CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso de Tecnologia em Analise e Desenvolvimento de Sistemas

Adalto da Silva dos Santos

AUDITORIA DE SISTEMAS NO DESENVOLVIMENTO DE SOFTWARE

Americana, SP

2014

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso de Tecnologia em Analise e Desenvolvimento de Sistemas

Adalto da Silva dos Santos

AUDITORIA DE SISTEMAS NO DESENVOLVIMENTO DE SOFTWARE

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas da FATEC de Americana, sob a orientação do Prof. Dr. Alexandre Mello Ferreira

Área: Auditoria de Sistemas

Americana, SP

2014

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Santos, Adalto da Silva dos
S233a Auditoria de sistemas no desenvolvimento de software. / Adalto da Silva dos Santos. – Americana: 2014.
64f.

Monografia (Graduação em Tecnologia em Análise e Desenvolvimento de Sistemas). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Dr. Alexandre Mello Ferreira

1. Auditoria de sistemas de informação 2. Desenvolvimento de software I. Ferreira, Alexandre Mello II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU:658.518.3
681.3.05

Adalto da Silva dos Santos

AUDITORIA DE SISTEMAS NO DESENVOLVIMENTO DE SOFTWARE

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Analise e Desenvolvimento de Sistemas pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Auditoria de Sistemas.

Americana, 04 de Novembro de 2014.

Banca Examinadora:

Alexandre Mello Ferreira (Presidente)
Doutor
Faculdade de Tecnologia de Americana

Antônio Alfredo Lacerda (Membro)
Especialista
Faculdade de Tecnologia de Americana

José William Pinto Gomes (Membro)
Graduado
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradeço primeiramente ao meu professor orientador pelo apoio que me deu e pela dedicação de me guiar pelo caminho correto.

Aos meus companheiros de faculdade pela amizade e ajuda nos trabalhos desenvolvidos.

À minha família pelo apoio e incentivo que sempre me deram para estudar.

DEDICATÓRIA

Dedico este trabalho a Deus, aos meus pais, aos meus tios, aos meus amigos que aqui fiz e que eternamente estarão em minhas lembranças.

RESUMO

Atualmente estamos na era digital onde as pessoas dependem da tecnologia. É praticamente impossível fazer qualquer coisa sem o uso da mesma, sendo que essa necessidade fez com que houvesse um grande aumento no número de organizações especializadas em desenvolvimento de software e isto inevitavelmente deixou o mercado mais competitivo. Para garantir a sobrevivência das corporações neste meio, as empresas precisam garantir cada vez mais a qualidade de seus produtos e assegurar que as atividades e processos sejam executados dentro das normas. Dessa forma, a auditoria de sistemas é um ótimo meio de se garantir o cumprimento das tarefas em torno do desenvolvimento de software, além de identificar os setores defeituosos para que sejam realizadas as devidas correções. Este trabalho traz um estudo sobre os conceitos, metodologias, procedimentos e melhores práticas no que diz respeito à auditoria de sistemas focada no ambiente de desenvolvimento, além de analisar a viabilidade de aplicação da mesma.

Palavras Chave: Auditoria de Sistemas; Informática; Tecnologia da Informação

ABSTRACT

Currently we are in the digital age where people depend of Technology. It's virtually impossible to do anything without the use of the same, and this need has made there was a large increase in the number of specialized in software development organizations and this inevitably made the market more competitive. To ensure the survival of corporations in this environment, companies must increasingly ensure the quality of their products and ensure that activities and processes are performed within the rules. Thus the systems audit is a great way to ensure compliance with the chores around the systems development, and identify bad sectors so that the necessary corrections are made. This paper presents a study of the concepts, methodologies, procedures and best practices with regard to the audit focused on systems development environment, and analyze the feasibility of implementation.

Keywords: *Systems Auditing; Computers; Information Technology.*

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

T.I	Tecnologia da Informação
ID	Identificação
ABNT	Associação Brasileira de Normas Técnicas
UML	*Unified Modeling Language*
MER	Modelo Entidade-Relacionamento
IDEA	*Interactive Data Extraction & Analisys*
ACL	*Audit Command Language*
ITF	*Integrated Test Facility*
ISACA	*Information Systems Audit and Control Association*
CISA	*Certified Information Systems Auditor*
ISO	*International Organization for Standardization*
SPICE	*Software Process Improvement and Capability Determination*
PMBOK	*Project Management Body of Knowledge*

SUMÁRIO

1. INTRODUÇÃO

Segundo Miranda (2007), a auditoria de sistemas tem o objetivo de avaliar a área de Tecnologia da Informação (T.I) para analisar e identificar possíveis riscos, como falhas e irregularidades que estejam ocorrendo e que possam ocorrer. Assim, a auditoria se encarrega de fazer recomendações para melhoria e correção, com objetivo de reduzir o impacto dos riscos levantados.

O autor ainda acrescenta que a T.I é composta de diversas áreas. Assim, cada uma dessas áreas necessita de um tipo de auditoria específica. Em relação a auditoria no desenvolvimento de software, Miranda destaca que nesta área o auditor deve ter um profundo conhecimento em analise de sistemas, principalmente nas questões metodológicas, técnicas e no papel desempenhado pelos profissionais (programador, analista, técnicos, entre outros).

Para Imoniana (2011) a auditoria de sistemas na construção de softwares tem como base a analise de recursos que serão empregados. Um desses recursos é o ciclo de desenvolvimento de sistemas, que é divido em várias etapas (início do projeto, estudos de viabilidade, testes, implantação, manutenção, entre outros).

Imoniana destaca que o auditor pode utilizar algumas técnicas e ferramentas durante este processo. Estas técnicas (como testes de observância e analise documental) facilitam a implementação da auditoria acerca de determinada metodologia, além de ajudar na elaboração de relatórios auditoriais ao fim do processo de auditoria.

Para Koscianski (2007), um dos fatores que mais implicam na qualidade de software e, consequentemente, no ciclo de desenvolvimento da aplicação, é o fator humano. O autor ainda acrescenta que existem várias maneiras de corrigir este problema, sendo que a auditoria de sistemas é uma delas, pois ela permite que a empresa e o trabalho desempenhado sejam vistos e analisados de forma transparente, obtendo um real resultado do que acontece na empresa.

O estudo se **justifica** pela importância que um auditor tem ao agregar as técnicas de auditoria durante a construção de sistemas para que assim a qualidade do software ganhe maiores chances de ser adquirida e os riscos de um sistema falho diminuam, ao mesmo tempo em que boas práticas no processo de desenvolvimento são implementadas por meio da auditoria.

O **problema** foi: Durante o desenvolvimento de softwares, alguns colaboradores não fazem corretamente o que foi pedido, como por exemplo, o cumprimento de normas, regras e padrões. Isto implica negativamente no desenvolvimento do projeto, além de aumentar os riscos do software apresentar falhas em curto prazo, comprometendo sua qualidade e gerando custo desnecessário com futuras atualizações para reverter o problema. Assim se faz necessário um processo de verificação que seja viável e que assegure a execução das tarefas de acordo com o esperado pela gerência, uma vez que as diversas corporações estão cada vez mais preocupadas em oferecer um produto de qualidade para seus clientes.

Como **pergunta** que se buscou responder: A aplicação da auditoria no desenvolvimento de sistemas é viável para pequenas e médias empresas?

As hipóteses foram: **a)** Com um correto gerenciamento dos custos, a aplicação da auditoria se torna viável para as corporações, visto que as mesmas possuem interesse na aplicação da auditoria e que tal aplicação faz com que colaboradores sigam as normas e cumpram corretamente cada tarefa designada, minimizando riscos de falhas no produto e em atividades de risco. **b)** A aplicação da auditoria no desenvolvimento de sistemas é inviável, pois não há quaisquer interesse em aplicar uma auditoria e ela não garante que as tarefas sejam executadas corretamente, muito menos diminui riscos iminentes e só gera custos adicionais para a empresa. **c)** Esta aplicação pode ser viável desde que haja um correto gerenciamento dos custos, colaboração dos funcionários, comprometimento dos auditores em suas atividades, conscientização dos benefícios que se obtém ao aplicar uma auditoria e a garantia de redução dos riscos.

O **objetivo geral** constituiu em estudar a auditoria de sistemas e seu papel no desenvolvimento de software, objetivando o cumprimento das etapas e normas estabelecidas e a viabilidade desta aplicação.

Os **objetivos específicos** foram: **a)** Estudar o ciclo de desenvolvimento do software, objetivando o conhecimento das etapas e processos necessários durante este ciclo. **b)** Fazer um levantamento sobre técnicas e processos de uma auditoria, visando o entendimento desta função e sua importância na área de T.I. **c)** Discutir a viabilidade da auditoria, buscando conhecer as possibilidades de aplicação da mesma através da analise dos resultados obtidos no estudo de caso.

Como **metodologia** do ponto de vista da sua natureza, a pesquisa é aplicada, pois procura solucionar problemas relacionados ao processo de desenvolvimento com a aplicação da auditoria, e para isso tem-se a necessidade de conhecer e analisar técnicas, procedimentos e o ambiente em questão.

Do ponto de vista da forma de abordagem, a pesquisa é qualitativa, visto que irá discutir o papel da auditoria de sistemas na resolução de problemas durante o desenvolvimento de software.

Do ponto de vista dos objetivos, a pesquisa é exploratória e descritiva, de modo que irá descrever a importância da auditoria, como auditar sistemas e identificar as melhores práticas, ferramentas e recursos para atingir os resultados esperados.

Do ponto de vista dos procedimentos técnicos, a pesquisa é bibliográfica, de modo que foi feita a pesquisa em teses, livros e demais materiais acadêmicos disponíveis na biblioteca e na internet.

O trabalho foi estruturado em quatro capítulos, sendo que o primeiro conceitua o ciclo de desenvolvimento de software, o segundo descreve e conceitua a auditoria de sistemas no processo de desenvolvimento, o terceiro analisa o estudo de caso referente a viabilidade de aplicação da auditoria e com base nas informações conseguidas a partir dos estudos realizados, o quarto se reserva às considerações finais.

2. O CICLO DE DESENVOLVIMENTO DE SOFTWARE

Antes de abordar a auditoria durante a construção de sistemas, devemos ter como base os princípios do ciclo de desenvolvimento de software. Este ciclo é essencial na construção de quaisquer sistemas. Assim, torna-se necessário o conhecimento das atividades envolvidas neste processo (como por exemplo, metodologia de desenvolvimento, diagramas de caso de uso, analise de requisitos, tipos de testes que serão aplicados, entre outros) pois os mesmos serão cuidadosamente analisados durante a auditoria.

Para Sommerville (2011), o ciclo de desenvolvimento de software consiste em todas as etapas e passos necessários para a fabricação de um sistema, desde a concepção até a implantação. Muitas das fases são comuns nas mais variadas metodologias, sejam elas ágeis ou clássicas.

Trata-se de algo muito abordado dentro da engenharia de software, sendo apontado como um dos melhores métodos para se obter um sistema com qualidade. Há uma sequência de etapas a serem cumpridas até a fase final, caracterizada pela implementação e entrega do sistema.

Por se tratar de um ciclo, após a entrega do software, o cliente pode solicitar novos recursos a serem implementados, fazendo com que se inicie novamente a sequência de atividades até que tais necessidades sejam atendidas. Assim, pode-se considerar o cliente como a peça-chave para que o ciclo fique em constante rotatividade.

2.1. DETALHES DO CICLO DE DESENVOLVIMENTO

Koscianski (2007) afirma que, das etapas presentes em quase todas as metodologias, se destacam o levantamento e analise de requisitos, analise do sistema, codificação, testes e implantação, conforme ilustrado na Figura 1.

Figura 1: Ciclo de Desenvolvimento de Software

Fonte: Koscianski (2007)

2.1.1. ANALISE DE REQUISITOS

Requisitos são condições necessárias para se obter determinado objetivo e podem ser divididos em dois tipos: funcionais e não funcionais. (Koscianski, 2007)

De acordo com Sommerville (2011), **Requisitos funcionais** são os requisitos que definem uma determinada função do sistema ou apenas uma parte dele. Assim, um requisito funcional é composto por um conjunto de entradas, seu comportamento e saída, envolvendo cálculos, manipulação, processamento de informações, entre outros. Exemplos: Um usuário pode realizar pesquisas em todo o banco de dados; Cada locação deve ser associada a um ID (Identificação); O sistema deve possuir uma interface intuitiva ao usuário, entre outros.

Os requisitos funcionais ainda podem ser divididos em três categorias: evidente, escondido e friso. Um requisito funcional evidente são aqueles na qual o usuário está ciente de sua execução. Requisitos funcionais escondidos são aqueles que são invisíveis ao usuário, ou seja, os mesmos não têm consentimento da função

que está em execução. Requisitos funcionais friso são aqueles que não afetam outras funções do software (Figueiredo, 2014).

De acordo com Pressman (2011), **Requisitos não funcionais** são definidos como requisitos que possuem relação com uso do software em termos de usabilidade, desempenho, confiabilidade, segurança, disponibilidade, entre outros. Muitas vezes, esse tipo de requisito acaba gerando algumas restrições aos requisitos funcionais.

O autor ainda divide os requisitos não funcionais em três categorias:

- Requisito do produto: especifica o comportamento do sistema (velocidade do sistema e desempenho);

- Requisitos Organizacionais: é tido como consequência das políticas e procedimentos encontrados nas empresas (como regras de negócio e padrões do cliente);

- Requisitos Externos: são derivados de fatores externos ao software ou ao ambiente (como a legislação, por exemplo).

Exemplos: O aplicativo deve ser desenvolvido em Delphi; Toda a documentação deve seguir o padrão da ABNT; Dados pessoais dos clientes não devem ser visualizados pelos operadores do sistema (Figueiredo, 2014).

De acordo com Mota (2013), a analise de requisitos é a primeira etapa de qualquer metodologia de desenvolvimento. Nesta etapa, utiliza-se diversas técnicas para levantamento de requisitos, como *brainstorming* (tempestade de ideias), coleta de dados através de conversações com usuários, entre outros. Esta etapa também consiste de sub estágios (como a analise de viabilidade, para ver se vai ser possível desenvolver o sistema).

Paula Filho (2009) destaca que para servir de base a um sistema de qualidade, o enunciado dos requisitos deve satisfazer uma série de características. Por enunciado dos requisitos entende-se o modelo do problema, especificação de requisitos ou artefato equivalente.

É desejável que o enunciado dos requisitos seja:

- Correto (o requisito deve ser realmente um requisito do produto a ser construído);
- Preciso (onde ele possui uma única interpretação);
- Completo (reflete todas as decisões de especificação que foram tomadas);
- Consistente (onde não há conflitos entre nenhum dos subconjuntos de requisitos);
- Priorizado (onde os requisitos são classificados de acordo com a complexidade, estabilidade e importância);
- Verificável;
- Modificável; e
- Rastreável.

2.1.2. ANALISE DE SISTEMA

Para Koscianski (2007), essa etapa do ciclo é onde todo o aplicativo é especificado em detalhes, sendo que o sistema também pode ser dividido em partes menores, facilitando o gerenciamento pelos desenvolvedores. Metodologias ágeis (como SCRUM, por exemplo) não costumam fazer documentação ou diagramas para detalhar algumas partes do processo, diferentemente das metodologias mais genéricas (como Cascata, Incremental, Espiral).

O autor ainda destaca que nesta fase deve-se transformar todos os dados obtidos no levantamento de requisitos em diagramas, que serão a base para

codificação do sistema. Nesta etapa, os diagramas são normalmente implementados usando a UML (Linguagem de Modelagem Unificada).

Para Sommerville (2011), “Diagrama de Caso de Uso, Diagrama de Sequência e Diagrama de Classe são muito comuns na analise de sistema e ambos atendem a fins específicos.” Nas subseções abaixo, os mesmos serão brevemente descritos.

2.1.2.1. DIAGRAMA DE CASO DE USO

Segundo Pressman (2011), “o diagrama de caso de uso visa representar uma unidade coerente de funcionalidade. Estes diagramas são comumente usados para descrever funções completas de um sistema, aplicação ou produto, mas podem ser usados também no nível de subsistemas e até em classes”.

Este diagrama é formado pelos atores e pelos casos de uso. Os atores são abstrações de uma entidade real. Os casos de uso são atividades que poderão ser desempenhadas por eles (Sommerville, 2011).

Sommerville (2011) acrescenta que, além do relacionamento entre os atores e os casos de uso, há também o relacionamento entre os próprios casos de uso. Dentre estes relacionamentos, destacam-se o relacionamento de **generalização** (onde um caso de uso mais especializado herda comportamentos e ações de um caso de uso mais genérico), o relacionamento por **extensão** (onde um caso de uso nada mais é do que um comportamento adicional de outro) e o relacionamento de **inclusão** (onde um caso de uso invoca outro dentro do seu fluxo de comportamento).

2.1.2.2. DIAGRAMA DE SEQUÊNCIA

O diagrama de sequência é tido como um pouco mais complexo e técnico do que o diagrama de caso de uso, sendo que este tem como foco descrever a sequência de ações necessárias para sair de um determinado estado do sistema para outro. (Mota, 2013).

Neste diagrama, há também a presença dos atores. Há partir do diagrama de sequência é possível determinar boa parte dos métodos das classes que serão implementadas. O diagrama de sequência também permite que outras funções da programação sejam representadas graficamente, como os loops (laços de repetição), estrutura if (se, senão, fimse), entre outros (Baesso, 2004).

2.1.2.3. DIAGRAMA DE CLASSE

Nas metodologias orientadas a objetos, os objetos representam entidades discretas que encapsulam estado e comportamento. O estado é representado pelos atributos do objeto. O comportamento de um objeto é representado pelas respectivas operações (métodos), que são especificações de transformações ou consultas que o objeto poderá chamar para a execução (Paula Filho, 2009).

Objetos similares são agrupados em classes. Um relacionamento é a conexão semântica entre elementos de um modelo. Os métodos e atributos de uma classe podem ser privados (apenas os elementos na classe podem "enxergá-los") ou públicos (todas as outras classes podem ver os atributos e métodos).

Neste tipo de diagrama é comum encontrarmos diversos paradigmas da orientação a objetos, sendo que o conceito de herança é tido como um dos mais importantes e essências. Este conceito permite que uma classe-filha herde atributos e métodos de uma classe-pai (Pressman, 2011).

2.1.3. CODIFICAÇÃO

Nesta fase, os diagramas da fase anterior são passados para a equipe de programadores, que se encarregarão de transformá-los em código-fonte de determinada linguagem de programação, sendo que antes de ser iniciado tal processo, as informações interpretadas pelos programadores são dispostas em estruturas de dados (Mota, 2013).

Estrutura de dados trata-se da organização dos dados e dos algoritmos de forma coesa e racional, de modo a melhorar o processo de codificação. Dependendo

do modo que determinado conjunto de dados é organizado, pode-se resolver de maneira simples problemas de extrema complexidade.

Durante a codificação, são implementados funções e rotinas específicas, que atendem diversas necessidades para o funcionamento da aplicação em desenvolvimento. Algumas linguagens de programação permitem o uso de funções já pré-estabelecidas pela linguagem em questão, além de permitir que os programadores desenvolvam suas próprias funções para atender um requisito ou especificação feita nos algoritmos (Pressman, 2011).

2.1.4. TESTES

De acordo com Rios (2002), a fase de testes é a mais importante no ciclo de desenvolvimento de software, visto que nesta fase se encontram atividades de testes para averiguar possíveis falhas no sistema, antes que o mesmo seja entregue ao cliente.

Caroline (2007) descreve um teste como uma atividade na qual o sistema ou componente é executado sob condições especificadas, com observação e registro dos resultados e avaliação de um ou mais aspectos. Todos os testes possuem uma finalidade, que é um conjunto identificado de características de software que serão medidas sob condições especificadas, comparando o comportamento real com o comportamento requerido. Critério de teste é um critério na qual um sistema ou função deve fazer para passar no teste. Enfim, os testes são mais do que meios de detecção de erros, são indicadores de qualidade do sistema.

Existem vários tipos de testes, e dentre eles se destacam os seguintes:

- **Aceitação**: busca simular operações de rotina executadas pelos usuários a fim de conferir se o comportamento está conforme com o esperado);

- **Integração**: procura encontrar falhas provindas da integração dos componentes do aplicativo;

- **Performance**: visa avaliar a capacidade limite de dados processados pelo software, forçando a taxa de transferência de dados até que a aplicação não consiga mais processá-las;

- **Operação**: simula a execução em ambiente final no qual o software entrará definitivamente em execução, para assegurar que a implementação do sistema será bem sucedida.

Durante a realização dos testes, deve ser realizado a documentação dos resultados obtidos. É documentado o ID do teste, o tipo, dados de entrada (quais informações foram inseridas durante a execução), roteiro de teste (a maneira que o teste foi executado), o resultado que se espera do teste, o que foi obtido, a data de execução e demais observações (Pressman, 2011).

2.1.5. IMPLANTAÇÃO

A fase de implantação do sistema fecha o ciclo de desenvolvimento de software. Nesta fase final do ciclo, o sistema (teoricamente) já não possui mais erros ou falhas e está pronto para ser usufruído pelo usuário final. Na fase de implementação também inclui atividades cujo objetivo é gerar a documentação (como manuais, ajuda on-line, entre outros recursos), e em alguns casos, dar suporte ao usuário (Pressman, 2011).

É muito comum o surgimento de novos requisitos após a implementação e até mesmo durante as etapas descritas anteriormente. Assim, repete-se o ciclo ilustrado na Figura 1 até que as novas necessidades sejam devidamente atendidas. Ou seja, é feita novamente a analise do novo requisito, novos diagramas, alterações na codificação do aplicativo, novos testes e as devidas implementações. (Koscianski, 2007).

Todas as etapas e funções vistas neste capítulo serão analisadas dentro de uma auditoria de sistemas, e para isso, o auditor necessita carregar consigo a bagagem de conhecimento necessária a respeito desse roteiro de desenvolvimento, bem como das atividades e conceitos presentes na auditoria, conforme veremos no próximo capítulo.

3. AUDITANDO SISTEMAS EM DESENVOLVIMENTO

Para Schmidt (2006), “A função da auditoria de sistemas é promover adequação, revisão, avaliação e recomendações para aprimorar os controles internos nos sistemas de informação da corporação, além de avaliar o uso de recursos (humanos, materiais e tecnológicos) envolvidos na execução dos mesmos.”

Carneiro (2014) destaca que a auditoria de sistemas deve atuar em todos os sistemas da organização, seja no nível operacional, tático e estratégico. Tendo em vista o desenvolvimento de sistemas, a auditoria atua em todo o processo de construção de software, desde a fase de requisitos até sua implantação, bem como o próprio processo ou metodologia de desenvolvimento, conforme apresentado no capítulo 2.

3.1. OBJETIVOS DA AUDITORIA

Segundo Lyra (2008), são objetivos universais da auditoria de sistemas:

- **Integridade**: confiança e consistência das transações processadas pelo sistema, para que assim os usuários possam tomar decisões com base nas informações sem receio;

- **Confidencialidade**: as informações são entregues somente aos usuários que necessitam conhecê-las;

- **Privacidade**: funções incompatíveis nos sistemas são segregadas. Durante o processo de autorização, os usuários apenas enxergam e fazem uso das informações necessárias par suas respectivas atividades;

- **Acuidade**: pode-se validar transações processadas. Um módulo de consistência para entrada de dados é capaz de auxiliar na verificação dos mesmos. Isto é fundamental para prevenir que dados indevidos sejam inseridos nos sistemas, gerando transações impróprias ou inválidas;

- **Disponibilidade**: há a necessidade do sistema estar disponível para o cumprimento dos objetivos da empresa, sendo que sua falta pode culminar em prejuízos financeiros ou gerar problemas;

- **Auditabilidade**: os sistemas devem gerar e documentar *logs* operacionais que permitam trilhas de auditoria;

- **Versatilidade**: o sistema deve ser de fácil usabilidade, fácil de se adaptar ao *workflow* operacional da empresa, utilizar recursos de importação e exportação de dados de forma simples, etc.;

- **Manutenibilidade**: procedimentos e políticas operacionais devem contemplar controles de teste, conversão, implantação e documentação de sistemas. Os riscos de contaminação dos ambientes devem ser eliminados.

3.2. CONCEITOS E PROCESSOS DA AUDITORIA EM SISTEMAS

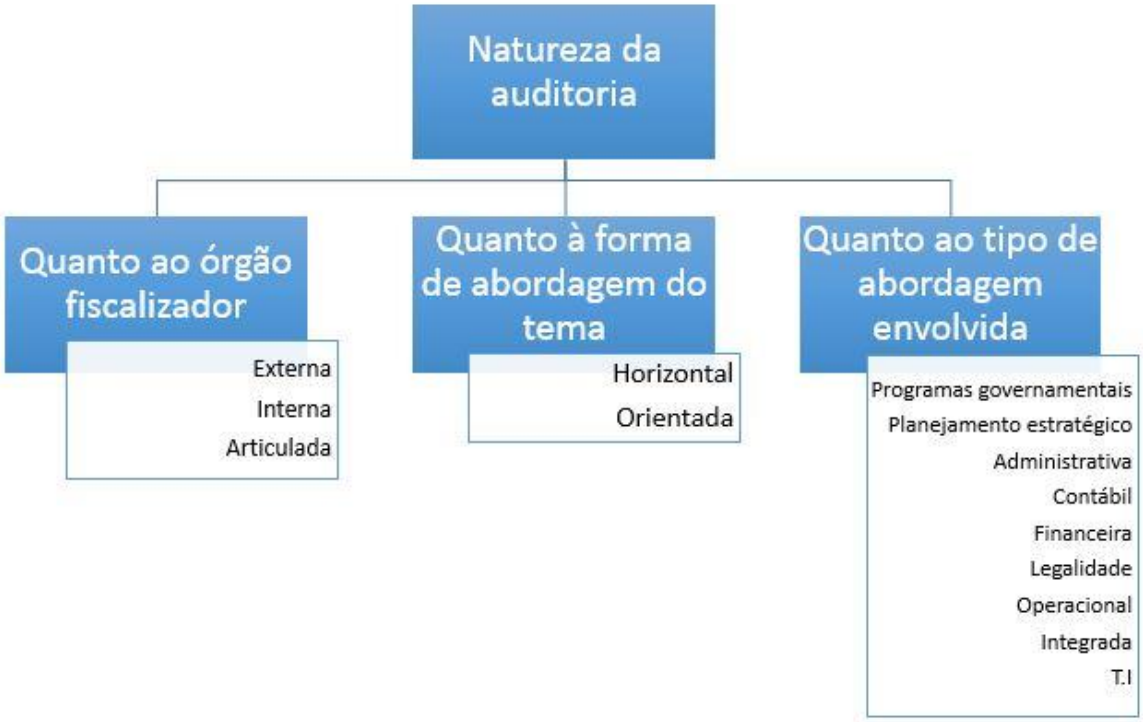
De acordo com Imoniana (2011, p. 54):

> "A auditoria é uma atividade que engloba o exame de operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o intuito de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões."

O autor ainda acrescenta que o **campo** da auditoria é constituído pelo objeto que será fiscalizado, pelo período e também pela natureza da auditoria. Tendo em vista o processo de desenvolvimento, fazem parte deste campo todas as áreas da empresa inclusas no ciclo de desenvolvimento de software (departamento de desenvolvimento, departamento de testes, entre outros). O período trata da frequência que a auditoria será feita (por exemplo, mensalmente, trimestralmente, anualmente, entre outros).

Os tipos da natureza de auditoria são classificados de acordo com os seguintes tópicos: quanto ao órgão fiscalizador, à abordagem do tema e ao tipo de área envolvida (Dias, 2000), conforme ilustrado na Figura 2.

Figura 2: Natureza da Auditoria



Fonte: Dias (2000)

- **Quanto ao órgão fiscalizador**

  - Auditoria externa: executado por uma instituição externa (totalmente independente da empresa fiscalizada) com objetivo de emitir uma analisa sobre a gestão dos recursos, situação financeira e legalidade, além da regularidade das operações;

  - Auditoria interna: executada pelo departamento de auditoria interno da própria entidade, com objetivo de reduzir as possibilidades de fraudes, erros e práticas ineficazes;

  - Auditoria articulada: trata-se da trabalho conjunto entre auditoria interna e externa.

- **Quanto à forma de abordagem do tema**

    - Auditoria horizontal: trata-se de uma auditoria cujo tema é específico e é realizada em várias corporações ou atividades paralelamente;

    - Auditoria orientada: possui enfoque em uma tarefa específica ou em atividades com grandes indícios de fraudes ou erros.

- **Quanto ao tipo de abordagem envolvida**

    - Auditoria de programas governamentais: avaliação e acompanhamento da realização de determinados programas ou projetos de governo;

    - Auditoria de planejamento estratégico: é verificado se os objetivos da corporação são alcançados e se as políticas relacionadas a aquisição, utilização e gerenciamento dos recursos são obedecidas;

    - Auditoria administrativa: compreende ao plano da organização, bem como os procedimentos e documentos que servem de suporte à tomada de decisões;

    - Auditoria contábil: compreende à segurança dos ativos da corporação. Tem a finalidade de garantir que as operações, uso e acesso aos ativos sejam efetuadas conforme as autorizações estabelecidas;

    - Auditoria financeira: embasa-se na análise das contas, situação financeira, bem como a regularidade e legalidade dos aspectos financeiros, contábeis e orçamentários, verificando se as operações e movimentações foram devidamente autorizadas e registradas;

- Auditoria de legalidade: é constituída pela analise da regularidade da gestão dos recursos, averiguando a conformidade da gestão com a legislação;

- Auditoria operacional: ocorre em todos os níveis da gestão sob o enfoque econômico. Verifica se os resultados almejados foram alcançados;

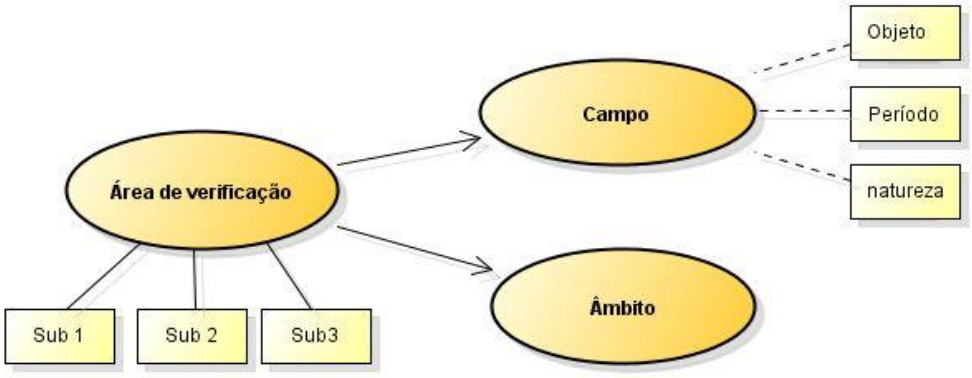
- Auditoria integrada: trata-se da aplicação simultânea da auditoria financeira e da auditoria operacional;

- Auditoria de T.I: Os auditores analisam todo a área de T.I, sistemas da empresa e setores comprometidos com a segurança de informação, identificando os pontos fortes e as deficiências.

Tendo em vista os aspectos descritos acima, a natureza que caracteriza uma auditoria em desenvolvimento de software é a auditoria de T.I, podendo até mesmo incluir alguns aspectos a respeito da auditoria de legalidade (Dias, 2000).

Para Saeta (2013), o **âmbito da auditoria** é constituído pela amplitude e exaustão dos procedimentos de auditoria, onde serão aprofundados as tarefas e o grau de abrangência. Dias (2000) destaca que o conjunto constituído pelo campo e âmbito de auditoria é denominado como **área de verificação**, sendo que tal conjunto pode ser divido em outros subconjuntos a fim de facilitar os processos da auditoria, conforme apresentado na Figura 3.

Figura 3: Conceitos e Organização da Auditoria



Fonte: Dias (2000)

Controle é a fiscalização aplicada sobre as atividades dos colaboradores, órgãos ou departamentos, para que as atividades ou produtos não se desviem do que foi preestabelecido. De acordo com Gomes (2008), os controles podem ser classificados em:

- **Preventivos**: previne erros, atos fraudulentos ou omissões;
- **Detectivos**: detectam omissões, erros ou fraudes, além de relatar a ocorrência;
- **Corretivos**: utilizados para diminuir impactos ou corrigir erros, uma vez que estes foram detectados.

Para avaliar a atuação de outros profissionais, é necessário que o auditor possua um modelo normativo, bem como um conjunto de padrões, que demonstre como determinada atividade operação deveria ser feita (Gomes, 2008).

Para Saeta (2013), este modelo normativo é composto por objetivos de controle que serão analisados pelo auditor em cada área específica. Enquanto os objetivos de controle compreendem a uma área mais ampla, os procedimentos de auditoria caracterizam padrões individualizados e mais detalhados. Por exemplo: no setor de programação, um dos objetivos pode ser o estabelecimento de regras para controle de versões do aplicativo em desenvolvimento. Um procedimento de auditoria

relacionado a esse objetivo pode ser: verificar se existem processos que definam a maneira que é realizada o controle de versões e quais funcionários poderão acessar versões mais antigas.

Para Lyra (2008), no decorrer da realização da auditoria, a equipe deve reunir evidências que sejam confiáveis, relevantes e úteis para a atingir dos objetivos da auditoria. Tais evidências podem ser classificadas em quatro categorias:

- **Evidência física;**
- **Evidência documentária;**
- **Evidência fornecida pelo auditado;**
- **Evidência analítica.**

Uma evidência definida como incompatível com o tipo de auditoria em questão pode servir como indicativo para outra auditoria. A manutenção dos papéis de trabalho (meio no qual são registrados os achados de auditoria, ou seja, os fatos observados pelo auditor) é essencial para a elaboração do relatório da auditoria em execução e para o planejamento de futuras auditorias (Carneiro, 2014).

3.3. METODOLOGIA DE AUDITORIA DE SISTEMAS

Metodologia de auditoria é um conjunto de fases que permite flexibilidade e aderência a todas as modalidades de auditoria em sistemas.

Esta metodologia é composta pelas seguintes fases: Planejamento e controle do projeto de auditoria; Levantamento do sistema; Identificação de inventários dos pontos de controle; Priorização, seleção e avaliação dos pontos de controle; e Acompanhamento da auditoria (Lyra, 2008), conforme exemplificado na Figura 4.

Figura 4: Metodologia de Auditoria

Fonte: Autor (2014)

3.3.1. PLANEJAMENTO E CONTROLE DO PROJETO DE AUDITORIA

De acordo com as diretivas da gerência da entidade, é estabelecido o planejamento inicial das ações e recursos necessários para executar a auditoria. É levado em consideração a abrangência das ações, o enfoque que se deseja, bem como o quantitativo de sistemas a serem auditados. Assim, é formado uma equipe de trabalho dividida em dois grupos, sendo que um deles é de coordenação e outro de execução (Lyra, 2008).

O grupo de coordenação deverá ser composto pelo gerente de auditoria, pelo gerente do setor responsável pelo sistema de informação, pelo gerente ou responsável técnico do sistema e também pelo gerente da área de T.I. Cabe a este grupo a definição dos procedimentos a serem utilizados durante o trabalho de auditoria, a escolha dos meios para a realização das tarefas, acompanhamento e moderação dos resultados obtidos e outras atividades gerenciais (Oliveira, 2006).

O grupo de execução deverá ser composto pelos auditores e pelos técnicos da área de T.I e usuária, sendo que os mesmos realizarão, de fato, a auditoria (Lyra, 2008).

3.3.2. LEVANTAMENTO DO SISTEMA

Para Imoniana (2011), uma vez delimitado o sistema ou setor de T.I a ser auditado, é iniciado o processo de abordagem das informações referentes ao sistema ou setor que são relevantes.

Como o objetivo de otimizar os recursos envolvidos, tal abordagem deve ser feito de um jeito abrangente, de forma que seja possível um entendimento das

características do sistema. Pode ser utilizada técnicas de entrevista e analise de documentação existente, inserindo as informações de forma gráfica e descritiva. Ferramentas como MER (Modelo Entidade-Relacionamento), dicionário de dados, diagramas de classe, diagramas de caso de uso, entre outros, são aliados em potencial durante essa fase, pois explicam o comportamento do sistema e seus relacionamentos (Imoniana, 2011).

O mais importante nesta fase é identificar claramente o escopo, pois este procedimento ajuda na determinação da abrangência da auditoria em questão e diminui a possibilidade de execução de trabalho em áreas que não pertencem ao escopo (Oliveira, 2006).

3.3.3. IDENTIFICAÇÃO E INVENTÁRIO DOS PONTOS DE CONTROLE

Para Moore (2012), Um ponto de controle trata-se de uma situação do ambiente de T.I considerada pelo auditor como interessante para avaliação, ou seja, são as possíveis fontes de erros, omissões, falha de procedimentos, entre outros.

Os pontos de controle podem ser encontrados em documentos de entrada, relatórios de saída, telas, arquivos, bancos de dados e outros elementos relevantes para o sistema. Cada ponto de controle deve ser relacionado, e suas funções no sistema bem como seus objetivos devem ser descritos de acordo com os termos de controle interno. Deve-se identificar seus parâmetros, seus pontos fracos e técnicas de auditoria mais adequadas à sua validação (Edna, 2004).

O resultado deste levantamento deve ser encaminhado ao grupo de coordenação para uma validação de pertinência e eventual triagem, para assegurar que o foco da auditoria será atingido (Schmidt, 2006).

Schmidt (2006) ainda destaca alguns pontos de controle típicos em uma auditoria no processo de desenvolvimento:

- Metodologia de desenvolvimento;
- Especificação de requisitos do sistema;

- Projeto lógico e físico;
- Construção e testes;
- Gerência do projeto;
- Plano de implantação e treinamento;
- Controle de versão, etc.

3.3.4. PRIORIZAÇÃO E SELEÇÃO DOS PONTOS DE CONTROLE

Esta etapa consiste na seleção e priorização dos pontos de controle que foram inventariados na etapa anterior, que devem fazer parte do trabalho a ser realizado (Lyra, 2008).

Essa seleção dos pontos de controle pode ser efetuada com base em:

- **Grau de risco existente no ponto**: a analise do risco consiste na verificação dos danos que podem ser acarretados pelo sistema. Grau de risco que existe no ponto em relação ao software ou setor como um todo. Prevê, com antecedência, quais ameaças prováveis de um ponto;
- **Existência de ameaças**: podemos auditar primeiramente os pontos que se encontram sob forte ameaça, e depois, aqueles sob menos pressão;
- **Disponibilidade de recursos**: escolha dos pontos que possam ser auditados com os recursos destinados.

Esta priorização deverá ser revisada ao longo do trabalho, para verificar sua pertinência em relação ao desenrolar das atividades da auditoria.

3.3.5. AVALIAÇÃO DOS PONTOS DE CONTROLE

Nesta etapa, é realizado os testes de validação dos pontos de controle, de acordo com as especificações e parâmetros determinados nas etapas anteriores.

Devem ser aplicadas as técnicas de auditoria capazes de evidenciar fraquezas ou falhas do controle interno. O uso de ferramentas adequadas à verificação em questão pode ser necessário para atingir um resultado que seja satisfatório. Para cada objetivo e característica do ponto de controle existe uma técnica de auditoria e ferramenta mais eficiente (Lyra, 2008).

3.3.6. ACOMPANHAMENTO DA AUDITORIA

Com a finalização da validação dos pontos de controle, deve-se elaborar um relatório de auditoria contendo o resultado encontrado, qualquer que seja ele. Este relatório deve conter o diagnóstico da situação atual dos pontos de controle e, caso existam, as fraquezas (Lyra, 2008).

Quando um ponto de controle apresenta fraqueza, logo este ponto de controle é transformado em ponto de auditoria, fazendo-se necessário apontar no relatório de auditoria, recomendações para solução dessa fraqueza. Cada ponto de auditoria deverá sofrer revisão e avaliação, após um prazo dado para tomada de medidas corretivas, por parte dos analistas e usuários responsáveis (Schmidt, 2006).

Assim, o acompanhamento da auditoria precisa ser efetuado até que todas as recomendações tenham sido executadas e as fraquezas tenham sido eliminadas ou atinjam um nível tolerável pela organização (Imoniana, 2011).

3.4. RELATÓRIOS AUDITORIAIS

O auditor deve apresentar seus achados e conclusões em um relatório, sendo que este relatório deve conter os fatos sobre a empresa auditada, comprovações, conclusões e, eventualmente, recomendações para a empresa (Schmidt, 2006).

De acordo com Lyra (2008, p. 114):

> “A linguagem utilizada no relatório deve ser clara, objetiva e simples, evitando-se o uso de termos técnicos e siglas. Se o uso desses termos e siglas forem necessários, então o relatório deve conter um glossário ou explanações ao longo do texto. A estrutura deve ser bem organizada e abranger todas as informações relevantes para análise pela chefia ou entidade que solicitou a realização da auditoria.”

Dependendo do motivo que acarretou na realização da auditoria, o relatório pode ser enviado à diretoria da organização, ao organismo que financia a empresa auditada ou ao organismo encarregado pelo controle e auditoria geral da empresa. A equipe de auditoria pode dar início ao relatório antes mesmo de iniciar as atividades de campo ou durante a fase de planejamento. Durante o planejamento já foram reunidas informações preliminares sobre a empresa e seus sistemas computacionais e já foram definidos os recursos necessários para a realização dos trabalhos, composição da equipe, metodologias, campo da auditoria, objetivos de controle e procedimentos a serem utilizados. Todos esses dados fazem parte da composição o relatório. É aconselhável documentar tudo que foi observado e dito pelos entrevistados durante os trabalhos de campo. Para que não haja quaisquer mal-entendido ou desvios de interpretação, a equipe deve confirmar os fatos documentados e mostrar ao entrevistado partes da documentação referentes a assuntos tratados com o mesmo durante a entrevista (Lyra, 2008).

Para Imoniana (2011), ao término das apurações, é recomendável apresentar aos responsáveis da área auditada, um relatório parcial contendo as principais deficiências encontradas. Os responsáveis justificam tais falhas e suas justificativas podem ser anexadas no relatório final. A apresentação de relatórios intermediários é importante para evitar quaisquer constrangimentos, inconsistências ou erros, que poderão ser corrigidos ou eliminados antes da apresentação do relatório final.

A equipe de auditoria deve revisar o relatório final, com a finalidade de verificar sua conformidade com os padrões da organização auditora e checar se ainda há algum erros ou inconsistência dos dados (Imoniana, 2011).

Dias (2000) acrescenta que os tipos de informações que serão apresentadas devem ser adaptadas para o seu público alvo, fazendo com que a estrutura de relatórios de auditoria sejam variáveis.

Lyra (2008) destaca alguns dos tópicos geralmente abordados em um relatório dirigido à órgãos de auditoria:

- **Dados da entidade auditada**: razão social, logradouro, natureza jurídica (empresa pública, empresa privada, órgão do governo), relação de responsáveis, entre outros;

- **Síntese**: contém um breve resumo do conteúdo;

- **Dados da auditoria**: objetivo da auditoria, período de fiscalização, integrantes da equipe, metodologia que foi adotada, natureza da auditoria e aplicativos específicos;

- **Introdução**: Pode ser incluso um breve histórico da empresa e também podem ser mencionados alguns dados de auditorias anteriores realizadas na mesma área. No que se refere a auditoria de T.I, deve ser incluso uma descrição da estrutura hierárquica do departamento de T.I, descrição do ambiente computacional, principais sistemas e projetos;

- **Falhas detectadas**: É tida como a parte mais importante do relatório pois apresenta, em detalhes, as irregularidades encontradas. Deve ser apresentado a descrição da falha, comentários iniciais, a justificativa do auditado e o parecer final da equipe;

- **Conclusão**: são sintetizados as recomendações ou determinações finais para corrigir as irregularidades encontradas;

- **Pareceres da Gerência Superior**: em determinados casos, as gerências superiores dão seu parecer a respeito dos achados e recomendações da equipe de auditoria. Os superiores poderão concordar totalmente ou em parte com os pontos apresentados pela equipe ou ainda discordar totalmente.

3.5. FERRAMENTAS DE AUDITORIA DE SISTEMAS

De acordo com Gil (2000), as ferramentas de auditoria são poderosos aliados para a extração, seleção e transações de dados a serem validadas, auxiliando na evidenciação de desvios. Existem softwares capazes de processar amostras, analisá-las e gerar dados estatísticos, apontando duplicidades e outras funções de interesse para o auditor.

Utilizar um software específico para auditoria oferece diversas vantagens, dentre elas se destacam o fato do aplicativo processar vários arquivos (de diferentes tipos e formatos), o atendimento a demandas específicas e determinadas funções que exijam especificações de uma auditoria, entre outros (Bittencourt, 2007).

Em contrapartida, o preço de um sistema do tipo pode ser muito caro, visto a limitação de seu uso ou a restrição a apenas um cliente. Há também os programas utilitário em geral, que podem executar algumas funções similares, de ordenar um arquivo, sumarizar, gerar textos e planilhas, entre outros. Vale ressaltar que estes recursos não são desenvolvidos especificamente para a autoria, portanto não há determinados recursos, como a verificação dos totais de controle e gravação de trilhas de auditoria (Lyra, 2008).

3.5.1. SOFTWARES DE AUDITORIA

Os softwares de auditoria são programas utilizados para gerar documentação, relatórios e também oferecem outros recursos que facilitam o trabalho do auditor. A maioria dos softwares não são gratuitos e cabe ao órgão fiscalizador de auditoria a realização da compra do produto diretamente com o fabricante. Dos softwares de auditoria gratuitos, destaca-se o **Open-Audit**, utilizado para auditar sistemas Linux e Windows conectados em uma rede local, permitindo que o auditor saiba exatamente o que está conectado na rede e como os recursos estão configurados (Mendes, 2010).

Quanto os softwares de auditoria pagos, destacam-se:

- **Galileo:** O Galileo é um software de gestão de auditoria, que inclui documentação de relatórios emitidos e gestão de risco;

- **Pentana:** O Pentana é um software estratégico de auditoria, que contém planejamento e monitoração de recursos, registro de *check-lists* e outros recursos específicos (como gerenciamento de plano de ação);

- **IDEA (Interactive Data Extraction & Analysis):** IDEA é um software focado para extração e analise de dados;

- **ACL (Audit Command Language):** ACL também é um software focado para extração e analise de dados.

3.5.2. CLASSIFICAÇÃO DE FERRAMENTAS DE AUDITORIA

As ferramentas de auditoria podem ser divididas em três categorias: generalista, especializadas e utilitários.

As ferramentas definidas como generalista são softwares com capacidade de processamento e analise, além de gerar amostras, sumarizar, mostrar possíveis duplicidades, criar dados estatísticos, entre outras funções. Assim, são softwares que processam várias coisas de diferentes tamanhos e formatos ao mesmo tempo, permitindo integração com outros de softwares e hardwares. Audit, ACL e IDEA são exemplos de ferramentas generalistas (Lyra, 2008).

As ferramentas definidas como especializadas são softwares programados para executar atividades em determinados momentos. Podem ser elaborados pelo próprio auditor ou por terceiros.

As ferramentas definidas como utilitários são aquelas próprias para a realização de tarefas comuns de processamento, como concatenar textos, gerar relatórios e sumarizar. A vantagem dos utilitários está na capacidade de servir como substitutos na falta de ferramentas mais completas (Carvalho, 2014).

3.6. TÉCNICAS DE AUDITORIA

As variadas metodologias de auditoria podem ser chamas de técnicas. Tais técnicas podem ser utilizadas pelo auditor a fim de otimizar o processo de auditoria e

manter a organização dos processos. As técnicas mais comuns de auditoria são os testes de observância e a aplicação de questionários, sendo que na primeira o auditor monitora e analisa determinada atividade, e na segunda é aplicada uma lista de perguntas relacionadas ao sistema ou as atividades de um colaborador ou setor. Além destas técnicas, também se destacam: Auditoria assistida por computador; Dados de teste; Simulação paralela; Rastreamento e mapeamento; Analise da lógica de programação (Schmidt, 2006).

3.6.1. TÉCNICAS DE AUDITORIA ASSISTIDA POR COMPUTADOR

As Técnicas de Auditoria Assistida por Computador (TAAC) são programas especializados para gerar amostras, importar dados, sumarizar e testar os controles, condições e processos implantados nos sistemas através das amostras que são selecionadas. Essas técnicas de auditoria assistida por computador são importantes pelo fato de auxiliar o auditor na avaliação do ambiente computacional, que geralmente processa volumes de transações muito extensas, além de auxiliar em tarefas de testes de controles gerais, testes de detalhes de transações, entre outros (Saeta, 2013).

3.6.2. DADOS DE TESTE

Esta técnica envolve o uso de determinado conjunto de dados especialmente projetados e preparados com o objetivo de testar as funcionalidades de entrada de dados do sistema. Após o processamento do arquivo, deve-se verificar os resultados obtidos com os planejados. Além disso, esta técnica pressupõe que os dados sejam abrangentes e verifiquem principalmente os limites de cada intervalo permitido para as variáveis (Lyra, 2008).

Assim, os dados podem ser elaborados por pessoas que possuem um mínimo de conhecimento em informática e existe softwares que auxiliam na geração de dados e tornam a tarefa bastante simples. Entretanto, há dificuldade em planejar e antecipar todas as combinações de transações que possam acontecer em ambiente de negócios da empresa (Lyra, 2008).

3.6.3. FACILIDADE DE TESTE INTEGRADO

Também conhecida por *Integrated Test Facility* (ITF), é melhor aplicada em ambientes *online*. Os dados de testes são introduzidos nos ambientes reais de processamento. O teste envolve a aplicação de entidades fictícias, tais como funcionários fantasmas na folha de pagamento ou cliente inexistente nas contas a receber. Os dados no processamento das transações reais são confrontados com os dados fictícios e os resultados, comparados com os predeterminados. Esta facilidade evita que se atualizem as bases reais da organização com os dados fictícios, criando-se arquivos de resultados em separado. Este procedimento é utilizado em ambiente de produção normal sem a anuência dos operadores ou do gerente de produção (Dias, 2000).

Com isso, a ITF não acarreta nenhum custo adicional, visto que funciona no ambiente de produção das empresas. Entretanto, os efeitos das transações precisam ser estornados, dando trabalhos adicionais e operacionais quando são misturados com dados reais. A quantidade e número de dados fictícios incluídos no ambiente de produção devem ser limitados, a fim de não comprometer o desempenho do sistema em produção. Além disso, existe possibilidade de se contaminar dados reais com dados fictícios no ambiente de produção da empresa, causando transtornos para a organização (Dias,2000).

3.6.4. SIMULAÇÃO PARALELA

Envolve o uso de um software que, comprovadamente, atenda a todas as lógicas necessárias para o teste, simulando as funcionalidades de programa em produção. Faz-se o processamento das transações e/ou dados nos dois programas e compara-se os resultados. É possível utilizar a técnica para rotinas que apresentam resultados recorrentes que são incoerentes. Neste processo, o auditor desenvolve o próprio programa para fazer execução paralela de dados atuais (Lyra, 2008).

Dentre as vantagens no uso da simulação paralela, destacam-se os custos relacionados com a preparação de massa de dados ou dados fictícios que tomam tempo nas técnicas anteriores, que são inexistes na simulação paralela. Além disso, os testes são mais detalhados e mais representativos, passando uma maior

segurança para o auditor. Como desvantagem, há a necessidade do auditor possuir uma habilidade específica para executar uma operação em paralela, atentando para prever o impacto negativo sobre operações, o que não é desejável (Carvalho, 2014).

3.6.5. RASTREAMENTO E MAPEAMENTO

Consiste em criar e implementar uma trilha de auditoria para realizar o acompanhamento os principais pontos da lógica do processamento das transações críticas, registrando seu comportamento e resultados para análise futura. As trilhas de auditoria são rotinas de controle que permitem a recuperação de informações processadas de forma inversa, através da reconstituição da composição das mesmas, devidamente demonstradas, tanto de forma sintética quanto analítica (Lyra, 2008).

Isto ajuda na avaliação dos controles internos que devem ser seguidos, além de permitir a criação de alertas quanto à aplicação de controles operacionais e seus cumprimentos. Contudo, o auditor precisa ter uma habilidade avançada com T.I para que possa interpretar as lógicas de programação, e isto pode aumentar o tempo de processamento das transações (Lyra, 2008).

3.6.6. ANALISE DA LÓGICA DE PROGRAMAÇÃO

Consiste, basicamente, na verificação da lógica de programação com o intuito de comprovar se os scripts dados ao computador são as mesmas encontradas na documentação do aplicativo. Esta técnica pode ser feita manualmente nos principais programas do sistema ou nos mais críticos para o negócio, ou pode ser suportada por ferramentas automatizadas (Lyra, 2008).

3.7. GESTÃO DE RISCOS

O termo risco é usado para representar a probabilidade de qualquer evento que possa gerar prejuízos econômicos e ameaças ao bom funcionamento da empresa.

Para Vitoriano (2012), Gestão de riscos é a adoção de medidas e políticas que visam o equilíbrio entre custos e riscos. Além disso a gestão de riscos comporta os processos de planejamento, direção e controle dos recursos da entidade.

A autora acrescenta que a gestão de risco geralmente é focada nos riscos financeiros das empresas, mas passou-se a englobar também os riscos operacionais, muito relacionados à T.I. Isso porque as violações nas informações e falhas provocam sérias perdas e crises de negócio. O colaborador responsável pela gestão de risco deve planejar e acompanhar todos os processos, intermediá-los e oferecer caminhos e conselhos.

3.8. MELHORES PRÁTICAS

De acordo com Schmidt (2006), a falta de padrões referentes à auditoria de sistemas, mais especificamente para a área de desenvolvimento, dificulta muito a vida dos profissionais da área. Esta despadronização pode ser explicada pelos seguintes fatores:

- A auditoria de sistemas sempre foi concebida como parte da auditoria geral das organizações;

- Normas com relação à execução das tarefas de auditoria não abordam isoladamente a auditoria de sistemas, e sim, como parte do processo de auditoria;

- A auditoria de sistemas sempre foi vista como um avanço nos trabalhos de auditoria normal para acompanhar a aplicação da tecnologia da informação pelas organizações, e nunca como uma profissão isolada.

Como ainda não está convencionado um padrão que seja aceito para auditoria de T.I, várias associações apresentam regras do exercício da profissão, que geralmente orientam a atuação dos profissionais (Schmidt, 2006).

3.8.1. COMITÊ DE PADRÕES DA ASSOCIAÇÃO DE CONTROLE E AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO

Lyra (2008) conceitua algumas das recomendações acerca dos trabalhos do auditor de sistemas, em conformidade com o Comitê de Padrões da Associação de Controle e Auditoria de Tecnologia de Informação:

- Responsabilidade, prestação de contas e autoridade: tais itens acerca da função do auditor devem ser documentadas apropriadamente numa carta proposta ou que faça aderência ao escopo;

- Independência profissional: o auditor precisa ser independente. No relacionamento organizacional, a função do auditor deve ser suficientemente independente do setor que está sob auditoria para permitir uma conclusão imparcial e objetiva da auditoria.

- Ética profissional e padrões: O auditor deve seguir o código de ética profissional do comitê em questão, prezando pelo cumprimento do zelo profissional. Tal zelo profissional e execução dos padrões de auditoria devem estar presentes em todos os aspectos do trabalho do auditor.

- Competência: O auditor, no uso de seus conhecimentos e habilidades, deve ser tecnicamente competente, possuindo habilidades e conhecimento necessários para executar de seu trabalho. Além disso, o auditor precisa manter sua competência técnica através do constante aprimoramento profissional.

- Planejamento: Deve-se planejar devidamente suas tarefas para direcionar os objetivos da auditoria, seguindo os padrões aplicáveis. Durante a execução da auditoria, o auditor deve obter evidência suficiente, confiável, relevante e proveitoso para alcançar, de fato, os objetivos da auditoria. As conclusões devem ser fundamentadas por meio da analise e interpretação apropriada desta evidência.

- Emissão de relatório: O auditor de T.I deve conceder um relatório para a organismo encarregada pelo controle e auditoria geral da empresa. Neste relatório deve conter o escopo, objetivos, período de abrangência, natureza e extensão do trabalho realizado. Deve identificar a organização, os usuários entrevistados e quaisquer restrições à sua circulação. No mesmo relatório, deve-se incluir as observações, conclusões, recomendações e todas as ressalvas que o auditor possua a respeito da auditoria.

- Atividades de *follow-up*: deve-se requisitar e avaliar todas as informações apropriadas sobre pontos, conclusões e recomendações anteriores e relevantes a fim de determinar se ações apropriadas foram implementadas.

3.8.2. ASSOCIAÇÃO DE AUDITORES DE SISTEMAS E CONTROLES

A Associação de Auditores de Sistemas e Controles (ISACA) introduziu o código de ética profissional com objetivo de guiar seus membros na condução de suas atividades. Segundo este código, os membros devem:

- Encorajar e apoiar o cumprimento de tais padrões;

- Exercer as atividades com objetividade e zelo profissional, conforme os padrões profissionais e melhores práticas;

- Dedicar-se aos interesses dos *stakeholders* de forma honesta, zelando pela manutenção do padrão de caráter e conduta profissional, e não encorajar atos de depreciação à profissão;

- Manter confidencialidade dos dados e informações obtidas, exceto quando for exigido legalmente. Tais dados e informações não devem ser usados em vantagem própria ou cedidos a pessoas desautorizadas;

- Manter competência em suas respectivas especialidades, atuando apenas com atividades nas quais tenha habilidade para competir profissionalmente;

- Expor todos os fatos significativos para as partes envolvidas, mantendo-os informados sobre seu trabalho;

- Apoiar a conscientização dos *stakeholders* a fim de auxiliar sua compreensão dos sistemas computacionais, segurança e controle.

A ISACA também administra as certificações CISA (Certified Information Systems Auditor – Certificação de Auditores de Sistemas da Informação), reconhecidas mundialmente como um padrão de realização para aqueles que exercem auditoria, controle, monitoramento e avaliação dos sistemas de informação de negócio nas organizações. Criada em 1978, mais de 75.000 profissionais em cerca de 160 países possuem a certificação CISA, que se tornou um sinônimo de experiência comprovada, credibilidade e conhecimento.

3.8.3. ISO 19011:2011 – DIRETRIZES PARA AUDITORIA DE SISTEMAS DE GESTÃO

A ISO 19011 é uma norma que fornece diretrizes sobre auditoria de sistemas de gestão, incluindo os princípios, a gestão e a realização de auditorias de sistemas, como também orientação sobre a avaliação da competência de pessoas envolvidas no processo de auditoria, incluindo a pessoa que gerencia o programa de auditoria, os auditores e a equipe. Esta norma também introduz o conceito de risco, além de dar enfoque à auditoria combinada, que é quando dois ou mais sistemas de gestão são auditados em conjunto.

Seção 3 – Termos e definições: são definidos os termos de auditoria, critérios, evidências, constatações, conclusão, cliente de auditoria, auditado, auditor, especialista, observador, guia, programa de auditoria, escopo, plano de auditoria, risco, competência, sistema de gestão, conformidade e não conformidade.

Seção 4 – Princípios de auditoria: No que diz respeito aos princípios, a norma considera de forma específica os requisitos de segurança e confidencialidade da informação, para que informações dos clientes, colhidas no ato da auditoria, não sejam usadas de forma indevida (para ganho pessoal do auditor ou terceiros, por exemplo).

Seção 5 – Permite e fornece uma base para gerenciamento de programas de auditoria de mais de um software de gestão. Também há orientação para alocar os recursos de auditoria para auditar os pontos mais importantes dentro do sistema, além de oferecer orientações para definição dos objetivos, critérios e escopo para cada auditoria individualmente. Programas de auditoria precisam ser personalizados, visto o tamanho da entidade, o nível de maturidade do sistema, complexidade e natureza da organização auditada.

Seção 6 – Nesta seção contém orientações sobre como planejar as atividades de auditoria, como o início das atividades de auditoria (estabelecimento de contratos e estudo de viabilidade da auditoria), preparação das atividades da auditoria, condução de tais atividades, preparação e distribuição dos relatórios, conclusão e acompanhamento.

Seção 7 – Trazendo um maior aprofundamento no que diz respeito as competências de avaliação dos auditores, esta norma pode ser utilizada para declarações de conformidade, além de também ser útil para entidades envolvidas na formação e certificação de auditores.

A ISO 19011 ainda conta com 3 anexos, sendo eles o anexo A (que contém competências e conhecimentos específicos de auditores), anexo B (que contém exemplos de avaliações sobre conhecimentos específicos dos auditores) e anexo C (que é uma guia adicional para auditoria em seu planejamento e condução).

Em suma, esta norma oferece orientações sobre a gestão dos programas de auditoria e a condução de auditorias de sistemas de gestão em geral, abordando também alguns aspectos relativos a avaliação das equipes.

4. ESTUDO DE CASO

Neste capítulo será analisado o estudo de caso realizado em três empresas de tecnologia na região de Americana, sendo que tal estudo tem o objetivo de trazer a perspectiva e conhecimento de tais empresas referente à auditoria no desenvolvimento de sistemas, além de analisar a viabilidade da aplicação da mesma.

4.1. DESCRIÇÃO DO ESTUDO DE CASO

O estudo foi feito através de uma pesquisa de campo, composta por um questionário (Apêndice A) disponibilizado na plataforma *Google Forms* e que engloba perguntas de rotinas operacionais das empresas, qualidade de software e a auditoria propriamente dita. A aplicação do questionário foi realizada entre os dias 8 de outubro de 2014 até 17 de outubro de 2014.

Um dos problemas mais comuns no ambiente operacional é garantir que os colaboradores da empresa cumpram normas e padrões em suas respectivas funções, sendo que assim se torna necessário um processo de verificação das atividades desempenhadas pelos colaboradores. A aplicação de uma auditoria possibilita esta verificação das atividades, trazendo ao nível gerencial o real estado da empresa, para que assim ela possa ser guiada por um caminho que corrija tais problemas.

O questionário aplicado em empresas de pequeno porte (como a S&C Informática e a área de Tecnologia da Informação da Secretaria da Educação de Americana) além da empresa de grande porte Sage Brasil Software, é composto por 12 perguntas, sendo que a grande maioria das questões são de múltipla escolha. Todas as questões possuem um objetivo diferente para o estudo de caso, conforme apresentado no quadro 1.

Quadro 1: Estudo de Caso – Questões

Questão	Objetivo da Questão
1) Você sabe o que é auditoria?	Partindo de um ponto de vista amplo, esta questão visa saber se a empresa possui conhecimento (seja profundo ou limitado)

	sobre a auditoria em sua forma mais genérica. A partir do momento que se tem uma noção do assunto, abre-se margens para saber mais detalhes do procedimento e como ela pode ser implementada para trazer benefícios à empresa.
2) Você considera a auditoria de sistemas importante para sua empresa?	Ainda com uma abordagem genérica do assunto, esta questão avalia o nível de interesse da corporação sobre o assunto. Uma vez que se tem interesse sobre o tema, aumenta-se a possibilidade de aplicação da auditoria.
3) Sua empresa costuma passar por algum tipo de auditoria, seja interna ou externa?	Procura-se conhecer mais sobre a atual situação da empresa, analisando o cenário para saber se a mesma já vivencia a auditoria. Assim, consegue-se uma perspectiva de aplicabilidade, pois uma empresa que já passa regularmente por esse procedimento está mais suscetível a implementar outros tipos de auditoria.
4) Caso a resposta da pergunta anterior seja “Sim”, com que frequência são realizadas auditorias na sua empresa?	Caso a empresa já passe regularmente por um auditoria, esta pergunta busca analisar o período no qual o procedimento é aplicado.
5) Você conhece a ISO 9126 ou algum outro padrão de qualidade de software?	De acordo com Côrtes (1998), a ISO 9126 é descrita como uma norma focada na qualidade do software, propondo atributos de qualidade, nos quais são distribuídos em categorias, tais como: Funcionalidade; Eficiência, Usabilidade, Confiabilidade, Manutenibilidade e Portabilidade. O intuito desta questão é saber se a empresa trabalha com algum padrão de qualidade (seja a ISO 9126 ou algum outro), pois esta informação mostra que a empresa possui preocupação em entregar um produto de qualidade e assim abre-se espaço para que

	a auditoria seja apresentada como uma ferramenta para consolidar a busca pela qualidade do sistema.
6) Dentre os benefícios que uma auditoria de sistemas proporciona para a qualidade de software, quais dos itens abaixo são de seu conhecimento? (A) Identificação dos setores ou funcionários que não cumprem corretamente determinadas tarefas essenciais no desenvolvimento de software (B) Redução dos riscos de um sistema falho (C) A representação do real estado do projeto através de dados obtidos pela auditoria (D) A implementação de boas práticas no desenvolvimento de software, que é consequente das atividades do auditor. (E) Não sei responder	Caso a empresa não conheça a auditoria no desenvolvimento de sistemas, aqui ela já é apresentada mais intimamente aos benefícios e resultados que pode-se conseguir ao adotar esse procedimento na empresa. Caso ela já conheça, com esta pergunta se obtém os itens na qual as empresas mais recorrem a uma auditoria, quando focada no desenvolvimento de sistemas.
7) Na sua opinião, qual é a maior desvantagem de uma auditoria de sistemas? (A) Custo (B) Tempo gasto com orientações (C) Atende mais as necessidades do nível gerencial/estratégico da empresa (D) Outros	O principal objetivo desta pergunta é descobrir qual a maior barreira que impede a aplicação da auditoria na corporação, para que assim sejam identificados meios de se romper tais barreiras e tornar viável a aplicação da auditoria.
8) O desenvolvimento de sistemas na sua empresa é guiado por algum processo de verificação/validação de software?	Esta pergunta serve de apoio a questão número 5, sendo que aqui se obtém a garantia de que a empresa realmente é preocupada com a qualidade de software ao implementar processos de verificação e validação.
9) Qual a metodologia de desenvolvimento utilizada na sua empresa?	Visando o ciclo de desenvolvimento de software apresentado no capítulo 2, esta pergunta busca conhecer como é feito o

	procedimento de desenvolvimento dos sistemas na empresa, para que assim seja identificado os itens que o auditor precisaria saber da rotina operacional para implementar a auditoria.
10) Para você, a presença de um auditor na empresa já faz com que haja mudanças no comportamento dos funcionários?	No ato da aplicação da auditoria (principalmente externa), os funcionários automaticamente já ficam mais atentos as suas atividades, pois uma pessoa estranha do seu cotidiano verificando seus afazeres gera insegurança no indivíduo e faz com que ele desempenhe o seu melhor (Schmidt, 2006), ou seja, mesmo que a auditoria não detecte nenhuma irregularidade no período que ela foi aplicada (que varia de acordo com a complexidade do projeto), a auditoria inevitavelmente traz benefícios para a empresa auditada. Assim, com a questão 10 busca-se saber se a empresa possui conhecimento deste benefício ao aplicar uma auditoria.
11) Qual técnica de auditoria já foi aplicada na sua empresa?	Com esta pergunta se obtém as técnicas de auditoria mais corriqueiras nas corporações.
12) Você sabe qual ferramenta foi utilizada para realizar a auditoria?	Assim como a pergunta 11, esta questão é específica no que se refere aos processos de auditoria. Assim, é identificado se as empresas possuem conhecimentos profundos sobre o tema.

Fonte: Autor (2014)

4.2. RESULTADOS OBTIDOS

Após o fim da aplicação do questionário, que se deu no dia 17 de outubro de 2014, os resultados obtidos (Anexo A) foram transportados para o quadro 2.

Quadro 2: Estudo de Caso – Respostas

Indicação de data e hora	**17/10/2014 16:03**	**15/10/2014 15:03**	**08/10/2014 16:34**
Nome da empresa	*Sage Brasil Software*	*S&C Informática*	*Secretaria da educação*
1) Você sabe o que é auditoria?	Sim	Sim	Sim
2) Você considera a auditoria de sistemas importante para sua empresa?	Sim	Não	Sim
3) Sua empresa costuma passar por algum tipo de auditoria, seja interna ou externa?	Sim	Não	Não
4) Caso a resposta da pergunta anterior seja “Sim”, com que frequência são realizadas auditorias na sua empresa?	De ano em ano	-	-
5) Você conhece a ISO 9126 ou algum outro padrão de qualidade de software?	iso 27001 - 27002	Spice e ISO 9126	ISO 9126
6) Dentre os benefícios que uma auditoria de sistemas proporciona para a qualidade de software, quais dos itens abaixo são de seu conhecimento?	A, B, C, D	A, B, C, D	B, C
7) Na sua opinião, qual é a maior desvantagem de uma auditoria de sistemas?	Tempo gasto com orientações	Custo	Custo
8) O desenvolvimento de sistemas na sua empresa é guiado por algum processo de verificação/validação de software?	Sim	Sim	Sim
9) Qual a metodologia de desenvolvimento utilizada na sua empresa?	Scrum	Scrum	Incremental
10) Para você, a presença de um auditor na empresa já faz com que haja mudanças no comportamento dos funcionários?	Sim	Sim	Sim
11) Qual técnica de auditoria já foi aplicada na sua empresa?	Questionários, Outros	-	Questionários, Observância
12) Você sabe qual ferramenta foi utilizada para realizar a auditoria?	Não sei responder	Não sei responder	Não sei responder

Fonte: Autor, 2014

4.3. ANALISE E DISCUSSÃO DOS RESULTADOS

Visto os objetivos das questões apresentados no quadro 1, foram analisadas as respostas obtidas com o questionário (quadro 2) para averiguar a viabilidade de aplicação da auditoria, e dentre os principais pontos desta abordagem, destacam-se:

- Todas as empresas possuem conhecimento sobre Auditoria de Sistemas e a maioria delas consideram a auditoria importante para a empresa, conforme apresentado com as respostas referentes às questões 1 e 2 do quadro 2. De acordo com Oliveira (2008), as atividades de gerenciamento em pequenas empresas são mais ágeis devido à baixa quantidade de funcionários bem como o fluxo de informações, o que torna, muitas vezes, inviável a aplicação da auditoria. No entanto, nota-se que empresas de pequeno porte já possuem um interesse pelas atividades em torno da auditoria de sistemas, mesmo que este interesse não seja absoluto em todas as empresas de pequeno porte.

- Conforme apresentado no quadro 2, a Sage Brasil Software é a única das empresas que aplica algum tipo de auditoria, sendo elas realizadas de ano em ano.

- A quinta pergunta do questionário se refere à ISO 9126. De acordo com Côrtes (1998), esta norma é descrita como uma norma focada na qualidade do software, propondo atributos de qualidade. A maioria das empresas avaliadas no estudo de caso possuem conhecimento deste padrão de qualidade. Também foram citadas as **ISOs 27001**, **27002** e **15504 (SPICE)** como parte integrante da bagagem de conhecimento referente aos padrões de qualidade. Isto mostra como as empresas estão comprometidas em garantir a qualidade de seus produtos e assim surgem possibilidades da auditoria ser oferecida como meio de garantir este objetivo.

- Os benefícios mais conhecidos pelas empresas referente a auditoria, são a **redução dos riscos de um software falho** e a **representação do real**

estado do projeto através de dados obtidos pela auditoria. É notável que mesmo a maioria das empresas não passando por um tipo de auditoria, as mesmas possuem conhecimento dos benefícios que esta prática oferece para a empresa, tornando a aplicação da auditoria em uma alternativa de verificação dos dados quando o cenário da corporação se tornar favorável a isto.

- O **custo** é listado como a principal desvantagem da auditoria, conforme apresentado no quadro 2. Isto vai de encontro com as afirmações de Oliveira (2008), onde o autor apresenta que em uma pequena empresa, as atividades gerenciais são de fácil execução devido a baixa quantidade de funcionários, fazendo com que outros recursos de gerenciamento e verificação sejam vistos como custos desnecessários. Entretanto, quando é aplicado o Gerenciamento de Custo do Projeto, de acordo com a Guia PMBOK (Corpo de conhecimento em gerenciamento de projetos), os processos envolvidos no planejamento, estimativas, orçamentos, financiamentos, gerenciamento e controle de custos, permitem que as atividades sejam executadas dentro do orçamento da empresa. Ou seja, esta desvantagem pode ser driblada ao aplicar o gerenciamento de custo do projeto, uma vez que os recursos necessários para as atividades da empresa serão gerenciados de tal modo que permite a locação financeira necessária para aplicação da auditoria.

- Todas as empresas citaram que utilizam algum processo de verificação/validação de software, o que reafirma o comprometimento das empresas com a qualidade de seus produtos, abrindo mais espaço para a aplicação da auditoria. Quando questionados sobre qual metodologia de desenvolvimento é aplicada no dia-a-dia, a metodologia **Scrum** é tida como a mais utilizada pelas empresas, o que vai de encontro ao que Shore sintetiza em seu estudo, na qual as metodologias ágeis passaram a ser bastante utilizadas nas mais diversas corporações nos últimos anos (Shore, 2007).

- No que se refere a aplicação da auditoria, todas as empresas reconhecem que a presença do auditor já faz com que haja mudanças no comportamento dos funcionários. Quanto as técnicas de auditoria, os **questionários** e **testes de observância** são tidos como os mais comuns para as empresas.

- A última pergunta do questionário é referente as ferramentas de auditoria utilizadas por um auditor, no entanto, nenhuma soube responder qual ferramenta já viram ser aplicadas, como softwares específicos (Galileo, Pentana, ACL) ou o uso de trilhas de auditoria.

Com base nas respostas obtidas e analisando-as juntamente com os objetivos das questões, conclui-se que as empresas possuem um cenário favorável para a aplicação de uma auditoria e que esta tarefa operacional é capaz de trazer resultados sólidos para garantir a execução correta em torno das atividades inclusas no ciclo de desenvolvimento de software. No entanto, a principal barreira para esta aplicação, principalmente para empresas de pequeno porte, é o custo de uma auditoria, mas esta barreira pode facilmente se dissipar ao aplicar o Gerenciamento de Custo do Projeto, permitindo um gerenciamento eficaz dos recursos orçamentários da empresa e viabilizando financeiramente a aplicação da auditoria.

A área da Tecnologia da Informação está a cada dia mais competitiva e as empresas estão cada vez mais preocupadas em se manterem ativas no ramo, e consequentemente elas passam a prezar pela qualidade de seus produtos. O fato das empresas conhecerem a ISO 9126 e outros padrões de qualidade reconhecidos internacionalmente, comprovam esta realidade marcada pelo prezar em oferecer um produto que satisfaça e exceda as expectativas de seus clientes.

A consciência de que a auditoria reduz os riscos de um sistema falho e traz uma representação real do estado dos projetos em desenvolvimento na empresa, faz da auditoria uma importante aliada para ajudar a empresa a se situar no competitivo ramo da Tecnologia da Informação, suprindo a necessidade de garantir um software de qualidade através de um ponto de partida que reduzirá os riscos que possam comprometer os projetos.

Enfim, apesar da auditoria de sistemas não ser uma atividade muito comum nas corporações, ela pode ser aplicada para se garantir a qualidade de um software, visto que ela alinha as atividades descritas no capítulo 2 de acordo com os padrões de qualidade que as próprias empresas possuem, se tornando, assim, em uma alternativa para atingir os resultados esperados pela gerência da corporação.

5. CONSIDERAÇÕES FINAIS

O objetivo desse trabalho de conclusão de curso foi mostrar um estudo bibliográfico sobre a auditoria de sistemas aplicada no desenvolvimento de software, analisando os benefícios que ela proporciona para alinhar o trabalho executado pela empresa com os padrões de qualidade e normas da área. Tendo o conhecimento sobre como é produzido um software, além de todas as atividades e recursos que se fazem necessárias para este processo, o auditor pode se dispor de diversas ferramentas e técnicas para identificar os processos defeituosos dentro do ciclo de desenvolvimento, guiando a corporação para realizar as devidas melhorias. Portanto, conclui-se que há diversas vantagens para a empresa que deseja aplicar uma auditoria de sistemas (como a redução dos riscos de um software falho e implementação de boas práticas no desenvolvimento de software), visto que ela se torna viável até mesmo para empresas de pequeno porte, conforme apresentado no estudo de caso. A aplicação da auditoria na prática não faz parte do escopo deste trabalho, visto sua natureza bibliográfica. Entretanto, esta aplicação da auditoria pode ser feita em estudos futuros, onde os procedimentos descritos no capítulo 3 seriam colocados em prática no ambiente empresarial.

GLOSSÁRIO DE TERMOS

BRAINSTORM: Trata-se de uma dinâmica em grupo, adotada como uma técnica em várias empresas a fim de resolver problemas específicos ou desenvolver novas ideias.

WORKFLOW: Fluxo de trabalho.

CHECK-LISTS: É um instrumento de controle, onde encontra-se uma lista de procedimentos que deve ser seguida

ONLINE: Em computação esse termo é usado para indicar que um usuário ou sistema está conectado ou ativo.

FOLLOW-UP: Trata-se do acompanhamento ou avaliação de algo que já foi feito.

STAKEHOLDER: Em tecnologia da informação, esse termo é utilizado para designar as pessoas ou grupos mais importantes para o planejamento estratégico de um projeto, ou seja, são as partes interessadas.

GOOGLE FORM: Plataforma do Google para criação de formulários na internet

REFERÊNCIAS

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Referências: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

BAESSO, M. A. S. **Diagrama de caso de uso e diagrama de sequência**. 2004. Disponível em: <http://www.dmo.fee.unicamp.br/~henrique/cursoc++/diagrama.pdf> Acesso em 14. Jun. 2014. 19h45.

BITTENCOURT, D. F de. **Auditoria de sistemas informatizados**. 3ª ed. UnisulVirtual. 2007

CARNEIRO, G. **Conceitos de auditoria de sistemas**. Disponível em: <http://pt.slideshare.net/sorayaNadja/aula-04-coneitos-de-auditoria-de-sistemas> Acesso em 04 Set. 2014. 19h30.

CAROLINE, A. **Testes de software**. Disponível em: <http://gtsw.blogspot.com.br/2007/10/tipos-de-testes-de-software.html> Acesso em 12 Mar. 2014. 15:45

CARVALHO, C. **Segurança e auditoria de sistemas**. Disponível em: <http://pt.slideshare.net/augustoseixas/introduo-auditoria> Acesso em 19. Out. 2014. 20h30.

CONAB. **Manual de auditoria interna**. Coaud – Coordenadoria de auditoria interna. 2ª Versão. 2008. Disponível em: <http://www.conab.gov.br/downloads/regulamentos/ManualdeAuditoriaInterna.pdf> Acesso em 14. Jun. 2014. 21h00.

CÔRTES, M. L., **Modelos de qualidade de software**. 1998. Disponível em: <http://www.ic.unicamp.br/~cortes/mc726/cap3.pdf> Acesso em 25. Out. 2014 19h15.

DIAS, C. **Segurança e auditoria da tecnologia da informação**. 1ª ed. Axcel Books. Rio de Janeiro, 2000.

EDNA, F. S.,MIRANDA, M. A. P., **Auditoria de sistemas**. 2004. Curso de ciências contábeis – FACAPE, Petrolina, Pernambuco. 2004.

FIGUEIREDO, E. **Requisitos funcionais e requisitos não funcionais**. Disponível em: <http://homepages.dcc.ufmg.br/~figueiredo/disciplinas/aulas/req-funcional-rnf_v01.pdf> Acesso em 03 Set. 2014. 19h00.

GIL, A. L. **Auditoria de computadores**. Atlas. 2000

IMONIANA, J. O. **Auditoria de sistemas da informação**. 2ª ed. São Paulo. Atlas. 2011. p. 54 – 190.

ISACA. **Code of professional ethics**. Disponível em: <http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx> Acesso em 18 Set. 2014. 18h10.

ISO ISO/IEC 19011:2011. **Guidelines for auditing management systems**. ISO Online Catalogue. 2011

KOSCIANSKI, A. SOARES, M.S dos. **Qualidade de software. Aprenda as metodologias e técnicas mais modernas para o desenvolvimento de software**. 2ª ed. São Paulo: Novatec editora. 2007. p. 157-169.

LYRA, M. R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro. Editora Ciência Moderna Ltda. 2008.

MENDES, S. **Auditoria com qualidade. Inventário de parque computacional com Open-Audit**. Linux Magazine. Vol. 71. Out. 2010. Disponível em: <http://www.linuxnewmedia.com.br/images/uploads/pdf_aberto/LM_71_64_67_04_tut_openaudit.pdf> Acesso em 09 Dez. 2014. 11h26.

MOORE, S. **Como funciona uma auditoria de sistemas?** 2012. Disponível em: <http://msbrasil.com.br/blog/contabilidade/como-funciona-uma-auditoria-de-sistemas/> Acesso em: 03 Set. 2013. 21h30.

MOTA, K. **Ciclo de desenvolvimento de software**. Disponível em: <http://www.klebermota.eti.br/2013/09/04/ciclo-de-desenvolvimento-de-software/> Acesso em 16 Nov. 2013. 15h25

OLIVEIRA, J. A. **Método de auditoria a sistemas de informação**. Porto Editora. 2006

OLIVEIRA, L. M. de, DINIZ FILHO, A., GOMES, M. B. **Curso básico de auditoria**. 2ª ed. Atlas. São Paulo. 2008.

PAULA FILHO, W. P. **Engenharia de software. Fundamentos, métodos e padrões**. 3ª ed. Rio de Janeiro. LTC. 2009.

PMI. **Um guia do conhecimento em gerenciamento de projetos (Guia PMBOK)**. 5ª Ed. Saraiva. 2014

PRESSMAN, R. S. **Engenharia de software**. 7ª ed. The McGraw-Hill. 2011

RIOS, E., RODRIGUES, T. **Projeto e engenharia de software – teste de software**. Rio de Janeiro. Alta Books. 2002.

SAETA, P. **Auditoria em sistemas de informação**. Disponível em: <http://paulosaeta.wordpress.com/2011/12/06/auditoria-em-sistemas-de-informacao/> Acesso em 03 Set. 2013. 21h35.

SCHMIDT, P., SANTOS, J. L. dos, & ARIMA, C. H. **Fundamentos de auditoria de sistemas**. Vol. 9. Atlas. 2006.

SHORE, J., WARDEN, S. **The art of agile development**. 1ª ed., O'Reilly Media. 2007

SOMMERVILLE, I. **Engenharia de software**. 9ª ed. Pearson Education. 2011

VITORIANO, B. C. **Gestão de risco**. Disponível em: <http://www.portaleducacao.com.br/educacao/artigos/12107/gestao-de-risco-voce-sabe-o-que-e> Acesso em 08 Set. 2014. 19h00.

APÊNDICE A – Questionário

Estudo de Caso - Auditoria no Desenvolvimento de Software

O objetivo deste questionário é a coleta de informações que possibilitem conhecer a perspectiva e discernimento dos profissionais de T.I em relação à Auditoria de Sistemas, para que assim, seja identificado as causas que favorecem ou não a aplicação da auditoria no ambiente de T.I

1) Você sabe o que é auditoria?

- ○ Sim
- ○ Não

2) Você considera a auditoria de sistemas importante para sua empresa?

- ○ Sim
- ○ Não

3) Sua empresa costuma passar por algum tipo de auditoria, seja interna ou externa?

- ○ Sim
- ○ Não

4) Caso a resposta da pergunta anterior seja “Sim”, com que frequência são realizadas auditorias na sua empresa?

- ○ A cada 3 meses
- ○ A cada 6 meses
- ○ De ano em ano
- ○ Não sei responder

5) Você conhece a ISO 9126 ou algum outro padrão de qualidade de software?

6) Dentre os benefícios que uma auditoria de sistemas proporciona para a qualidade de software, quais dos itens abaixo são de seu conhecimento?

- [ ] A - Identificação dos setores ou funcionários que não cumprem corretamente determinadas tarefas essenciais no desenvolvimento de software
- [ ] B - Redução dos riscos de um sistema falho
- [ ] C - A representação do real estado do projeto através de dados obtidos pela auditoria
- [ ] D - A implementação de boas práticas no desenvolvimento de software, que é consequente das atividades do auditor.
- [ ] Não sei responder

7) Na sua opinião, qual é a maior desvantagem de uma auditoria de sistemas?

- ( ) Custo
- ( ) Tempo gasto com orientações
- ( ) Atende mais as necessidades do nível gerencial/estratégico da empresa.
- ( ) Outros

8) O desenvolvimento de sistemas na sua empresa é guiado por algum processo de verificação/validação de software?

- ( ) Sim
- ( ) Não

9) Qual a metodologia de desenvolvimento utilizada na sua empresa?

10) Para você, a presença de um auditor na empresa já faz com que haja mudanças no comportamento dos funcionários?

- Sim
- Não

11) Qual técnica de auditoria já foi aplicada na sua empresa?

- Observância
- Questionários
- Técnica de Auditoria Assistida por Computador (TAAC)
- Dados de testes
- Outros
- Não sei responder

12) Você sabe qual ferramenta foi utilizada para realizar a auditoria?

- Software Galileo
- Software Pentana
- Software ACL
- Trilhas de auditoria
- Não sei responder

ANEXO A – Respostas obtidas com o questionário

1) Você sabe o que é auditoria?
   Sage Brasil Software: Sim
   S&C Informática: Sim
   Secretaria da educação: Sim

2) Você considera a auditoria de sistemas importante para sua empresa?
   Sage Brasil Software: Sim
   S&C Informática: Não
   Secretaria da educação: Sim

3) Sua empresa costuma passar por algum tipo de auditoria, seja interna ou externa?
   Sage Brasil Software: Sim
   S&C Informática: Não
   Secretaria da educação: Não

4) Caso a resposta da pergunta anterior seja “Sim”, com que frequência são realizadas auditorias na sua empresa?
   Sage Brasil Software: De ano em ano
   S&C Informática: -
   Secretaria da educação: -

5) Você conhece a ISO 9126 ou algum outro padrão de qualidade de software?
   Sage Brasil Software: ISO 27001 - 27002
   S&C Informática: Spice e ISO 9126
   Secretaria da educação: ISO 9126

6) Dentre os benefícios que uma auditoria de sistemas proporciona para a qualidade de software, quais dos itens abaixo são de seu conhecimento?
   Sage Brasil Software: A, B, C, D
   S&C Informática: A, B, C, D
   Secretaria da educação: B, C

7) Na sua opinião, qual é a maior desvantagem de uma auditoria de sistemas?

   Sage Brasil Software: Tempo gasto com orientações

   S&C Informática: Custo

   Secretaria da educação: Custo

8) O desenvolvimento de sistemas na sua empresa é guiado por algum processo de verificação/validação de software?

   Sage Brasil Software: Sim

   S&C Informática: Sim

   Secretaria da educação: Sim

9) Qual a metodologia de desenvolvimento utilizada na sua empresa?

   Sage Brasil Software: Scrum

   S&C Informática: Scrum

   Secretaria da educação: Incremental

10) Para você, a presença de um auditor na empresa já faz com que haja mudanças no comportamento dos funcionários?

   Sage Brasil Software: Sim

   S&C Informática: Sim

   Secretaria da educação: Sim

11) Qual técnica de auditoria já foi aplicada na sua empresa?

   Sage Brasil Software: Questionários, outros

   S&C Informática: -

   Secretaria da educação: Questionários, Observância

12) Você sabe qual ferramenta foi utilizada para realizar a auditoria?

   Sage Brasil Software: Não sei responder

   S&C Informática: Não sei responder

   Secretaria da educação: Não sei responder