais da organização.

Outro importante é o princípio da independência. O auditor será independente da organização auditada, mesmo se tratando de uma auditoria interna, eliminando qualquer causa de interesse e nunca perder o foco em seus objetivos. O último princípio orienta o auditor a utilizar e apresentar seus argumentos baseados em provas, coletando amostras confiáveis para documentação e comprovação (ABNT NBR ISO19001, 2012).

O auditor de sistemas, em seu trabalho, deverá elicitar[2] em sua análise todos os itens que abrangem os sistemas de tecnologia da informação, documentando e reportando qual será o seu impacto e riscos traçando níveis de gravidade e focalizando na importância do acompanhamento para seus superiores (IMONIANA, 2008).

3.2. Diretrizes e para a aplicação da auditoria de sistemas de informação

Em certas ocasiões, o profissional que exerce a função de auditor de sistemas, não é considerado pela organização e pela equipe de auditoria em geral como uma profissão especializada da área.

São muitas as dificuldades que o auditor de sistemas de informação encontra como a falta de leis que regulamentam sua carreira profissional e pela falta de independência. Muitas vezes o auditor é confundido como parte de uma auditoria geral das organizações, junto com todos os processos de auditoria e não uma especialização ou uma parte importante que audita e usa a TI em todos os processos da auditoria (IMONIANA, 2013).

Para exercer a profissão de auditor de sistemas e ser profissionalmente reconhecido como uma profissão importante e destacada das demais auditorias, apresentando um diferencial de valor, o profissional auditor deverá seguir os padrões adotados pela equipe de auditoria com base na ética e desempenho profissional.

Um importante comitê internacional responsável é a Associação dos Auditores de Sistemas e Controle (ISACA). Este comitê estabeleceu um código de ética para os auditores, orientando uma boa conduta profissional e estabelecendo para os auditores e para os responsáveis da empresa auditada, padrões, diretrizes e procedimentos (IMONIANA, 2013).

Os padrões visam às regras que um auditor tem de aceitar e cumprir no exercício de sua função. Normas de conduta são estipuladas com o intuito de todas

[2] Levantar dados e informações sobre determinado assunto, estudo ou trabalho e documenta-los.

as partes envolvidas, gerentes e equipes de auditoria, cumprir com zelo de acordo com as melhores práticas.

Os auditores participantes deste comitê que não estiverem em concordância coma as normas estipuladas, sofrerá investigação de conduta e poderá ser punido com ações disciplinares.

As diretrizes especificam a conduta que o auditor levará para acatar as normas e padrões da auditoria de SI. Já os procedimentos são técnicas adicionais que o auditor poderá adotar no exercício da auditoria. Ser competente nas tarefas desempenhadas e manter informada as partes envolvidas no processo (ISACA, 2004).

Para que o auditor de SI seja devidamente respeitado em sua função deverá acatar todos os padrões de auditoria estabelecidos pelo ISACA. É importante ressaltar ainda a devida importância que este comitê traz para a formação profissional do auditor.

O profissional que faz uso da responsabilidade, da independência profissional, da ética, do estudo detalhado do comportamento e aplicação de habilidades, planeja suas tarefas, exerce seu ofício com responsabilidade e integridade, requisitando e avaliando as atividades anteriores, certamente será bem sucedido e reconhecido no exercício da função (IMONIANA, 2013).

3.3. Procedimentos para a execução da auditoria de sistemas

O principal objetivo desta seção é relatar a as ações e os procedimentos de auditoria com base em normas e padrões já estabelecidos e organizados, avaliando as competências do profissional auditor e de toda a equipe de auditoria e, até mesmo, fornecendo a este profissional indicação para criar suas próprias condições de trabalho, evitando a formação e execução de uma auditoria mal sucedida que não atinge os objetivos e prejudica o sistema da organização (ARIMA, 1993).

O primeiro passo da auditoria é traçar os objetivos do programa de auditoria, definindo as finalidades e o tempo que a equipe utilizará para completar este programa. A equipe de auditoria não deve atrapalhar os processos corriqueiros da

organização, como as entradas, o processamento e as saídas. Alguns deles são de grande importância para o auditado, por isso, não podem ser interrompidos e cabe ao auditor de sistemas detectar qual a melhor forma de abordagem (ABNT NBR 19011, 2012).

Após traçar os objetivos a equipe os põe em prática com atenção. O foco determinante do sucesso é a politica da organização que não pode ser violada. A equipe traça a direção da auditoria, os requisitos, as necessidades e os riscos para definir um objetivo ou vários na organização.

A próxima fase é definir os papéis e responsabilidades de cada membro da equipe. Definir o líder que será responsável pelo alcance do programa, os objetivos, o escopo, identificando e avaliando os riscos como, avaliar os recursos disponíveis, o tempo ou a segurança dos controles, a disponibilidade e a qualificação da equipe e exemplo de métodos eficazes de auditoria (ABNT NBR 19011, 2012).

O auditor responsável traça o planejamento junto com sua equipe cria o escopo da auditoria, definido em reuniões. O escopo da auditoria serve para descrever os objetivos formais, os sistemas e as pessoas que serão auditados. Define as ferramentas que serão usadas para a coleta de dados e defini os controles que apresentam riscos para a organização e para a auditoria (IMONIANA, 2013).

Também são definidas nesta fase as competências dos membros da equipe de acordo com o conhecimento e habilidades de cada membro. Se o gerente de auditoria não encontrar na equipe um membro competente para determinada função de auditoria, ele nomeia especialista para auxiliar os membros da equipe, porém, este não tem a função de auditor (ABNT NBR 19011, 2012).

O gerente de auditoria também define os responsáveis por liderar as equipes o que não pode ser feito depois do início a auditoria. Ele gerencia os resultados expondo análises críticas e acompanha monitoramento detalhadamente os acontecimentos, avaliando os fatores que podem mudar os rumos da auditoria como, mudanças de leis, constatações negativas ou positivas de auditoria e muitas outras mudanças que podem ocorrer no foco da auditoria.

Na última fase cabe ao responsável pela equipe analisar criticamente, apontando melhorias e falhas no programa de auditoria e verificando se todos os objetivos foram atingidos. Convém registrar os fatores de sucesso para aplicar em auditorias futuras e, aprendendo com os erros, procurando evita-los da próxima vez, criando medidas de contenção a erros e/ou novas medidas de abordagem (ABNT NBR 19011, 2012).

3.3.1. Etapas que podem ser seguidas para execução da auditoria

Estudaremos o desenvolvimento das etapas de auditoria de sistemas. Abordaremos sete fases para os processos da aplicação de auditoria de SI em uma organização, que pode ser usada como metodologia de trabalho e apresentaremos um fluxograma para auxiliar o entendimento das fases do processo. A intenção não é obrigar o auditor a seguir todos os passos, mas expor uma metodologia de exemplo que pode ser adaptada de acordo com a organização auditada (ARIMA,1993).

O fluxograma representa um sistema e seus processos graficamente. Quando as partes envolvidas no processo que ele representa a observam, passam a compreender facilmente, permitindo a completa visualização dos processos sem se preocupar com assuntos mais detalhados. Neste estudo, visa aprofundar o conhecimento das etapas padronizadas pela equipe de auditoria para exercê-la na organização auditada, na maioria das vezes aplicadas por auditores de sistemas experientes (SILVA, 2011).

Todos os símbolos apresentam uma legenda para o entendimento das operações. Foi utilizado o programa de construção de diagramas e fluxo de dados Bizage Modeler© versão 2.4.0.8, para a construção do fluxograma. O símbolo a demonstrado a seguir indica o início das operações, representado pela cor verde, e fim demonstrado pela cor vermelha:

Figura 2 – Símbolo início do processamento. Fonte: (SILVA, 2012).

O símbolo a seguir indica o processamento dos dados e foi representada pela legenda explicando a função processamento:

Figura 3 – Símbolo do processamento de dados e informações. Fonte: (SILVA, 2012).

As setas representam a direção do fluxo dos processos. A seguir será demonstrado o fluxograma com todos os passos do processamento de auditoria de SI com ênfase nas fases de processamento:

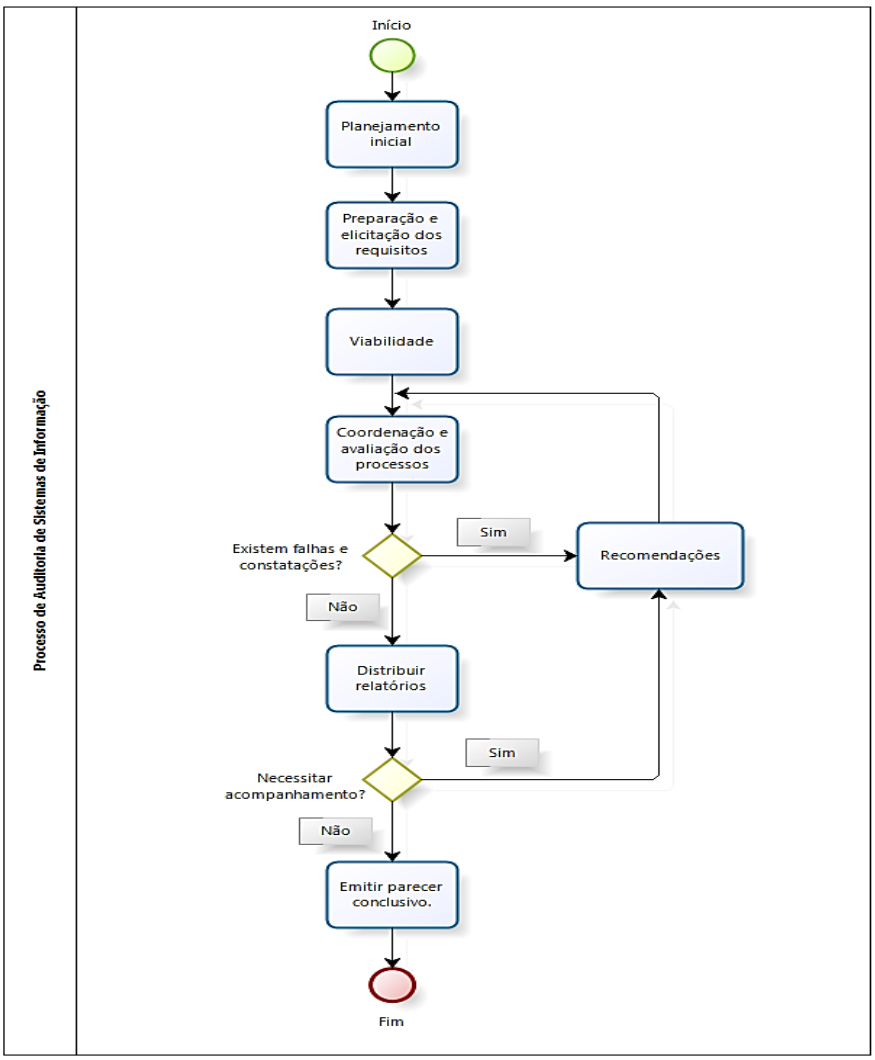

Figura 4 – Processo de Auditoria de SI. Fonte: (ABNT NBR 19012, 2012).

A primeira fase é o ‘planejamento inicial’. Ele acontece quando o líder da equipe é definido como responsável pela abertura dos processos e as demais

atividades. O primeiro contato com o auditado pode ser formal ou informal e sempre será executado pelo líder da equipe e posteriormente acompanhado pelos demais membros da equipe.

Na segunda fase dos processos, ‘preparação e elicitação’, é estabelecida a comunicação com o auditado por meio de entrevistas ou plebiscitos para destacar as informações iniciais. Estas reuniões tem a função de conscientização sobre a importância da auditoria, o tempo necessário para realizar os trabalhos, apresentar a equipe, determinar as normas, e explicar para o auditado a importância da contribuição dos requisitos informados por ele para satisfazer as necessidades da auditoria (ABNT NBR 19011, 2012).

Na terceira fase será determinada a ‘viabilidade’ da auditoria de SI na organização que, responderá aos seguintes fatores:

I. As Informações levantadas pela equipe ou disponibilizadas pelo auditado são suficientes para a continuação dos processos? (disponibilidade de informações);

II. Existe a cooperação do auditado em diversos fatores, ou seja, como irá cooperar e quando poderá cooperar? (integridade das informações);

III. O tempo necessário até a conclusão dos trabalhos e os recursos disponíveis é suficiente para o sucesso da auditoria? (planejamento do tempo e recursos).

A quarta fase será preparar as atividades de ‘coordenação e avaliação’ dos processos, de acordo com o ambiente e as pessoas que serão auditados, definindo o escopo, preparando um plano de auditoria, definindo as técnicas de amostragem que se fundamentarão em entrevistas individuais ou coletivas, além de, definir a formação da equipe e se conscientizar dos riscos gerados pela auditoria (ABNT NBR 19011, 2012).

Ainda nesta fase são detalhados os responsáveis para auditar os processos específicos, definindo as atividades, as funções e localidades. O líder coordena as

instruções, as atribuições de trabalho, de acordo com o progresso da auditoria sempre em cumprimento dos objetivos. Recolhe a documentação para avaliar e analisar as informações relacionadas às tarefas de auditoria e destaca as áreas críticas da auditoria. Estes documentos podem conter listas e formulários de verificação e os planos de amostragem utilizados que devem ser guardados adequadamente por conterem informações confidenciais (ABNT NBR 19011, 2012).

Na quinta fase o líder precisa analisar se existem falhas e constatações importantes. Em seguida distribui ‘recomendações’ dos processos de auditoria. Para isso, o líder marca uma reunião para esclarecer as partes envolvidas sobre o plano de auditoria e pode afirmar que todas as atividades podem ser realizadas. Ele obtém confirmação que todas as atividades estão em concordância com o plano de auditoria, com a intenção de continuar ou suspender os processos para uma avaliação mais detalhada, de acordo com o que foi relatado na documentação.

A equipe de auditoria se reúne formalmente para a troca de informações. A finalidade destas reuniões é a descobrir o progresso do trabalho ou se comunicar com entidades regulamentadoras conforme necessário. O líder da auditoria poderá utilizar da ajuda de guias que conhecem os módulos da organização para a coleta de informações ou esclarecimentos pertinentes, desde que, estes não interfiram nos processos de auditoria e podem até servir de testemunhas para o auditado (ABNT NBR 19011, 2012).

A equipe gera comprovações de conformidade ou não conformidade com os critérios de auditoria podem ser classificadas e registradas. Na conclusão a auditoria identifica os pontos de abrangência e eficácia junto com o cumprimento dos objetivos de escopo. Indica recomendações de melhorias e atividades a serem realizadas. É feita a reunião de encerramento com todas as partes envolvidas utilizando linguagem compreensível, explicando os métodos de amostragem, o manuseio da informação auditada e as atividades pós-auditoria.

A sexta fase dos processos de auditoria é distribuído os relatórios com toda a documentação sobre as conclusões de auditoria evitando a entrega com atrasos. Se houver atrasos todas as partes serão devidamente comunicadas. Os documentos de

trabalho são guardados com segurança ou destruídos. Se houver solicitação para revelação dos documentos, todas as partes serão informadas sobre o ocorrido. Os responsáveis podem exigir da auditoria um acompanhamento dos módulos que necessitam de mais atenção ou fogem do escopo da auditoria. Se isto ocorrer, a auditoria renova as constatações e avaliações ou um novo processo de auditoria ocorre.

Na sétima fase o auditor emite um parecer conclusivo da auditoria e propõe soluções. A equipe pode ser requisitada pelo auditado a acompanhar os processos de melhorias, ou o auditado recorre à auditoria subsequente (ABNT NBR 19011, 2012).

3.4. Desenvolvendo uma equipe de auditoria

Para desenvolver uma equipe de auditoria é necessário que profissionais menos experientes assistam os trabalhos desenvolvidos por uma equipe mais experiente, principalmente quando esta última possui conhecimentos adicionais como formação nos estudos de Análise de Sistemas e Ciências da Computação.

Com o decorrer do tempo e da carreira, as evoluções na TI influenciam diretamente na profissão do auditor de sistemas. Estas evoluções deixam o trabalho do auditor e do analista de sistemas mais complexo, obrigando estes profissionais a se atualizarem no mercado de trabalho.

Esta junção de profissionais mais experientes com menos experientes inicia-se com uma abordagem aos sistemas da informação e a TI utilizando o computador para auditar e auditando ao redor do computador efetuando simulações e técnicas de auditoria (IMONIANA, 2013).

Para compor uma boa equipe é necessário que o auditor em treinamento aprenda conceitos sobre os processos de gerenciamento e controle de uma organização, aprenda também os conceitos sobre os sistemas de informação gerenciais, além de se adaptar com algumas ferramentas para auxílio da auditoria ou até mesmo, quando conseguir uma boa experiência, projetar uma ferramenta personalizada.

Profissionais analistas de sistemas podem passar por um processo de treinamento para exercerem a prática da auditoria de sistemas, pois, conhecem bem os sistemas de informação e suas tecnologias. De acordo com seu grau de experiência, podem ainda estimular seu conhecimento desenvolvendo novas metodologias de abordagem como novas ferramentas de busca de requisitos para auxílio na auditoria (IMONIANA, 2013).

Porém, ainda existe certa dificuldade de adaptação a novas técnicas de trabalho, devido a conhecimentos e paradigmas de estudo e hábitos seguidos por estes profissionais, causando uma barreira para novas maneiras de aplicações. Se não houver uma atualização dos estudos e práticas, sem abordar as bases de auditorias de sucesso - *know-how*[3] - haverá um baixo desempenho com o propósito, sem contar com o tempo necessário para um desenvolver bom senso crítico e comprometimento com a profissão.

3.4.1. Estudando a hierarquia da auditoria de sistemas da informação

As grandes equipes de auditoria procuram formandos da área de TI, criando programas de contratação e meios de treinamento como a criação da carreira de *trainee*[4]**,** e futuramente estes jovens contratados passam por diversos níveis de atuação até atingir o patamar da hierarquia e se tornam sócios (IMONIANA, 2013).

A experiência é adquirida no ato de exercer de forma gradativa os trabalhos de auditoria e/ou acompanhar o trabalho de outros auditores mais experientes. Participar de congressos da categoria e se aprofundar nos conhecimentos educacionais necessários para a profissão.

Os profissionais que possuem pouca ou nenhuma experiência em TI aprendem os conceitos de relacionados da área de TI, como arquiteturas de sistemas, entrada e saída de dados e informações, programação e outros conceitos pertinentes da área que não serão amplamente citados aqui (IMONIANA, 2013).

---

[3] Conhecimento desenvolvido e documentado por uma organização como um resultado da aprendizagem e da experiência adquirida (PAPADAKIS, 2013).

[4] Termo em inglês que significa colaborador em treinamento (PAPADAKIS, 2013).

Os profissionais que já vem com uma bagagem de conceitos, estes citados no parágrafo anterior, necessitarão da revisão dos conhecimentos dos controles gerais da organização, os princípios e práticas de auditoria, as estratégias e os padrões especialistas e muitos outros que atendem a áreas específicas e seus métodos.

Os cursos necessários para o aprimoramento das técnicas podem ser ministrados por organizações de auditoria independente com boa experiência seguindo os níveis de hierarquia da carreira e de acordo com a experiência do profissional a ser treinado.

Ao longo da experiência adquirida pelo ofício, sua carreira e suas expectativas de carreira podem ser representadas por cinco níveis hierárquicos. Faremos uma breve descrição de todos os cinco: *trainee*, assistente, seniores e supervisores, gerentes e sócio de auditoria conforme é mostrado na figura abaixo (IMONIANA, 2008).

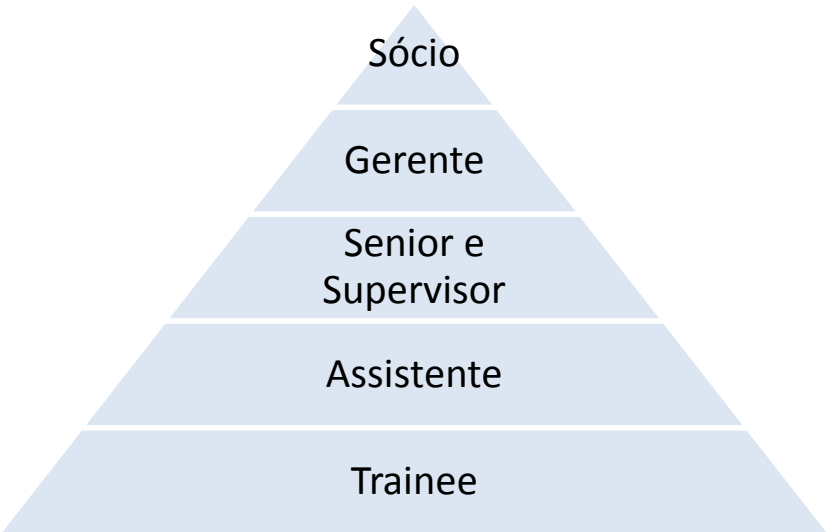

Figura 5 – Associação da hierarquia da carreira de auditor de TI. Fonte: (IMONIANA, 2013).

No nível de base, ou *trainee*, é estudada a TI em paralelo com os princípios de auditoria. Estudam também sobre as formas de processamento, a arquitetura de computadores, os sistemas operacionais e as linguagens de programação no campo de trabalho.

No nível *assistente*, o profissional aprende métodos para *construção* de programas, assim como distinguir as ferramentas de softwares utilizadas na auditoria generalistas e especialistas. Aprende conceitos mais aprofundados de controle de processamento, ciclo de vida do software, elicitação, implementação, protótipos, testes e conceitos sobre uso de ferramentas CASE (*Computer Aided Software Engineering*) e na criação de trilhas de auditoria (IMONIANA, 2013).

No nível *sênior ou supervisor*, o auditor aprende conceitos mais elaborados sobre a auditoria e segurança da TI. Aprende conceitos sobre barreiras físicas e lógicas como, *firewall*[5] e demais softwares para o controle de acesso e assinaturas digitais. Ele constrói e aprova documentos e propõe a melhoria do ambiente auditado.

No nível *gerente,* o profissional conclui os trabalhos e as necessidades da equipe de auditoria. Ele necessita de experiência de suas atividades em equipe, pois é responsável pela tomada de decisões da sua equipe (IMONIANA, 2008).

No nível sócio o profissional se torna conselheiro para os demais, visto que já tem um conhecimento de todos os outros níveis. Sua atitude profissional é julgada pelo relacionamento com seus clientes, pela verdade e certeza de suas opiniões, e no auxílio do aconselhamento estratégico dos seus clientes.

[5] Termo em inglês para um programa ou dispositivo que verifica informações recebidas e enviadas pela rede (WINDOWS, 2013).

4. TÉCNICAS E FERRAMENTAS NECESSÁRIAS PARA A AUDITORIA DE TECNOLOGIA DE INFORMAÇÃO.

É importante resgatarmos neste trabalho, a importância do estudo sobre a utilização de Técnicas de Auditoria Assistidas por Computador (TAAC) auxiliando o trabalho do auditor para que consiga compreender toda a área auditada e especificar os controles de auditoria que serão feitos não só auditando o computador como utilizando para automatizar os processos de auditoria (TERUEL, 2010).

Os trabalhos que o auditor fará com o apoio de ferramentas, podem auxiliar o auditor a reduzir esforço e tempo de execução dos processos. Também poderá ser ampliada a cobertura dos módulos da organização que contém uma grande quantidade de informações a serem analisadas e coletadas (IMONIANA, 2013).

Neste capítulo estudaremos sobre as técnicas de auditoria e estudaremos as características de algumas ferramentas de auditoria. O principal objetivo é mostrar para o leitor/auditor como a auditoria pode ser amplamente usada alinhada a TI da organização, já que a TI também precisa ser auditada e confiável.

4.1. Técnicas de auditoria

O estudo detalhado a seguir das técnicas de auditoria tem como objetivo ressaltar a importância de uso do computador no auxilio do profissional auditor, para ter mais eficiência em seu trabalho e mais, economizando tempo e retrabalho em suas atividades, principalmente quando os sistemas se tornam cada vez mais informatizados (IMONIANA, 2013).

As técnicas de auditoria visam o aperfeiçoamento da prestação dos serviços do auditor. Algumas relatam a eficiência de produtividade como a visão de planejamento e metas que o auditor aplica nos módulos mais importantes. A redução de custos onde o auditor decide qual melhor ferramenta para aquela função e qual será a extensão da sua portabilidade, permitindo que o auditor amplie seus relatórios.

As mais variadas formas e métodos de aplicação da auditoria podem ser chamados de técnicas de auditoria. Existe uma infinidade delas, porém

conheceremos as mais utilizadas. O auditor pode fazer uso de técnicas para aumentar a produtividade, no custo, na qualidade, no valor, auxiliando a gestão nas decisões importantes e globais da organização, para aumentar a reputação da corporação ou para aumentar os benefícios para o auditor reduzindo os riscos da auditoria.

A seguir veremos algumas técnicas de auditoria. Não podemos citar todas as técnicas porque nosso estudo seria imenso de acordo com a variedade de técnicas de auditoria de sistemas de informação disponíveis e as que estão surgindo e ainda não foram documentadas, ou ainda não foram utilizadas devido a paradigmas elaborados pelo profissional auditor que está acostumado a exercer determinado método de trabalho (IMONIANA, 2013).

4.1.1. Simulação paralela

A técnica simulação paralela consiste em desenvolver programas de computadores que aparentam ter as mesmas funções dos programas utilizados pelo auditado. Sua principal função é simular os processos de entrada de dados normais e localizar e analisar erros decorrentes desta função (MAGALHÃES, 2013).

As vantagens desta operação é que os programas operam em no ambiente e não precisam de tratamento para ser transportados e auditados em outro local. O auditor pode facilmente efetuar os testes pessoalmente e possuir um nível mais detalhado, porém a desvantagem fica evidente quando os testes são executados em uma porção dos dados e não em sua totalidade aumentando os custos com o uso de ferramentas personalizadas (IMONIANA, 2013).

4.1.2. Dados de teste

Esta técnica testa os dados de acesso de um controle qualquer. É simulada uma variedade de combinações e possibilidades para tentar o acesso a controles protegidos. O auditor testa os controles a partir de uma ferramenta geradora de dados, ou seja, um programa gera senhas repetidas. O auditor utiliza o programa nos ambientes controlados para detectar falhas de segurança.

Como vantagem qualquer pessoa pode manipular um gerador de senhas e combinações deste aspecto, não precisando ser um perito em informática, porém é difícil conseguir todas as combinações possíveis (IMONIANA, 2013).

4.1.3. Questionários

Com esta técnica o auditor elabora um conjunto de perguntas para levantar requisitos de verificação de um ponto de controle alinhando com os padrões de segurança física e lógica, obediências às normas e padrões, e muitos outros requisitos.

O questionário deverá obedecer a alguns critérios importantes como seguir as características do ponto de controle e a disponibilidade das pessoas envolvidas. O auditor deverá relacionar suas perguntas sobre a segurança em redes de computadores, acesso físico e lógico a áreas restritas, como a sala do servidor central da empresa, uso correto e eficiente dos sistemas computacionais e aplicativos (MAGALHÃES, 2013).

4.1.4. Visita *in loco*

A visita *in loco*[6] consiste em uma visita efetuada pelo auditor pessoalmente as instalações do ambiente auditado. Esta técnica poderá ser combinada, ou seja, efetuada em conjunto com outras técnicas de auditoria. Ela pode ser dependente da disponibilidade do auditado, porém, dependendo da gravidade e sensibilidade da auditoria, um especialista pode ser convocado e disponibilizado às reuniões, que pode participar como guia nas instalações e como entrevistado, podendo até mesmo ser testemunha da auditoria.

A principal função da visita *in loco* é a possibilidade de o auditor emitir relatórios analisando as fraquezas do ambiente, como falta de controle de acesso, anotar procedimentos manuais onde não pode ser utilizado o ambiente

[6] No local, pessoalmente (DICIONÁRIO ...2013).

computadorizado, analisando rotinas de *backup*[7] verificando se estas rotinas seguem os padrões de controle (MAGALHÃES, 2013).

4.1.5. Análise do programa fonte

Na aplicação desta técnica, o auditor analisa visualmente o código-fonte de programas auditados. Foca sua atenção na versão do código para não cometer erros e analisando registros de versões. Ele ainda pode comparar o código-objeto gerado de um software específico em paralelo com o que executa a geração de código-objeto de um programa que esta sendo auditado e relatar os pontos de divergência.

O auditor que executar esta tarefa deverá ter conhecimentos de linguagem de programação avançada ou pode fazer uso de terceiros, como analistas de sistemas para auxiliar na comparação. O auditor verifica se o programador utilizou dos padrões mínimos necessários para construção das rotinas de programação, analisando ainda a estruturação dos programas definindo os níveis adequados (MAGALHÃES, 2013).

4.2. Estudo das ferramentas generalistas e especialistas

As ferramentas de auxílio à auditoria de sistemas de informação dividem-se em ferramentas generalistas e especialistas. As ferramentas generalistas são programas que abordam diversos controles e módulos da organização de uma só vez.

As vantagens das ferramentas generalistas são muitas, entre elas está o poder do processamento de dados e operações em conjunto com outros tipos de equipamentos e programas, podendo até mesmo, atingir outros módulos dos sistemas de uma só vez. Esta técnica auxilia as demais equipes de auditoria lançando diversos relatórios (IMONIANA, 2013).

As desvantagens desta técnica e uso desses procedimentos generalistas é que não mantém seu foco em um determinado problema, ou seja, avaliar mais

[7] Cópias de arquivos contidos em disco magnéticos, muitas vezes programas para acontecerem em determinado horário e frequência (DICIONÁRIO ...2013).

profundamente um conjunto de cálculos financeiros e contábeis, o que torna difícil a especialização do ambiente auditado.

As ferramentas de auxílio especialistas na maioria das vezes são desenvolvidas pelo próprio auditor ou pela equipe de auditoria ou por terceiros contratados por ele. Estas ferramentas especialistas são específicas para determinada função. Se estes forem devidamente documentados como ferramentas que obtiveram sucesso ou resultados satisfatórios nos processos de auditoria, o auditor poderá usar estas ferramentas com vantagens competitivas entre os demais concorrentes (IMONIANA, 2013).

As vantagens de se utilizar uma ferramenta especialista estão no aprofundamento da análise e observação onde ferramentas generalistas não conseguem atuar sendo obrigatoriamente substituídas.

Já as desvantagens abordam o custo de desenvolvimento destas ferramentas, o tempo necessário para desenvolvê-las, além de, serem difíceis de atualizar e acompanhar devido as constantes mudanças de programas e máquinas nas organizações, dificultando a portabilidade de uso em diversos clientes por usarem sistemas e módulos distintos (IMONIANA, 2013).

Seguirá um estudo mais detalhado das ferramentas generalistas não com propósito de comparação, mas com o propósito de descrição para auxiliar o auditor de sistemas a escolher a melhor ferramenta para determinado processo de auditoria.

4.2.1. Pentana

Ferramenta de auditoria desenvolvida no Reino Unido, em 1992, com o intuito de auxiliar auditores em todos os países do planeta. Esta ferramenta fornece quadros de monitoramento e avaliações de qualidade e desempenho da auditoria(PENTANA, 2013).

Oferece também suporte as tecnologias da Microsoft©. Promove integração dos ciclos de auditoria, desde o planejamento a avaliação de risco detalhada e testes de controle através de rastreamento de ações do comitê de auditoria. Em

ambientes com acesso a Internet, ela atualiza sem precisar da intervenção do usuário, porém, trabalha em ambientes sem conexão com a Internet normalmente.

Em 2002 a empresa lançou um programa de auditoria integrado a um sistema de gestão de risco chamado *Pentana Audit Work System* (PAWS) que tem como principal função organizar o planejamento anual da auditoria, ajudar na gestão de risco, formulação de relatórios e rastreamentos (PENTANA, 2013).

A imagem a seguir demonstra o mapa de riscos gerado pela ferramenta de auditoria PAWS com base na pontuação dos riscos estratégicos da organização:

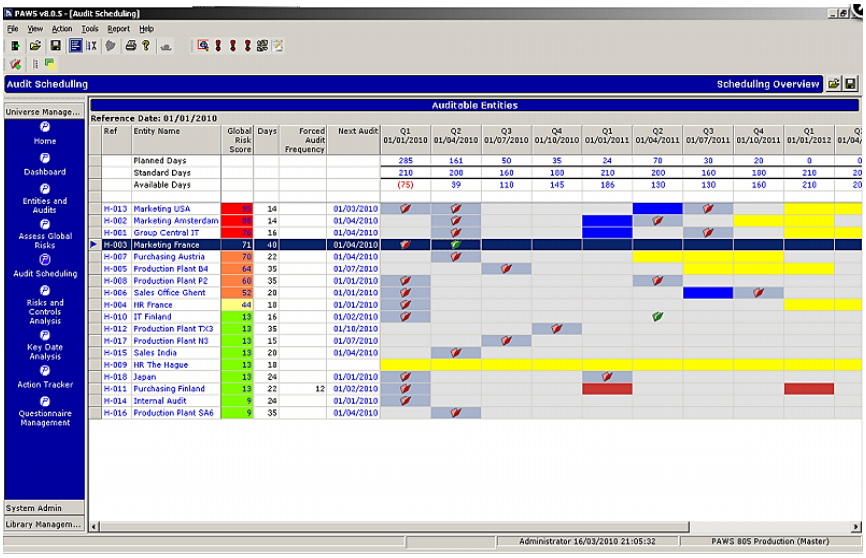

Figura 6 – Gerenciamento de riscos estratégicos em PAWS. Fonte: (SEPIA SOLUTIONS, 2013).

O planejamento demonstrado na figura acima disponibiliza informações detalhadas dos problemas que podem ocorrer de acordo com o mapeamento e pontuação dos riscos. A ferramenta comunica o gerente de auditoria o agendamento de uma solução para os problemas mais graves ou as soluções pendentes (SEPIA SOLUTIONS, 2013).

Atualmente ela foi sucedida pela ferramenta *Pentana Vision*, projetada em 2011, porém a empresa ainda presta suporte à ferramenta antecessora. A imagem a seguir demonstra a navegação das telas de gerenciamento da auditoria pela ferramenta *Pentana Vision* demonstrando estatísticas da auditoria:

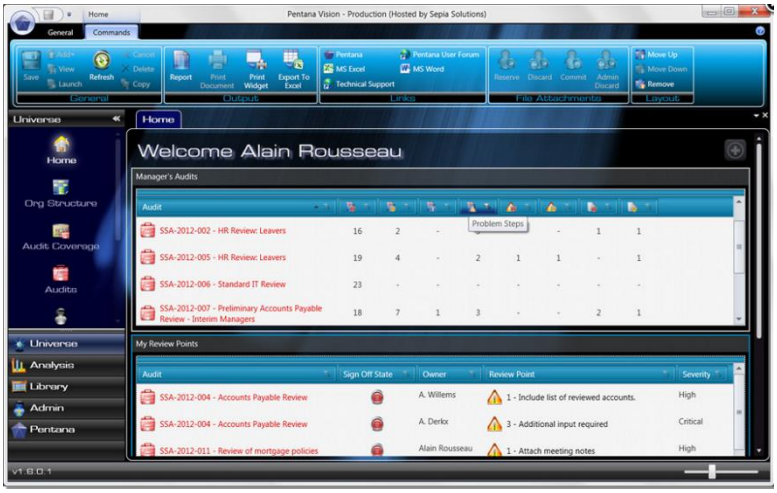

Figura 7 – Tela de gerenciamento da auditoria *Pentana Vision*. (SEPIA SOLUTIONS, 2013).

A tela acima apresenta soluções de gerenciamento da auditoria, com até dez telas de visualização mostrando entre elas as etapas dos processos (processo iniciado, parado, atrasado ou concluído), as descrições dos processos, os resultados, os responsáveis, etc. (SEPIA SOLUTIONS, 2013).

Todas as ferramentas da empresa Pentana trabalham em conformidade com a lei *Sarbanes-Oxley*[8] (SOx), desenvolvida nos Estados Unidos com a intenção de combater e punir os responsáveis por fraudes financeiras nas grandes organizações (PENTANA, 2013).

4.2.2. Interactive Data Extraction & Analisys (IDEA)

IDEA é uma ferramenta de auxílio para os processos de auditoria desenvolvido pela CaseWare, fundada em Toronto, Canadá em 1988. Distribuído em mais de 130 países, disponibiliza uma versão de demonstração e tutoriais explicativos em sua página de divulgação na Internet (IDEA, 2013).

A ferramenta IDEA disponibiliza para o auditor personalização e adaptação para empresas de grande, médio e pequeno porte. O usuário pode até mesmo personalizar a ferramenta caso encontre diferentes áreas de trabalho e necessite de ajustes funcionais para uma determinada área. Apresenta uma grande variedade de

[8] Lei criada em 30 de julho de 2002 com a intenção de combater fraudes contábeis aumento o valor e créditos dos investidores as organizações (MONITOR ...2013).

bibliotecas de auxílio e suporte. Cria rastreamento e controles de risco e imprime relatórios digitais sobre os controles. (IDEA, 2013).

O programa IDEA é uma ferramenta para computador pessoal baseada na pesquisa de arquivos, orientada para o uso de auditores, contadores, consultores, fiscais e profissionais de segurança da informação. Pode analisar e manipular, extrair amostras ou arquivos de dados de qualquer fonte - de computadores de grande porte a computadores pessoais. (BRACCO, 2013)

Podendo até ser comparado a um software de planilha como MS Excel®, diferente apenas pelo fato de ser projetado para auditores e não ter limite de linhas para a extração de dados cumprindo com os objetivos da auditoria. Entre suas funções para auxílio da auditoria estão:

I. Criação de registros de todas as operações e alterações em um SGBD identificando o acesso do usuário pelos identificadores de acesso;

II. Importa ou exporta dados em diferentes formatos;

III. Geração de gráficos para visualização;

IV. Obtenção de amostras utilizando diferentes técnicas de amostragem.

O programa IDEA possui sua própria linguagem de programação chamada IDEAScript, compatível com MS Visual Basic®. A linguagem de programação permite a gravação de etapas e possui um explorador de arquivos permitindo a criação de pastas e organização dos arquivos de acordo com os departamentos do auditado.

Utilizar o IDEA traz benefícios para o auditor na detecção de investigação de fraude, como lavagem de dinheiro, auditorias e investigações especiais utilizado mais comumente nas áreas financeiras efetuando cruzamento de informações ou efetuando cálculos específicos. Pode ser utilizado com amostras e destas tirar conclusões ou prever resultados financeiros.

4.2.3. Audit Command Language (ACL)

ACL é uma empresa de desenvolvimento de ferramentas de auditoria e auxílio em gestão fundada no Canadá. Ela desenvolve ferramentas para análise de dados como a ACL *Data Analysis* que pode ser aplicada a um único auditor, ajudando na detecção de falhas, analisar rapidamente um banco de dados, ou a uma equipe de auditoria, conduzindo um repositório centralizado e compartilhado entre os membros, além de programar os horários de extração de dados garantindo a disponibilidade dos dados (ACL, 2013).

Uma das ferramentas da empresa ACL pode ser usada nas atividades de Governança, Risco e Conformidade (GRC) de uma organização por auditores especializados nesta área. Denominada ACL GRC organiza os trabalhos separando e organizando o foco de todas as partes envolvidas. A figura a seguir demonstra a tela da ferramenta na parte do gerenciamento do risco, auxiliando a auditoria de risco, executivos e responsáveis pela conformidade dos investimentos e processos.

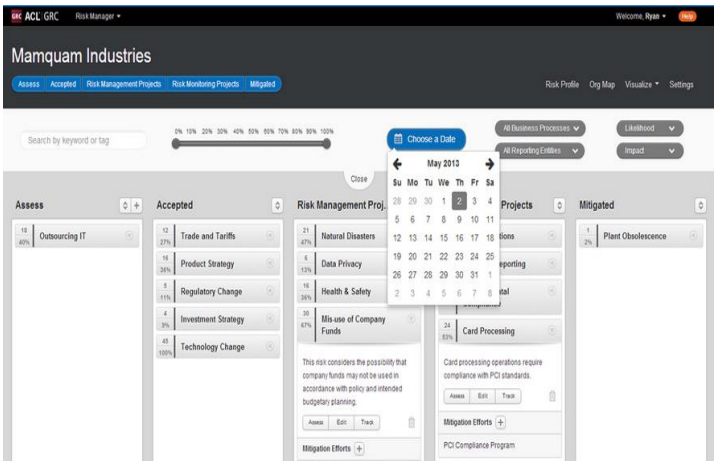

Figura 8 – Gerenciamento do risco em ACL GRC. Fonte: (ACL, 2013).

O programa ACL GRC também é desenvolvido para acompanhar o gerenciamento de recursos de auditoria, gerenciar projetos e ajudar no planejamento da auditoria oferecendo portabilidade com dispositivos móveis em ambiente de rede. A figura a seguir demonstra uma das fotos de tela do programa na função de gerenciamento de projetos (ACL, 2013):

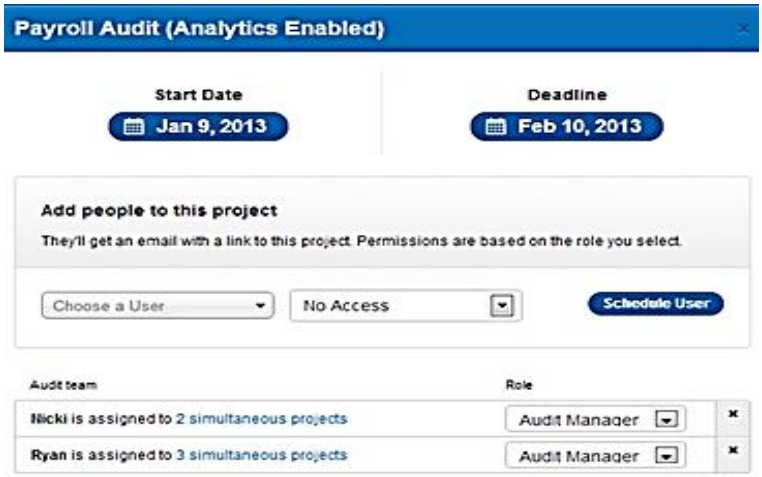

Figura 9 – Gerenciamento de projetos em ACL GRC. Fonte: (ACL, 2013).

Finalizando o estudo sobre esta ferramenta, ACL GRC aborda o gerenciamento de resultados da auditoria apontando itens que precisam de revisão ou apresentaram problemas específicos identificados nos relatórios de conclusão da auditoria, com a atenção voltada aos riscos mais importantes comunicando os responsáveis pelas situações. Abaixo analisamos uma foto de tela que mostra os itens que precisam de revisão, identificando os responsáveis, definindo prioridades, etc. (ACL, 2013):

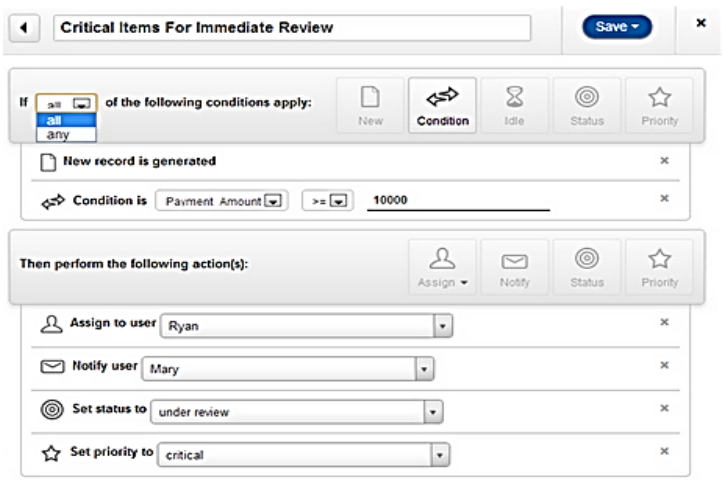

Figura 10 – Gerenciamento de resultados em ACL GRC. Fonte: (ACL, 2013).

4.2.4. Magique Galileo

Magique Galileo é um programa de auditoria baseada em risco, desenvolvido na linguagem Microsoft ASP.NET®. É utilizado pela equipe de auditoria interna para análise de registros, avaliações e gerenciamento de riscos (MAGIQUE ...2012).

Magique é um programa de gerenciamento de riscos que analisa e mantém registros de riscos e os avalia por módulos e entidades de acordo com as necessidades da organização e suas regulamentações, classifica e pontua os riscos. Separa os riscos que precisam de mais atenuação, gera mapas de calor, como demonstrado na figura abaixo retirada do site do fabricante:

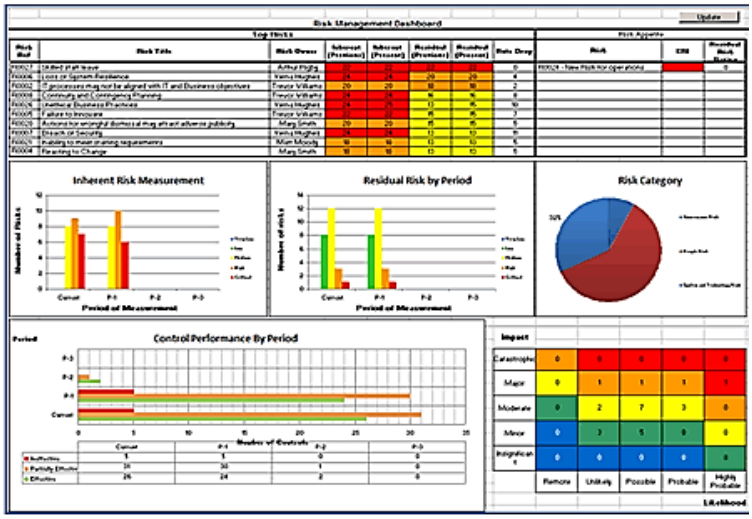

Figura 11 – Gerenciamento de riscos. Fonte: (MAGIQUE ...2012).

Com esta ferramenta é possível a geração de relatórios on-line para todas as partes envolvidas, além de geração de questionários e análises de respostas, determina pontos de vista e verifica conformidade com os regulamentos internos e externos da organização.

Galileo é uma ferramenta de auditoria especializada no gerenciamento de auditoria de sistemas, que pode ser usado sem a ferramenta Magique de acordo com a estratégia da empresa. Seu foco é na priorização da auditoria, trabalhando de acordo com as necessidades do auditor.

Com ela pode planejar as rotinas de auditoria e avaliação de recursos viabilizando a garantia de cobertura. É um grande gerador de relatórios anuais, analisando conformidades dos objetivos da auditoria com os planejamentos da auditoria, acompanhando e mostrando se os objetivos específicos estão sendo alcançados.

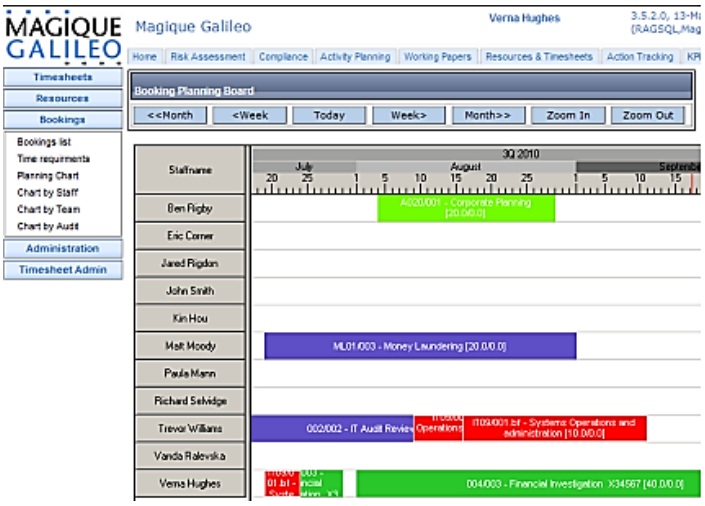

Figura 12 – Gerenciamento de recursos. Fonte: (MAGIQUE ...2012).

A figura demonstrada acima retrata uma foto de interface da ferramenta Galileo que demonstra o gerenciamento de recursos de auditoria de SI como, gestão de equipe e funcionalidades, tempo e atividades de cada membro, a partir de gráficos de Gantt[9].

A ferramenta Galileo exporta os papéis de trabalho ou relatórios funcionando em interação com as ferramentas do pacote MS Office®. Funciona como uma biblioteca de gerenciamento de relatórios de auditoria podendo trabalhar *on-line* e *off-line*. Sua ligação com o Magique resulta na geração de documentos de controles e gerenciamento de riscos. Muitas outras soluções de auditoria podem ser encontradas no site do fabricante.

[9] Ferramenta de gerenciamento de recursos, pessoas e tempo. Torna visível uma linha de tempo de execução de determinado projeto, que visa demonstrar a porcentagem do trabalho concluída, gerar relatórios de atraso de tarefas e o responsável pelas tarefas (SIMÕES, 2013).

4.2.5. SE AUDIT

A SE (SOFTEXPERT) é uma empresa de desenvolvimento de ferramentas de auditoria fundada em 1995. Veremos as funções do SE Audit, uma de suas ferramentas. Esta realiza o gerenciamento de todas as etapas do processo de auditoria, desde o planejamento e aprovação, até o monitoramento, seja ela interna, de fornecedores e clientes, e/ou de organismos certificadores (SOFTEXPERT, 2013).

O SE Audit é um sistema voltado para a rede, multiusuário e multidepartamental, que incorpora ferramentas de organização, classificação e pesquisa. Disponibiliza diversas funcionalidades como cadastro de requisitos de auditorias, com dicas que podem ser impressas e utilizadas pelos auditores durante o processo de auditoria, cadastro de critérios de auditoria, cadastro de clientes e organizações certificadoras que realizarão auditorias de primeira e segunda parte, registro de processos, registro de áreas/departamentos e pessoas que serão auditadas, através de interface com o SE *Process.*

A figura abaixo se refere à tecnologia de trabalho em equipe que a ferramenta proporciona junto às etapas do processo de auditoria:

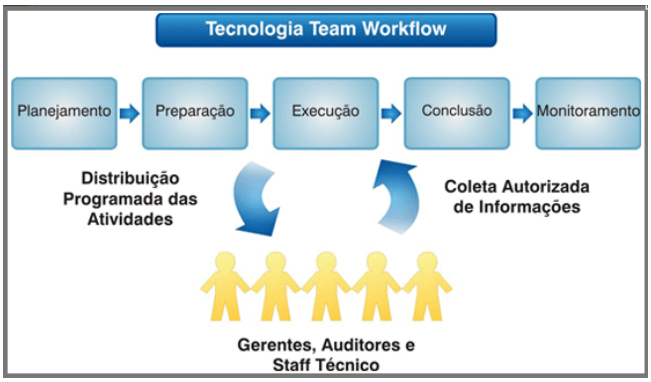

Figura 13 – Processos de auditoria e trabalho em equipe. Fonte: (SOFTEXPERT, 2013).

Também proporciona o trabalho em equipe, através de um prático mecanismo de controle de pendências, que notifica via e-mail, no momento certo, aos responsáveis por atividades pendentes, exibe estas pendências e autoriza o registro das assinaturas eletrônicas e demais informações aplicáveis a cada etapa do

processo. Este mecanismo assegura a agilidade e o compromisso com o cumprimento dos prazos em todas as etapas do processo de auditoria (SOFTEXPERT, 2013).

A foto de tela a seguir mostra a interface do programa e exibição de alguns critérios e certificações adotados pela SE Audit:

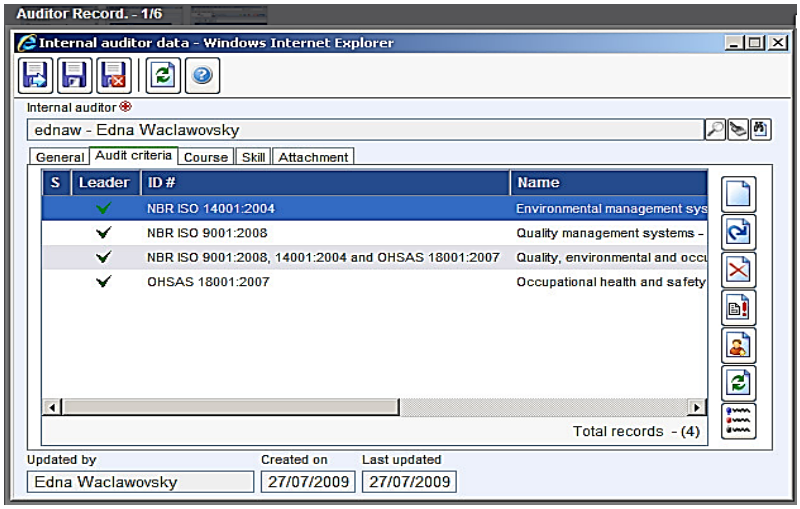

Figura 14 – Certificações adotadas no processo de auditoria. Fonte: (SOFTEXPERT, 2013).

A figura a seguir demonstra os ciclos de auditoria e o tempo determinado para cada ciclo e seus responsáveis:

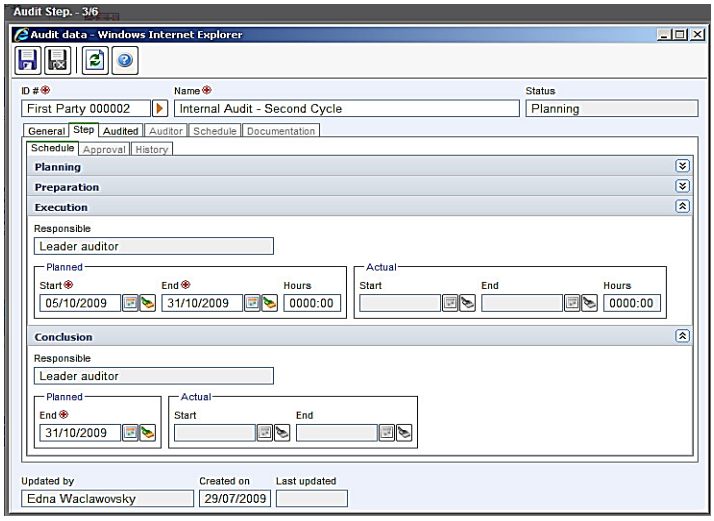

Figura 15 – Ciclos de processo de auditoria. Fonte: (SOFTEXPERT, 2013).

CONSIDERAÇÕES FINAIS

Antigamente a auditoria era feita por auditores que não usavam quase nenhuma tecnologia para auxiliá-lo, a não ser a forma de escrita, o papel e a caneta. Com o progresso da tecnologia de informação nas organizações, os auditores acrescentaram à tecnologia presente nas organizações de trabalho e governo, recursos de computação, como as ferramentas (programas de computador) para prestar assistência nos processos e nas conclusões de auditoria tornando o trabalho eficiente, prático e controlado.

A auditoria de SI evoluiu junto com a organização acompanhando os seus processos e a globalização das empresas. O auditor se especializou em sistemas de informação e tecnologia de informação, já que estes se tornaram requisitos básicos em uma organização estando presente em quase todas as empresas de pequeno, médio e grande porte.

Analisamos e conhecemos os sistemas de informação e a tecnologia de informação e qual o seu impacto e geração de valor para a organização. A segurança dos sistemas de informação é um fator de sucesso para a proteção dos ativos da organização, dados e informações, analisando as bases para a implantação dos sistemas de gerenciamento de segurança da informação, sempre alinhando os processos de segurança aos processos de auditoria, já que estes identificam os riscos e apontam soluções eficazes para os gestores.

O auditor de sistemas de informação, ao planejar a auditoria em uma organização pode fazer uso de diversas diretrizes e padrões de conduta. Do mesmo modo, pode fazer uso de ferramentas que auxiliam no processo de coleta de requisitos de auditoria, planejamento dos trabalhos, listagem de recursos, planejamento do tempo e divisão de papéis de auditoria.

Citamos algumas especificações e funcionalidades técnicas das cinco principais ferramentas existentes no mercado oferecendo um estudo detalhado sobre algumas delas, apresentando fotos de tela, abordando a interface com o usuário, esclarecendo para as partes interessadas, os níveis de avalição e soluções para os processos de auditoria de cada uma delas, não as comparando, mas,

procurando encontrar fatores decisivos para sua exata utilização na organização auditada.

Deixamos de lado muitas outras ferramentas importantes evitando que nosso estudo fosse interminável devido à diversidade de ferramentas e informações desta que podem ser encontradas para uso do auditor e de sua equipe. O que não impede ao leitor e/ou auditor de buscar mais estudos e recursos para alcançar seus objetivos.

O auditor pesquisa quais serão os padrões de amostragem de requisitos e como será planejada a auditoria. Quais módulos serão auditados, avalia a inserção de uma ferramenta mais generalista ou especialista, dependendo da necessidade aplicada nos processos de auditoria, buscando sempre a ferramenta mais conclusiva. Conclui assim, qual será a ferramenta que mais se adapta aos padrões da organização e da auditoria.

A auditoria, em geral, necessita de alinhamento e conformidade com os diversos padrões da organização e do governo. O auditor tem que ser constante aos motivos da auditoria, não aos seus motivos pessoais ou se deixar influenciar pelo auditado.

Ele também pode participar de comitês que regulam a categoria da profissão e tomar parte de assembleias e desenvolvimento de conceitos específicos em treinamentos com outras equipes de auditoria mais experientes. Pode fixar em sua meta, de acordo com a organização em que trabalha, planos de carreira subindo de posição em níveis de hierarquia de acordo com sua experiência até chegar a carreira de conselheiro em uma organização.

O auditor que não faz uso da ética profissional e dos padrões, executando os processos com exatidão e responsabilidades exigidas, perde sua credibilidade junto a seus responsáveis, que depositam nele sua confiança para agregar valor à empresa e investir em uma organização livre de fraudes.

O estudo dos processos de auditoria e das ferramentas objetivam auxiliar o auditor e o auditado. Algumas ferramentas de auditoria podem ser usadas em conjunto com outras ferramentas, ou seja, o auditor pode e fará uso de ferramentas

especialistas, desenvolvendo um programa que atinja um nível de auditoria mais específico ou contratando terceiros para que o faça, e/ou fazer uso de ferramentas mais generalistas atingindo diversos módulos dos sistemas.

Todas as técnicas e ferramentas de auditoria observadas aqui demonstraram atingir os objetivos da auditoria, detectando fraudes, analisando, comparando resultados e auxiliando o auditor em seu planejamento de auditoria.

Cabe ao auditor avaliar ainda os recursos necessários para a implantação das ferramentas e como será feita o acompanhamento e a utilização delas no ambiente real quando o auditor e sua equipe escolhem os modos da aplicação prática de suas técnicas e ferramentas.

REFERÊNCIAS

ACL. Choose the Ideal Data Analysis Solution for Your Organization. In:__**Data Analysis**. Disponível em: <http://www.acl.com/solutions/products/acl-analytics/>. Acesso em: 27 maio 2013. 10h11.

_____. Governance, Risk and Compliance. In:__**ACL GRC**. Disponível em: <http://www.acl.com/solutions/products/acl-grc/>. Acesso em: 03 jun 2013. 12h41.

AMARIZ, L. C. **Hackers e Cracker's.** (2008). Disponível em <http://www.infoescola.com/informatica/hackers-e-crackers/>. Acesso em: 27 nov. 2012. 22h12.

ARIMA, C. H. Etapas da Metodologia de Auditoria de Sistemas. In__ **Auditoria de Sistemas Computadorizados. Revista de Administração**, São Paulo, v. 28, n. 3, p.22-32, julho/setembro de 1993. Disponível em: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CEMQFjAA&url=http%3A%2F%2Fwww.rausp.usp.br%2Fdownload.asp%3Ffile%3D2803022.pdf&ei=L6yoUdTKFIaH0QGk6oC4CA&usg=AFQjCNGqP-n0NjqqVtczrG0T07hseoyRvQ&bvm=bv.47244034,d.dmQ>. Acesso em: 31 maio 2013. 11h06.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Citação**: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências Bibliográficas**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências Bibliográficas**: NBR-27001/mar. 2006. Rio de Janeiro: ABNT, 2006. p. 4-6.

_____. **Referências Bibliográficas**: NBR-9000/2005. Rio de Janeiro: ABNT, 2005. p.18.

_____. **Referências Bibliográficas**: NBR-19011/fev - 2012. Rio de Janeiro: ABNT, 2012. p.4-36.

BARROS, L. A. M. de. **Sistemas Abertos e Fechados.** (2011). Disponível em <http://www.monteirodebarros.net/sistemas-abertos-e-fechados.php>. Acesso em: 26 nov. 2012. 21h25.

BRACCO, T. **Características do software IDEA.** [mensagem pessoal] Mensagem recebida por: <sidnei.1984@yahoo.com.br>. em: 27 maio 2013. 14h07.

BUENO NETO, A.; SOLONCA, D. **Auditoria de Sistemas Informatizados**. 3ª ed. rev. e atual. Palhoça: Unisul Virtual, 2007.

DAWEL, G.. **Segurança da Informação Nas Empresas**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2005.

DEGASPERI JUNIOR, M. **Um Método Para Estudo de Viabilidade Técnica-Operacional Para a Implantação de Negócios Eletrônicos**. (2006). f.26-37. Tese de Doutorado. UNIMEP/Santa Bárbara D'Oeste/2006

_____. **Sistemas de Informação**. Americana/SP. FATEC. 2010.

DICIONÁRIO ONLINE DE PORTUGUÊS. In Loco. Disponível em: <http://www.dicio.com.br/in_loco/>. Acesso em: 02 jun. 2013. 20h33.

_____. Backup. Disponível em: <http://www.dicio.com.br/backup/>. Acesso em: 02 jun. 2013. 20h36.

FERREIRA, A. M. **Auditoria de Sistemas de Informação**. Americana/SP. FATEC. 2013.

GOMES, E. D.; ARAÚJO, A. F. de; BARBOSA, R. J. Origem da Auditoria. In__ Auditoria: Alguns Aspectos A Respeito De Sua Origem. **Revista Científica Eletrônica de Ciências Contábeis**: ISSN: 1679-3870, Garça/SP, a. VII, n. 13, p.3-4, maio 2009. Semestral. Disponível em: <http://www.revista.inf.br/contabeis/pages/artigos/ART06-ANOVII-EDIC13-MAIO2009.pdf>. Acesso em: 22 maio 2013. 22h45.

IDEA. Caseware. ¿Qué puede hacer IDEA por ti?. In:__ IDEA VERSION OCHO. Disponível em: <http://www.caseware.com/downloads/pdf/IDEA/IDEAFunc-PDF-es.pdf>. Acesso em: 26 maio 2013. 21h33.

IMONIANA, J. O. **Auditoria de Sistemas de Informação**. 2ª ed. São Paulo: Atlas S.A., 2008. p.1-65.

_____. **Auditoria em Sistemas de Informação.** 2ª ed. 5. reimpr. São Paulo: Atlas, 2013. p.1-65.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (USA). **Padrão de Auditoria de SI.** Rolling Meadows, Il, 2004. p. 2. Disponível em: <http://www.isaca.org/Knowledge-Center/Standards/Documents/Standards-IT-Portugese-S7.pdf>. Acesso em: 30 maio 2013. 17h28.

LAUDON, K. C.; LAUDON, J. P. Perspectiva Empresarial Sobre Sistemas de Informação**.** In:__**Sistemas de informação Gerenciais**. 5ªed. Tradução Arlete Simille Marques. São Paulo: Pearson Prentice Hall, 2004. p.11, p.447.

MAGALHÃES, C. E. G. de. Programas de computador. In:__**Auditoria em Sistemas de Informação.** Disponível em: <http://xa.yimg.com/kq/groups/21677002/1362646326/name/GTI126+-

+Auditoria+em+Sistemas+de+Informa%C3%A7%C3%A3o.pdf>. p. 18-19, p. 20, p. 24, p. 26. Acesso em: 02 jun. 2013. 19h34.

MAGIQUE GALILEO SOFTWARE LTD (United Kingdom). **Your Solution to Effective Risk Management and Risk- Based Auditing.** London, 2012. p. 23. Disponível em: <http://www.magiquegalileo.com/pdf/MagiqueGalileoOverview.pdf>. Acesso em: 01 jun. 2013. 17h40.

MARCUSSO, N. A. **Gestão e Governança da TI**. Americana/SP. FATEC. 2013.

MICROSOFT. **O que é um firewall.** Disponível em: <http://windows.microsoft.com/pt-br/windows-vista/what-is-a-firewall>. Acesso em: 24 maio 2013. 13h25.

MONITOR DAS FRAUDES. Fraudes Contábeis e Internas. **Introdução à lei Sarbanes-Oxley (SOx)**. Disponível em: <http://www.fraudes.org/showpage1.asp?pg=312>. Acesso em: 02 jun. 2013.

NOBRE, J. C. A. Ameaças ao Sistema de Informação: Prevenir e Antecipar. **Cadernos UniFOA.** Volta Redonda, a. 2, nº 05, dez. 2007. Disponível em: <http://www.unifoa.edu.br/pesquisa/caderno/edicao/05/11.pdf> Acesso em: 03 nov. 2012. 18h32.

PAPADAKIS, A. Know-How. In:__**La gran Enciclopedia de Economía**. Disponível em: <http://www.economia48.com/spa/d/know-how/know-how.htm>. Acesso em: 02 jun. 2013. 14h27.

PENTANA. **Where Will You Be Using Pentana Vision?** Disponível em: <http://www.pentana.com/vision/>. Acesso em: 26 maio 2013. 19h03.

SANTIAGO, H. L. P.; LISBOA, G. S. dos. A Segurança da Informação nas organizações. In:__**Segurança dos Sistemas de Informação** – 'O Contexto da Segurança dos Sistemas de Informação'. Paracatu/MG: Faculdade Atenas.

SEPIA SOLUTIONS. Home screen & dashboards. In:__**Pentana VISION illustrated** Disponível em: <http://www.sepiasolutions.net/Software/Vision_for_Auditors.html>. Acesso em: 03 jun. 2013. 9h

SILVA, E. L. da; MENEZES, E. M. A Pesquisa e suas Classificações. In:__. **Metodologia da Pesquisa e Elaboração de Dissertação.** 3ª ed. rev. atual. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001. p.19-21.

SILVA, N. P. Da. Como Construir Fluxogramas de Sistemas. In:__**Análise e Estruturas de Sistemas de Informação.** São Paulo: Ética, 2011. p. 157-163.

SIMÕES, J. M. de O. **Papo Empreendedorismo:** Diagrama de Gantt. Disponível em: <http://www.papoempreendedorismo.com.br/2011/09/diagrama-de-gantt.html>. Acesso em: 02 jun. 2013. 8h55.

SOFTEXPERT. Gestão de Auditorias. In:__**SE Audit.** Disponível em: <http://www.softexpert.com.br/planejamento-controle-auditorias.php>. Acesso em: 27 maio 2013. 09h41.

SOMMERVILLE, I. Engenharia de Sistemas Com Base Em Computadores. In:__ **Engenharia de Software.** 6ªed. Tradução André Maurício de Andrade. São Paulo: Addison Wesley, 2003. p.17.

_____. **Sistemas Organizacionais.** (2011). Disponível em <http://www.monteirodebarros.net/sistemas-organizacionais.php>. Acesso em: 26 nov. 2012. 21h32.

TERUEL, E. C. **Principais ferramentas utilizadas na auditoria de sistemas e suas características.** 2010. 10 f. Universidade Nove de Julho, São Paulo/SP. Disponível em: <http://centropaulasouza.sp.gov.br/pos-graduacao/workshop-de-pos-graduacao-e-pesquisa/anais/2010/Trabalhos/gestao-e-desenvolvimento-de-tecnologias-da-informacao-aplicadas/Trabalhos%20Completos/TERUEL,%20Evandro%20Carlos.pdf>. Acesso em: 26 maio 2013. 18h09.