Auditoria em Sistemas de Informação

Graduação Tecnológica: Tecnologia da Informação

Autor: Prof. Carlos Eduardo Gertners de Magalhães

SUMÁRIO

LISTA DE FIGURAS

UNIDADE I – INTRODUÇÃO

1.1-Auditoria nas organizações

Auditoria → **1** Cargo de auditor. **2** Casa ou tribunal onde o auditor desempenha as suas funções. **3** Função de auditor junto às empresas comerciais. **4** *Econ* Exame analítico minucioso da contabilidade de uma empresa ou instituição.

Entidades governamentais e privadas, independente de porte ou ramo de atividade, convivem e subsistem graças a doses cada vez mais elevadas de tecnologia computacional.

A maioria das organizações de hoje não conseguem funcionar nem por poucas horas com a ausência dos computadores.

A auditoria pode ser interna ou externa. Pode ser uma auditoria permanente (constante) ou esporádica (eventual).

Auditoria Interna → Com o aumento da complexidade das operações de uma empresa, aumentou a necessidade de normas e procedimentos internos (controles internos). Como o proprietário da empresa (ou o administrador) não poderia fazer isto, alguém deveria fazer isto por ele. Daí surge a figura do auditor interno cuja função principal é verificar se as normas internas vem sendo seguidas. Paralelamente o auditor interno executa auditoria contábil. O auditor interno é funcionário da empresa mas como executa auditoria contábil e operacional, deve ter uma certa independência dentro da entidade. Em empresas de grande porte, existe um verdadeiro departamento de auditoria interna.

Auditoria Externa → É feita por um profissional totalmente independente da empresa auditada. O objetivo do auditor externo é emitir uma opinião (chamado parecer) sobre as demonstrações financeiras. Note que o objetivo é apenas emitir um parecer sobre as demonstrações contábeis. Logo conclui-se que a auditoria externa não é realizada para detectar fraudes, erros ou para interferir na administração da empresa, ou ainda, reorganizar o processo produtivo ou demitir pessoas ineficientes. Naturalmente, no decorrer do processo de auditoria, o auditor pode encontrar fraudes ou erros, mas o seu objetivo não é este. Seu objetivo é emitir um parecer.

A auditoria nas organizações é um instrumento da direção da entidade, dos acionistas, do ambiente externo à organização, do povo para validar e avaliar a qualidade em termos de segurança, eficiência dos trabalhos desenvolvidos com a tecnologia computacional.

O advento do microcomputador provocou pulverização acentuada da tecnologia de processamento eletrônico de dados (PED), e a distribuição e a descentralização da criação e da execução de processos computadorizados constituem a tônica empresarial atual.

Podemos considerar que PED apóia e sustenta todas as atividades meio e fim das organizações, sendo imprescindível a aproximação dos profissionais de computação com os profissionais responsáveis pelas atividades meio e fim das empresas.

Na realidade, o modelo de implantação de PED é a transferência dessa tecnologia diretamente ao usuário, através de linguagens de programação de 4ª geração ou do uso da inteligência artificial, eliminando ou diminuindo a participação de uma série de profissionais de computação (programadores, digitadores, operadores de computador, etc).

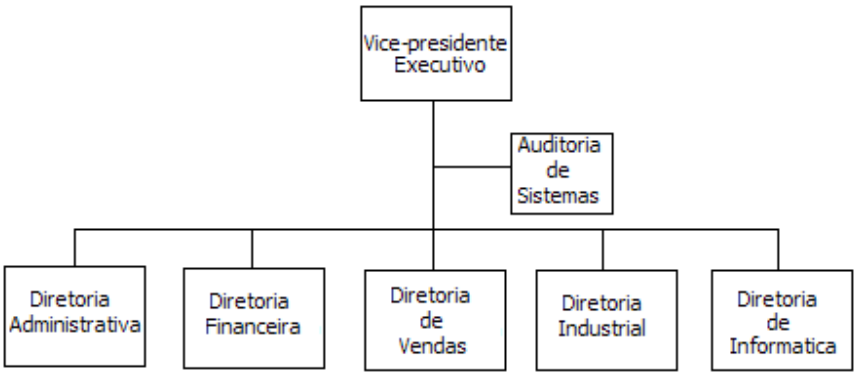

Figura 1: Ambiente empresarial e situação da área de informática e da área de auditoria de sistemas

ATIVIDADE	OBJETIVOS	CARACTERÌSTICAS COMPUTACIONAIS
EMPRESARIAL	- Evolução tecnológica - Poder de competição - Capacidade de adaptação - Especialização - Crescimento	- Crescentes investimentos em tecnologia de computação - Necessidade de treinamento em processamento eletrônico de dados aos funcionários - Iniciando convívio com o conceito de inteligência artificial
COMPUTAÇÃO	- Apoio e envolvimento do usuário - Disseminação da inteligência artificial - Total integração empresarial	- Falta de profissionais de computação, com a necessidade de investimentos nos profissionais existentes, para o posterior repasse de tecnologia e sustentação do pessoal usuário - Necessidade de especialização de profissionais de computação
AUDITORIA DE SISTEMAS	- Velocidade no acompanhamento do binômio “computação-empresa” - Agente de maior participação do computador na empresa	- Forte evolução da área em termos de compreensão do papel da auditoria de sistemas por parte do auditor contábil-financeiro - Tecnologia em intensa evolução - Escassez de profissionais

Evolução da computação no ambiente empresarial e consequente acompanhamento pela auditoria de sistemas

1.2-Importância da auditoria de sistemas

Sistemas de informação adquiriram uma importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.

A esta constatação, você pode adicionar o fato de que hoje em dia não existem mais empresas que não dependam da tecnologia da informação, num maior ou menor grau. Pelo fato de que esta mesma tecnologia permitiu o armazenamento de grande quantidade de informações em um local restrito e centralizado, criou-se aí uma grande oportunidade ao acesso não autorizado.

A segurança da informação tornou-se estratégica, pois interfere na capacidade das organizações de realizarem negócios e no valor de seus produtos no mercado.

Visando minimizar as ameaças, a ISO (International Standardization Organization) e a ABNT (Associação Brasileira de Normas Técnicas), em sintonia com a ISO, publicaram uma norma internacional para garantir a segurança das informações nas empresas, a ISO 17799:1. As normas ISO e ABNT são resultantes de um esforço internacional que consumiu anos de pesquisa e desenvolvimento para se obter um modelo de segurança eficiente e universal.

Este modelo tem como característica principal tentar preservar a disponibilidade, a integridade e o caráter confidencial da informação.

O **comprometimento do sistema de informações**, por problemas de segurança, pode causar grandes prejuízos à organização. Diversos tipos de incidentes podem ocorrer a qualquer momento, podendo atingir a informação confidencial, a integridade e disponibilidade.

Problemas de **quebra de confidência,** por vazamento ou roubo de informações sigilosas, podem expor para o mercado ou concorrência as estratégias ou tecnologias da organização, eliminando um diferencial competitivo, comprometendo a sua eficácia, podendo perder mercado e até mesmo ir à falência.

Problemas de disponibilidade podem ter um impacto direto sobre o faturamento, pois deixar uma organização sem matéria-prima ou sem suprimentos importantes ou mesmo, o impedimento de honrar compromissos com clientes, prejudicam sua imagem perante os clientes, gerando problemas com custos e levando a margem de lucro a ficar bem comprometida.

Problemas de integridade, causados por invasão ou fatores técnicos em dados sensíveis, sem uma imediata percepção, irão impactar sobre as tomadas de decisões. Decisões erradas fatalmente reduzirão o faturamento ou aumentarão os custos, afetando novamente a margem de lucros.

A **invasão da página de Internet de uma empresa**, com modificação de conteúdo, ou até mesmo a indisponibilidade de serviços on-line, revela a negligência com a segurança da informação e causa perdas financeiras a quem sofreu algum tipo de ataque.

A auditoria é de suma importância para os negócios, independente de sua origem, seja ela contábil ou de tecnologia de informação. O termo auditoria é relacionado com diversas áreas de nossa sociedade.

1.3-Necessidades na área de auditoria de sistemas

Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes cada vez mais especializadas para a sua implementação e gerência.

Constatou que o crescente uso de soluções informatizadas dentro das empresas cresceu muito nos últimos anos. Um novo mundo de oportunidades surgiu com o uso descontrolado dos sistemas de informação, havendo a necessidade iminente de controle e as empresas optaram por um plano de auditoria.

Necessidade do envolvimento da alta direção, que terá a responsabilidade de fazer refletir o caráter oficial da política da empresa através de comunicação e compartilhamento com seus funcionários.

A auditoria surgiu então da necessidade de confirmação por parte dos investidores e proprietários, dos valores retratados no patrimônio das empresas que possuíam ou as que pretendiam realizar seus investimentos, principalmente com o grande crescimento econômico-financeiro e com o aparecimento das grandes empresas que são representadas em vários países.

Existe a necessidade de segurança em sistemas de informação em poder saber quais ações foram executadas e quem as executou. Neste contexto, torna-se necessário um mecanismo de gravação e recuperação das ações ou eventos que foram realizados no sistema. É de grande importância que as informações geradas por este mecanismo sejam precisas, pois formarão as trilhas de auditoria. A geração de trilhas de auditoria, a análise e a forma de armazenamento são definidas de acordo com a necessidade da aplicação e são os principais pontos para o planejamento de um sistema de auditoria.

1.4-Papel do auditor de sistemas

O auditor de sistemas informatizados é uma pessoa que acima de tudo deve estar atenta às novidades de mercado, pois todos os dias são descobertas novas formas de se invadir os computadores e redes.

Para garantir que os investimentos feitos em tecnologia da informação retornem para a empresa na forma de lucros, custos menores e um menor custo total de propriedade é que o auditor de sistemas informatizados irá atuar. De posse dos objetivos, normas ou padrões da corporação o auditor irá verificar se tudo está funcionando como deveria.

De mero fiscalizador de processos, o auditor de sistemas tornou-se um profissional com participação estratégica no desenvolvimento da competitividade da empresa.

Para se ter uma noção do crescimento da profissão de auditor, observe que em 1900 eram apenas 250 auditores autorizados a exercer a profissão nos Estados Unidos e hoje são mais de 500.000. (Fonte: Wise, 2002).

Os sistemas informatizados têm afetado duas funções básicas dos auditores: coleta e avaliação das evidências.

Coletar evidências sobre a segurança em um sistema informatizado é muito mais complexo do que em um sistema manual, sem automação, justamente devido à diversidade e complexidade da tecnologia de controle interno. Os auditores devem entender estes controles e ter know-how para coletar evidências corretamente.

Com seu conhecimento do negócio, o auditor pode reconhecer que uma companhia não está utilizando adequadamente os seus ativos de informação e pode fazer recomendações sobre como outras empresas o fazem ou, até mesmo, como as normas e padrões de segurança mais conceituados no mercado o fariam.

O auditor ocupa posição privilegiada em nossa sociedade por entender o funcionamento de várias organizações e saber de que forma elas utilizam os recursos de tecnologia para atingir seus objetivos.

É possível resumir, em três características, os principais valores de um auditor:

. manter princípios éticos;
. possuir integridade;
. possuir objetividade.

Auditores necessitam de grande capacidade de comunicação, pois o serviço pede que ao levantar-se questões relacionadas com o objeto auditado, a discussão seja levada para a camada executiva da empresa e os resultados deste trabalho também.

O auditor deve procurar fazer com que suas competências não somente sejam ditadas por normas, mas decorram de foco no cliente e no mercado.

Os principais serviços prestados por auditores são:

assurance;
consultoria gerencial;
certificação de normas.

Assim, os serviços de ***assurance*** são as traduções de informações provindas dos recursos encontrados no objeto auditado, melhorando o contexto e a qualidade para que a camada executiva possa tomar suas decisões.

Os serviços de **consultoria gerencial** abrangem as recomendações sobre como utilizar os sistemas de informação do cliente de uma forma mais proveitosa e que atenda aos objetivos de negócio da empresa auditada.

Os serviços de **certificação de normas** são aqueles em que o auditor irá prover um *check-list* apontando conformidades e não-conformidades segundo determinada norma e irá emitir uma parecer sobre a emissão ou não para uma empresa daquele certificado.

1.5- Tendências da Auditoria de Sistemas na Organização

Internet → Fazer com que sejam criadas novas ferramentas e técnicas de auditoria através da internet.

Comércio Eletrônico → Criar utilitários, ferramentas de auditoria mais específicas para o comércio eletrônico. Que está tendo uma grande utilização.

BPR → Business Process Reengineering. Reengenharia de processos do negócio. Melhorias que visam uma aproximação da gerência por meio do aumento da eficiência e a eficácia dos processos no qual existem dentro das organizações.

Privacidade dos dados → Ter mecanismos mais eficientes para manter a privacidade dos dados. Evitando que pessoas indevidas tenham acesso.

Outsourcing → Fazer a auditoria a partir de mão de obra externa a organização. Auditar o que está sendo feito por indivíduos que não pertençam à organização de forma direta.

Obs.: Outsourcing → Contratação de mão de obra externa a empresa. Muitas empresas hoje estão buscando focar mais no seu negócio (na sua atividade fim), deixando atividades não vitais serem desempenhas por não funcionários.

Base de conhecimento e mineração de dados → Utilizar técnicas através de bases de conhecimento e mineração de dados para tornar mais eficiente a auditoria de sistemas na organização.

Gestão por Exceção Quantificada → Usar a auditoria baseada na metodologia integrada por procedimentos com foco em minimizar possíveis fracassos quando do desenvolvimento, instalação ou operação de sistemas informatizados.

Tratamento de Exceções → Ter mecanismos de auditoria que tratem exceções de forma mais eficiente.

FCS (Fatores Críticos de Sucesso) → Mecanismos que auxiliem a auditoria através de fatores críticos de sucesso. Que são os pontos chave que definem o sucesso ou o fracasso de um objetivo definido por um planejamento de determinada organização.

Pontos de Falha → Usar mecanismos e técnicas que venham a ser utilizados para auditoria.

Auditoria de Negócio → Criação, aprimoramento da auditoria de sistemas no nível do negócio. Uma forma de auditoria mais direcionada para o negócio em si.

Novas necessidades e restrições com o aperfeiçoamento da informática

a) Necessidades:

. reformulação dos programas e currículos para treinamento dos profissionais de computação, com novas matérias/assuntos a serem abordados:

> . negociação técnica, com ênfase no desenvolvimento de argumentação lógica para negociação de soluções a problemas empresariais;
>
> . critérios negociais, para formação de raciocínio em conceitos de mercado, concorrência, linhas de negócios/produtos/serviços, novos empreendimentos, pioneirismo, inovações tecnológicas;
>
> . estímulos à criatividade, via discussão de aspectos comportamentais dos profissionais dos centros de responsabilidade das empresas, para geração de sinergia de qualidade organizacional.

. desenvolvimento e delimitação de know-how em informática, já de domínio dos profissionais de computação, para consumo dos usuários:

> . metodologia (etapas, técnicas, documentação) de desenvolvimento de sistemas pelos usuários;
>
> . sistemática e critérios para suporte técnico, como atendimento a chamadas de defeitos/registro de ocorrências, e às atividades de processamento de processamento eletrônico de dados;
>
> . planejamento e controle das atividades e tecnologia de informática.

b) Restrições:

. baixo nível, em geral, de formação dos usuários, quanto à tecnologia de processamento eletrônico de dados, particularmente no tocante a sua abrangência e em termos históricos;

. agregação ao ambiente usuário de mais uma variável, que vai acelerar os processos de mudanças nas áreas organizacionais (uso total de informatica);

. aumento de responsabilidade para os executivos e profissionais, quanto ao desempenho empresarial, pela disponibilização direta da tecnologia de informática a esses usuários.

Criação de novas funções:
a) analista de qualidade em informática: responsável pelo planejamento, controle e operacionalização de sistemas/ações/indicadores de qualidade em informática em toda a organização;
b) analista de segurança em informática: atua via segurança lógica/física/ocupacional/ambiental/confidencial, com a tecnologia de informática como base;
c) engenheiro do conhecimento: projeta e dinamiza a fluência do conhecimento empresarial em todos os pontos da organização.

UNIDADE II – AUDITORIA DE SISTEMAS

2.1-Conceitos

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

A auditoria de sistemas é o ramo da auditoria que revisa e avalia o controles internos informatizados, visando:

. proteger os ativos da organização;
. manter a integridade e autenticidade dos dados;
. atingir eficaz e eficientemente os objetivos da organização.

Auditoria de Sistema de Informação é instrumento da direção, dos acionistas, do ambiente externo, do usuário para: opinar, avaliar, validar a qualidade dos dados, da informação e dos sistemas que a geram e mantêm, em termos de segurança, confiabilidade e eficiência.

Todo e qualquer sistema deve ser observado sob 3 enfoques:

Os programas
. Existe máquina própria para desenvolvimento ou a área de desenvolvimento utiliza a máquina de produção?
. Existe norma de Catalogação de Programas de Produção com registro de alterações que demonstre:

- a data da alteração;
- impacto da alteração na área do usuário;
- outros impactos (em outros programas, rotinas ou sistemas);
- as instruções alteradas dentro dos programas.

A entrada de dados (front end)
. Submeter a entrada de dados a todas as condições possíveis de teste.

Como?
- Separando todas as telas e documentos de entrada.
- Examinando cada campo e comparando com a listagem da consistência.
- Submetendo os dados a uma bateria de testes em ambiente apropriado (não de produção).

Varredura das bases de dados (back end)
. Fundamental verificar a base de dados com programas de varredura.

Como?
- Examinando cada campo e comparando com a listagem da consistência.
- Submetendo os dados a uma bateria de testes em ambiente apropriado (não de produção).

2.2-Organização do trabalho

Planejamento
1º Passo: Conhecer o ambiente a ser auditado: Levantamento dos dados acerca do ambiente computacional (fluxo de processamento, recursos humanos e materiais envolvidos, arquivos processados, relatórios e telas produzidos).

2º Passo: Determinar os pontos de controle (processos críticos)

3º Passo: Definição dos objetivos da auditoria:
. Técnicas a serem aplicadas;
. Prazos de execução;
. Custos de execução;
. Nível de tecnologia a ser utilizada.

4º Passo: Estabelecimento de critérios para análise de risco
5º Passo: Análise de Risco
Avaliar para cada ponto de controle o grau de risco apresentado para posterior hierarquização:
Grau de Risco
1 – Muito Fraco
2 – Fraco
3 – Regular
4 – Forte
5 – Muito forte
6º Passo: Hierarquização dos pontos de controle

Definição da Equipe

1º passo: Escolher a equipe.

. Perfil e histórico profissional;
. Experiência na atividade;
. Conhecimentos específicos;
. Formação acadêmica;
. Linguas estrangeiras;
. Disponibilidade para viagens, etc.

2º passo: Programar a equipe

• Gerar programas de trabalho;
• Selecionar procedimentos apropriados;
• Incluir novos procedimentos;
• Classificar trabalhos por visita;
• Orçar tempo e registrar o real.

3º passo: Execução dos trabalhos

• Dividir as tarefas de acordo com a formaçao, experiência e treinamento dos auditores;
• Efetuar supervisão para garantir a qualidade do trabalho e certificar que as tarefas foram feitas corretamente.

4º passo: Revisão dos papéis

• Verificar pendências e rever o papel de cada auditor para suprir as falhas encontradas.

5º passo: Avaliação da equipe

• Avaliar o desempenho, elogiando os pontos fortes e auxiliando no reconhecimento e superação de fraquezas do auditor;
• Ter um sistema de avaliação de desempenho automatizado.

Documentação do trabalho

• Documentação de todo o processo de Auditoria de Sistemas a ser executado.

2.3-Produtos gerados

Relatório de problemas/fraquezas no controle interno

Este relatório tem por objetivo apresentar os resultados do trabalho da auditoria de sistema e esta estruturado em:

. Objetivos da auditoria;

. Pontos de controle auditados:

O banco de dados;
Um sistema;
Um sistema integrado;
Um acesso (password);
Etc.

. Conclusão alcançada a cada ponto de controle;

. Alternativas de solução proposta para correção das fraquezas de controle interno identificadas:

Segurança física;
Confidêncialidade;
Obediência à legislação;
Eficácia;
Etc.

Certificado de controle interno

O certificado contém as colocações claras se o ambiente computacional auditado se encontra em boa, razoável ou má situação no tocante aos parâmetros de controle interno:

. Segurança física;
. Confidêncialidade;
. Obediência à legislação;
. Eficácia;
. Etc.

Apresenta a opinião da auditoria em termo globais e sintéticos, permitindo a colocação e reunião dos achados, de fraquezas de controle interno, dos vários pontos de controle auditados, sob uma ótica de avaliação e de emissão de opinião total;

O certificado permite a “venda” imediata dos resultados dos trabalhos de auditoria de sistemas para a alta administração.

Relatório de redução de custos
Tem o objetivo de explicitar as economias financeiras a serem feitas com a adoção das recomendações efetuadas;

Serve de base para a realização das análises de retorno de investimento e de custo / beneficio a serem realizadas como parte da aplicação dos controles constantes dos projetos de auditoria de sistemas.

Manual de auditoria do sistema auditado
Tem por objetivo:

. Armazenar o planejamento da auditoria;
. Conter os pontos de controles inventariados;
. Conter os pontos de controle testados;
. Conter os pontos de auditoria flagrados.

É um referencial e base para as futuras auditorias daquele mesmo ambiente computacional a serem realizadas;

Contribui para a evolução tanto do ambiente computacional quanto dos processos de auditagem;

O conjunto de manuais de auditoria irá, ao longo dos anos, servir como comprovação histórica das atividades de auditoria de sistemas.

2.4-Apresentação dos resultados da auditoria à alta administração

Os seguintes fatores na comunicação precisam ser atendidos:

1.Objetividade na transmissão dos resultados da auditoria;
2.Esclarecimento dos debates entre auditoria e auditado;
3.Clareza nas recomendações de soluções;
4.Explicação da coerência de atuação de auditoria.

Os auditores devem preparar os seus relatórios de auditoria de forma a torná-los apropriados para apresentação à alta direção das organizações. Pode ser adequado apresentar um sumário executivo de cada relatório de auditoria, para apresentação a essa alta direção e a outros setores importantes, interessados, da organização. O sumário executivo deve destacar os resultados principais, positivos e negativos e identificar as oportunidades de melhorias.

Eficácia
Avalia quais os objetivos definidos para o sistema a ser criado e se as informações a serem geradas e apresentadas através de relatórios e gráficos, atendem aos requisitos.

Obediência a legislação em vigor
Verificar a aderência dos requisitos a legislação no que tange a cálculos e tratamento do dado, padrões de apresentação das informações definidos em lei e as orientações para guarda das informações no que tange a periodicidade.

Obediência as políticas da alta administração
Verificar a aderência dos requisitos as normas e orientações no que tange a concessões e restrições, a necessidade das informações a serem apresentadas e distribuídas.

O Relatório do auditor é o produto final do seu trabalho e, como tal, deve ser apresentado, visto e entendido pelo auditado, ou mesmo pelo usuário da auditoria. Considerado como veículo principal de relacionamento entre o auditor e a entidade auditada, o Relatório é documento técnico e deve obedecer a normas de apresentação, forma e objetivos.

O Relatório é o ponto de ligação entre o trabalho planejado e o efetivamente realizado. É o instrumento que revela à administração da empresa a qualidade e a contribuição da Auditoria Interna, suas constatações, opiniões técnicas e recomendações. Serve também como documento de avaliação do trabalho efetuado pelo auditor.

O Relatório do auditor é o produto final do seu trabalho e, como tal, deve ser apresentado, visto e entendido pelo auditado, ou mesmo pelo usuário da auditoria. Considerado como veículo principal de relacionamento entre o auditor e a entidade auditada, o Relatório é documento técnico e deve obedecer a normas de apresentação, forma e objetivos.

UNIDADE III – TÉCNICAS DE AUDITORIA

3.1-Programas de computador

Simulação paralela

- O método que consiste na elaboração de programas de computador para simular as funções da rotina do sistema em operação que está sendo auditada.
- Utiliza-se os mesmos dados de *input*, da rotina em produção, como *input* do programa de simulação.

Análise de dados

- Método que consiste na análise de arquivos através de programas de computador que poderão realizar, entre outras, as seguintes funções:
  1. Seleção de registros;
  2. Contagem de registros;
  3. Soma, cálculo da média, variância, desvio padrão, modo, mediana, etc;
  4. Construção de histogramas;
  5. Análise horizontal = comparação entre campos de um mesmo registro;
  6. Análise vertical = comparação de campos entre registros.

Comparação de dados

- O método que consiste na comparação entre os registros de dois arquivos “a” e “b”, diferentes, através de programas de computador, objetivando averiguar a existência de possíveis inconsistências que poderão realizar, entre outras, as seguintes funções:
  1. Seleção de registros (“a” que não está em “b”; “b” que não está em “a” ou que está em “a” e em “b”).
  2. Contagem de registros.
  3. Soma, cálculo da média, variância, desvio padrão, moda, mediana etc.

Confirmação de dados

- O método que consiste na confirmação dos dados armazenados em um arquivo, através de programas de computador, possibilitando verificar a veracidade dos mesmos.
- A estratégia mais utilizada para atingirmos tal objetivo implica na realização de uma circularização.
- Particularmente, neste caso, deve-se utilizar as técnicas de análise de dados e de comparação de dados, de forma integrada e/ou complementar.

3.2-Questionários

Corresponde à elaboração de um conjunto de perguntas com o objetivo de verificação de determinado ponto de controle do ambiente computacional.

Essas questões buscam verificar a adequacidade do ponto de controle aos parâmetros do controle interno (segurança lógica, segurança física, obediência à legislação, eficácia, eficiência, etc.).

Dois aspectos são críticos na aplicação da técnica de questionário:
. Características do ponto de controle;
. Momento histórico empresarial ou objetivos da verificação do ponto de controle.

Os objetivos de verificação do ponto de controle vão determinar a ênfase a ser dada ao parâmetro do controle interno.

As características do ponto de controle têm agregada a natureza da tecnologia computacional e o correspondente perfil técnico do auditor que irá aplicar o questionário.

Dessa forma, podemos ter questionários voltados para pontos de controle cujas perguntas guardarão características intrínsecas referentes a:

. Segurança em redes computacionais
. Segurança do centro de computação
. Eficiência no uso dos recursos computacionais
. Eficácia de sistemas aplicativos

A técnica do questionário pode ser aplicada com outras técnicas: Entrevistas, Visita in loco entre outras. O questionário pode ser aplicado à distância. Desta forma é possível que ocorra uma auditagem maior com menor número de auditores.

A sequência básica de aplicação de questionários á distância é:
. Analisar o ponto de controle e elaborar o questionário;
. Selecionar os profissionais auditados que deverão responder ao questionário;
. Elaborar um conjunto de instruções de como responder às questões;
. Distribuir/remeter o questionário para os profissionais selecionados;
. Controlar o recebimento dos questionários respondidos;
. Analisar as respostas às questões;
. Formar uma opinião do ponto de controle auditado em decorrência das respostas obtidas;
. Elaborar relatório de auditoria.

3.3-Simulação de dados

É a técnica por excelência aplicada para teste de porcessos computacionais. Corresponde à elaboração de um conjunto de dados de teste a ser submetido ao programa de computador ou a determinada rotina que o compõe, que necessita ser verificada em sua lógica de processamento.

Evidentemente, uma vez comprovada a inadequação da lógica do processo auditado, podemos concluir pela correção de todos os resultados que forem gerados por aquela rotina irregular.

Os dados simulados de teste necessitam prever situações corretas e situações incorretas de natureza:

. Transações com campos inválidos;
. Transações com valores ou quantidades nos limites de tabelas de cálculos;
. Transações incompletas;
. Transações incompatíveis;
. Transações em duplicididade.

Também conhecida como test-deck.

Figura 2: Etapas da simulação de dados

Algumas características para simulação de dados:
a) o auditor necessita conhecer computação em termos de análise de sistemas;
b) a documentação dos sistemas é deficiente, o que implica o auditor precisar atualizar ou complementar a documentação existente, principalmente no tocante a fluxos de informação e de programas. Muitas vezes a documentação existente compreende somente listagens de programas e fluxos ou sequência de execução de programas de produção;
c) a elaboração do ambiente de teste é complexa, particularmente em programas principais que manipulem grande quantidade de arquivos de entrada, saída e de trabalho.

3.4-Visita in loco

Corresponde à atuação pessoal do auditor junto a sistemas, procedimentos e instalações do ambiente computadorizado.

Normalmente, combina com outras técnicas de auditoria de computador, particularmente questionário, a visita in loco implica o cumprimento dos seguintes procedimentos:

. Marcar data e hora com a pessoa responsável que irá acompanhar as verificações, ou convocá-la no momento da verificação.

. Anotar procedimentos e acontecimentos, coletar documentos, caracterizar graficamente a situação via elaboração de fluxo de rotinas e de layout de instalações.

. Anotar nomes completos das pessoas e data/hora das visitas realizadas;

. Analisar os papéis de trabalhos obtidos, avaliar respostas e a situação identificada;

. Emitir opinião via relatório de fraquezas de controle interno.

Essa técnica é aplicada em vários pontos de controle clássicos de auditoria de sistemas, como:
. inventário de volume de arquivos magnéticos (discos, fitas, disquetes, CDs, DVDs);
. inventário de insumos computacionais armazenados em almoxarifado (fitas de impressora, formulários contínuos);
. visita à sala de operação/utilização de computadores com o objetivo de verificar problemas de controle de acesso, etc.;
. acompanhamento da rotina de backup de arquivos magnéticos (se todas as etapas são feitas de forma correta).

3.5-Mapeamento estatístico

Também conhecido como mapping.

Técnica de computação que pode ser utilizada pelo auditor para efetuar verificações durante o processamento dos programas flagrando situações como:
. Rotinas não utilizadas;
. Quantidade de vezes que cada rotina foi utilizada quando submetida a processamento de uma quantidade de dados.

A análise dos relatórios emitidos pela aplicação do mapeamento estatístico permite a constatação de situações:
. Rotinas existentes em programas já desativadas ou de uso esporádico;
. Rotinas mais utilizadas, normalmente a cada processamento do programa;
. Rotinas fraudulentas e de uso em situações irregulares;
. Rotinas de controel acionadas a cada processamento.

Há necessidade de ser processado um software de apoio em conjunto com o processamento do sistema aplicativo, ou rotinas específicas deverão estar embutidas no sistema.

Incluir instruções especiais junto aos programas em processamento na produção.

3.6-Rastreamento de programas

Técnica que possibilita seguir o caminho de uma transação durante o processamento do programa.

Durante a aplicação da técnica, a sequência de instruções executadas é listada. Dessa forma obtemos os números das instruções segundo sua ordem de execução.

00001-00002-00003-001150-001151-001152-
90190-90191-90192- etc.

Quando o teste de alimentação de determinada transação a um programa é realizado, podemos identificar as inadequações e ineficência na lógica de um programa.

Esta abordagem viabiliza a identificação de rotinas fraudulentas pela alimentação de transações particulares.

3.7-Entrevista

O método de trabalho corresponde à realização de reunião entre o auditor e os auditados - profissionais e usuários envolvidos com o ambiente ou o sistema de informação sob auditoria.

A sequência de procedimentos corresponde a:
. Analisar o ponto de controle e planejar a reunião com os profissionais envolvidos.
. Marcar antecipadamente data, hora e local com os auditados bem como comunicar a natureza do trabalho a ser desenvolvido.

. Elaborar um questionário para realização da entrevista.
. As questões devem ser divididas por parâmetro do controle interno, por área ou por assunto de processamento eletrônico de dados (PED).

. Realização da reunião com aplicação do questionário e anotação das respostas e comentários dos entrevistados a cada questão efetuada.
. dependendo do nível de sensibilidade das questões, as reuniões devem ser individuais;
. os níveis hierárquicos das áreas auditadas devem ser respeitados, comunicando-se aos superiores a natureza das entrevistas com os subordinados.

. Elaboração de uma ata de reunião com o registro dos principais pontos discutidos a cada questão apresentada.

. distribuir cópia da ata da reunião para cada participante da entrevista.

. Análise das respostas e formação de opinião acerca do nível controle interno do ponto de controle.

. Emissão do relatório de fraquezas de controle interno.

A técnica de entrevistas é frequentemente casada com outras técnicas de auditoria, visita in loco, questionário, etc.

3.8-Análise de relatórios/telas

Implica a análise de documentos, relatórios e telas do sistema sob auditoria no tocante a:

. Nível de utilização pelo usuário;
. Esquema de distribuição e nújmero de vias emitido;
. Grau de confiabilidade do seu conteúdo;
. Forma de utilização e integração entre relatórios/telas/documentos;
. Distribuição das informações segundo o layout vigente.

Implica no cumprimento das seguintes etapas:

. Relacionar por usuário todos os relatórios/telas/documentos que pertençam ao ponto de controle a ser analisado.

. Poderá ser feita uma classificação desses relatórios para efeito de estabelecimento de prioridades na análise;

. Obtenção de modelo ou cópia de cada relatório/documento/tela para compor a pasta de papéis de trabalho;

. Elaborar um questionário para a realização dos levantamentos acerca dos relatórios/telas/documentos;

. Marcar antecipadamente a data e hora com as pessoas que fornecerão opinião acerca dos relatórios;

. Realizar as entrevistas e anotar as observações e comentários dos usuários;

. Analisar as respostas, formar e emitir opinião acerda do nível de controle interno.

Principais fraquezas identificadas:

a) Relatórios/telas/documentos não mais utilizados;
b) Layout inadequado;
c) Distribuição indevida de vias;
d) Confidencialidade não estabelecida ou não respeitada.

Esta técnica é primordial para avaliação do parâmetro eficácia do sistema.

As conclusões do trabalho, frequentemente possibilitam redução de custo com a desativação total ou parcial de relatórios/telas/documentos.

3.9-Simulação paralela

Elaboração de um programa de computador para simular as funções de rotina do sistema sob auditoria.

Esta técnica utiliza-se dos dados rotineiros alimentados à rotina do sistema sob auditoria como entrada do programa de computador para auditoria, simulado e elaborado pelo auditor.

Enquanto no test-deck simulamos dados e submetemos ao programa de computador que, normalmente é processado na produção, na simulação paralela simulamos o programa e submetemos os mesmos dados que foram alimentados ao programa em processamento normal.

A estrutura de aplicação desta técnica corresponde a:

. Levantamento e identificação, via documentação do sistema, da rotina a ser auditada e respectivos arquivos de dados trabalhados.

. Elaboração do programa de computador com a lógica da rotina a ser auditada. Compilação e teste deste programa que irá simular em paralelo a lógica do programa de computador sob auditoria.

. Preparação do ambiente de computação para processamento do programa de computador elaborado pelo auditor.

3.10-Análise de log/accounting

O Log/Accounting é um arquivo, gerado por uma rotina componente do sistema operacional, que contêm registros de utilização do hardware e do software que compõem um ambiente computacional.

A tabulação destes arquivo Log/Accounting permite a verificação da intensidade de uso dos dispositivos componentes de uma configuração ou rede de computadores, bem como o uso do software aplicativo e de apoio vigente.

Tanto a rotina quanto o corresponddente arquivo de Log/Accounting foram desenvolvidos para serem usados pelo pessoal de computação.

Excelente ferramenta para a auditoria de sistema para:
. identificação de ineficiência, no uso do computador;
. apuração do desbalanceamento da configuração do computador, pela caracterização de dispositivos (unidade de disco, fita magnética, impressora, terminais) que estão com folga ou sobrecarregados;

. determinação de erros de programas ou de operação do computador;
. flagrar uso de programas fraudulentos ou utilização indevida do computador;
. captar tentativas de acesso a arquivos indevidos, ou seja, por senhas não autorizadas.

O trabalho da área de computação sobre Log/Accounting deve gerar Indicadores de Qualidade (IQ) do monitoramento do computador, bem como estudos de planejamento de capacidade da configuração/rede de equipamentos, com a finalidade de obter maior rendimento do parque computacional dentro de um nível de segurança adequado.

O auditor poderá construir um software para auditoria de Log/Accounting, o qual trabalhará registros de:
a) Contabilização
. Quais usuários utilizam quias programas e por quanto tempo;
. Identificação do usuário, características do hardware necessário para trabalhar o job (sequência de programas) e como o job foi completado.
b) Atividade dos arquivos
. Quais arquivos de dados foram usados durante o processamento e que usuário solicitou o uso do arquivo;
. Registro: nome do arquivo, tamanho do registro, número de série do volume e usuário do arquivo.
Obs.: Pode ser usado o termo data set ao invés de arquivo.

Para esta técnica o auditor deverá:
a) Entrevistar o pessoal de software básico e do planejamento e controle da produção para entender:
. o sistema de monitoração de uso de software e de hardware existente;
. o layout dos registros gerados no arquivo log/accounting;
. as opções possíveis de rotina de job/accounting;
. o tempo de retenção do arquivo log/accounting.

b) Decidir que tipo de verificação serão efetuados em cima dos dados do arquivo de log como período de tempo que será contemplado, quando será efetuado o teste, etc.

c) Elaborar e aplicar o programa de computador de auditoria de Log, ou utilizar a mecânica de análise do Log praticada pelos profissionais de computação;

d) Analisar os resultados da tabulação do Log;

e) Emitir opinião acerca da qualidade do uso do hardware e do software em determinado período de tempo.

Existem dois tipos de Log:
1. Aqueles que registram o uso da CPU, dos arquivos, da carga e do nível de utilização dos dispositivos computacionais.

2. Log de transações, ou seja, um arquivo que registra todos os dados que foram processados/transmitidos. Este tipo de arquivos de Log é comum em ambiente online no qula todas as transações processadas ficam registradas em um arquivo - log de transações - para posterior uso ou análise.

3.11-Análise do programa fonte

Implica a análise visual do código fonte do programa de computador do sistema sob auditoria.

O auditor de sistemas necessita assegurar-se de que está testando a versão correta do programa.

O auditor pode verificar as instruções que efetivamente compõem o programa em linguagem de máquina executando os seguintes procedimentos:
. Preencher uma ordem de serviço determinando à produção que compile o módulo-fonte que está na biblioteca-fonte;
. Executar um programa (software específico) que compare o código objeto-gerado com o código-objeto do programa que está em produção;
. Fazer as devidas verificações no caso de divergência dos códigos comparados.

É importante ressaltar que está técnica existe profundos conhecimentos técnicos por parte do auditor de sistemas. Entretanto, a análise visual do código-fonte do programa auditado permite ao auditor:
. Verificar se o programador cumpriu normas de padronização do código de rotinas, arquivos, programas;
. Analisar a qualidade da estruturação dos programas;
. Detectar vícios de programação e o nível de atendimento às características da linguagem de programação utilizada.

3.12-Exibição parcial da memória snap shot

Técnica que fornece uma listagem ou gravação do conteúdo das variáveis do programa (acumuladores, chaves, áreas de armazenamento) quando determinado registro está sendo processado. A quantidade de situações a serem extraídas é predeterminada.

Corresponde na realidade a um dump parcial de memória das áreas de dados.

À semelhança do mapping e do traccing, necessita de um software especial "rodando" junto com o programa aplicativo, ou que as características SNAPSHOT estejam embutidas no sistema operacionol.

É uma técnica usada como auxílio à depuração de programas, quando há problemas e realmente exige fortes conhecimentos de processamento eletrônico de dados por parte do auditor de sistemas.

3.13-Ciclo PDCA

O ciclo PDCA abrange: Planejar - Plan (P), Executar - Do (D), Verificar – Check (C) e Atuar – Action (A).

É um ciclo de gerenciamento a ser seguido para que seja feita a auditoria de forma mais organizada. Apresentam as seguintes características:
. Definir as metas (Planejar – P);
. Definir os métodos que permitirão atingir as metas propostas (Planejar – P);
. Educar e treinar (Executar – D);
. Executar a tarefa – coletar dados (Executar – D);
. Verificar os resultados da tarefa executada (Verificar – C);
. Atuar corretivamente (Atuar – A).

UNIDADE IV – FERRAMENTAS DE AUDITORIA DE SISTEMAS

4.1- Software generalista de auditoria de tecnologia da informação

Envolve o uso de software aplicativo em ambiente batch, que pode processar, além de simulação paralela, uma variedade de funções de auditoria e nos formatos que o auditor desejar.

Exemplos

• ACL (Audit Command Language): é um software de extração e análise de dados desenvolvido no Canadá;
• IDEA (Interactiva Data Extraction & Analysis) software para extração e análise de dados também desenvolvido no Canadá;
• Audimation: é a versão norte-americana do IDEA, da Caseware-IDEA, que desenvolve consultoria e dá suporte para o produto;
• Galileo: software integrado de gestão de auditoria. Inclui gestão de riscos de auditoria, documentação e emissão de relatórios para auditoria interna;
• Pentana: software de planejamento estratégico da auditoria, sistema de planejamento e monitoramento de recursos, controle de horas, registro de checklists e programas de auditoria, inclusive de desenho e gerenciamento de plano de ação.

Vantagens:

• Pode processar vários arquivos ao mesmo tempo;
• Pode processar vários tipos de arquivos com formatos diferentes, por exemplo EBCDIC ou ASCII;
• Poderia também fazer uma integração sistêmica com vários tipos de softwares e hardwares;
• Reduz a dependência do auditor do especialista de informática para desenvolver aplicativos específicos para todos os auditores de sistemas de informação.

Desvantagens:

• Como o processamento das aplicações envolve gravação de dados (arquivos) em separado para serem analisados, poucas aplicações podem ser feitas em ambiente on-line;
• O software não consegue processar cálculos complexos, pois como se trata de um sistema generalista, não aprofunda na lógica e na matemática muito complexas.

4.2- Softwares Especialistas de auditoria

Consiste em programa desenvolvido especificamente para certas tarefas em certas circunstâncias.

Vantagens:
• Pode atender sistemas ou transações não contempladas por softwares generalistas;
• O auditor, quando consegue desenvolver softwares específicos numa área muito complexa, pode utilizar isso como vantagem competitiva.

Desvantagens:
• Pode ser muito caro, pois terá uso limitado e normalmente restrito a determinado cliente;
• Atualização pode ser complicada devido a falta de recursos que acompanhem as novas tecnologias.

4.3- Programas utilitários

O auditor utiliza softwares utilitários para executar funções muito comuns de processamento, como sortear arquivo, sumarizar, concatenar, gerar relatórios. Pode ser um EXCEL, ou recursos de bancos de dados como o SQL, OQL, etc.

Vantagem:
• Pode ser utilizado como alternativa na ausência de outros recursos.

Desvantagem:
• Sempre necessitará do auxílio do funcionário da empresa auditada para operar a ferramenta (no caso de ferramentas complexas, como bancos de dados).

UNIDADE V – AUDITORIA DO AMBIENTE COMPUTACIONAL

5.1-Auditoria de Sistemas em Operação

- Transformação de dados em informação
- Captação e registro de dados
- Conversão de dados
- Consistência dos dados
- Atualização de arquivos
- Armazenamento e recuperação de dados
- Apresentação das informações
- Utilização das informações

Pontos de Controle auditados:
Análise dos Relatórios Emitidos pelo Sistema

Parâmetros avaliados:
• Eficácia - Verifica o nível de satisfação dos usuários com:
  • Natureza, correção e qualidade das informações recebidas;
  • Periodicidade e intensidade das informações recebidas;
  • Forma de apresentação da informação (sintética / analítica) e distribuição do relatório.
• Confidencialidade – sigilo das informações contidas no relatório, distribuição e destruição física dos relatórios.
• Segurança física – falta de qualidade na distribuição dos relatórios (rasgados, sujos, faltando vias, etc...).

Análise de Cadastro

Parâmetros avaliados:
• Segurança física – Verifica cuidados com transporte, armazenagem e manuseio de dispositivos que contém os cadastros, contra calor, poeira, magnetismo, queda, etc.;
• Segurança lógica – Verifica a existência de pontos de controle tais como: somatório de campos de valor, password, data de gravação e expiração do arquivo, quantidade de registros;
• Eficiência – Forma de organização do arquivo; campos ou registros existentes no arquivo e que não são utilizados.

Outros pontos de controle: Rotinas de Atualização, Programas de Cálculo, Rotinas de Backup, Documentação do Sistema.

Documentação utilizada: O DFD
O auditor necessitará de uma documentação do sistema e deverá elaborar, caso não exista, um DFD (Diagrama de Fluxo de Dados).

O DFD:
• Obedece o esquema TOP DOWN;
• Dá prioridade à representação de processos;
• Permite a representação gráfica até o nível de detalhamento desejado.

Os pontos de controle podem ser definidos em quaisquer um dos níveis, sendo mais aconselhável colocá-los no nível mais baixo, para maior facilidade de entendimento.

Técnicas mais utilizadas:
• Questionários, Visita in loco, Mapeamento estatístico (mapping), Entrevistas, Análise de relatórios/telas.

5.2-Auditoria de Sistemas em Desenvolvimento

- Exige fortes conhecimentos de análise de sistemas por parte do auditor;
- É necessário que o auditor tenha atuado na auditoria de sistemas em operação antes de atuar na auditoria de sistemas em desenvolvimento.

O auditor de sistemas em desenvolvimento deve conhecer:
• Uma metodologia de desenvolvimento de sistemas computadorizados, com suas etapas, técnicas, formulários e conceitos bem como o papel dos profissionais da área de sistemas
• Uma metodologia de auditoria que delineie a conceituação e a forma de participação do auditor na elaboração do sistema em computador.

5.2.1. O ciclo de desenvolvimento de sistemas

Inicialização do projeto
Estudo de viabilidade
Análise da situação atual
Projeto lógico
Projeto físico
Desenvolvimento e testes
Implantação
Administração
Manutenção

5.2.2. Pontos de controle para auditoria de desenvolvimento de sistemas

Processos:

- Etapas do ciclo de desenvolvimento
- Rotina operacional
- Rotina de Controle

Resultados:

- Documentação
- Relatórios
- Estrutura lógica
- Estrutura física
- Modelo de dados
- Projeto de arquivos
- Layouts de telas
- Definição de programas

5.2.3 Análise da Metodologia de Desenvolvimento de Sistemas

- Entendimento da metodologia através da documentação
- Identificação dos pontos de controle:
  Encadeamento lógico de idéias
  Objetivos de cada etapa
  Técnicas de análise utilizadas
  Produtos gerados
  Responsabilidade pela execução de cada etapa
  Documentação exigida nas etapas de desenvolvimento
  Qualidade de desenvolvimento do sistema
- Avaliação da adequação dos equipamentos ao sistema
- Emissão de opinião e debate com a equipe de computação

5.2.4. Análise da documentação do desenvolvimento de sistemas

- Entendimento das especificações através da documentação
- Identificação dos pontos fracos da documentação no que se refere a:
  Objetivos do sistema
  Análise de custo / benefício
  Levantamento do sistema atual
  Anteprojeto
  Projeto lógico
  Projeto físico
  Testes isolados e integrados
  Programação
  Implantação
  Documentação geral
- Analisar e avaliar os resultados obtidos emitindo o relatório.

5.3-Auditoria do Centro de Computação

Deve abranger:
• Instalações;
• Profissionais que executam tarefas comuns a todos os aplicativos;
• Contratos de hardware e software;
• Equipamentos;
• Software básico e de apoio;
• Redes de comunicação, para integração local e remota;
• Procedimentos administrativos, técnicos e gerenciais;
• Plano de integração de tecnologia.

5.3.1. Auditoria de Contratos de Hardware e Software

• Auditar transações de compra, venda, aluguel, leasing, seguros e manutenção de equipamentos, compra, locação e manutenção de software e seus contratos.

5.3.2. Auditoria de utilização de hardware e software

Utiliza a técnica de análise de log/accounting, podendo também ser utilizadas as técnicas de entrevista e questionários.

Utiliza indicadores que permitem:
• Estabelecer critérios para treinamento de profissionais e usuários;
• Montar um PDI possível de ser cumprido;
• Manter um orçamento de hardware, software e pessoal equilibrado;
• Conduzir a inovação tecnológica do ambiente;
• Estabelecer critérios de depreciação de equipamentos;
• Desclassificar fornecedores não idôneos;
• Identificar a causa de mau uso de hardware e software.

5.3.3. Auditoria de funções

Análise de funções, estudo do CPD e fluxo de informações do ambiente:
• Assegurar a qualidade, o rendimento, a eficácia e a produtividade na área sob auditoria;
• Assegurar o aproveitamento da especialização, a maximização dos recursos, o controle e a coordenação;
• Assegurar a adequação do fluxo de informações entre os setores do CPD e os usuários
Técnicas utilizadas: Questionários, entrevistas, análises de documentos/relatórios e telas.

5.3.4. Auditoria de Normas e Procedimentos

• Assegurar a divulgação e o uso de informações referentes a politica, diretrizes, organização e serviços de forma sistematizada, criteriosa e segmentada;
• Assegurar o treinamento e a capacitação dos recursos humanos e o funcionamento do CPD.

Documentação das normas e procedimentos:
• Informações sobre o objetivo da normatização;
• Facilidade de atualização;
• Distribuição dos manuais;
• Padrão estético;
• Consistência do conteúdo;
• Atualização das informações.
Técnicas utilizadas: questionários, visita in loco, entrevistas, análise da documentação.

5.3.5. Auditoria dos custos de PED
• Verificar os critérios para apuração de custos;
• Verificar os indicadores de custo apurados e sua evolução histórica e comparação com o mercado;
• Verificar o esquema de análise de custo vigente;
• Verificar as ações tomadas e as pendências para minimização de custos

Exemplos:
• Custo de digitação de um pedido
• Custo de utilização de máquina por ítem de estoque processado
Técnicas utilizadas: entrevista, visita in loco, questionários

5.4-Auditoria em ambiente de Microcomputadores

• Identificar inventário de micros, localização física, usuários, configuração, softwares, etc.;
• Identificar a política do Centro de Informação da empresa;
• Verificar tempo, natureza, segurança fisica, segurança lógica e confidencialidade no uso dos microcomputadores dentro da empresa;
• Verificar integração entre os micros;
• Verificar a documentação dos sistemas.

5.4.1. Auditoria do Centro de informação (CI)
• Problemática de relacionamento usuários X CPD: fila de espera para desenvolvimento de novas aplicações, alto custo de desenvolvimento de pequenos projetos, custo de hardware baixo X custo de software alto, etc.;
• Objetivo do Centro de informações: acesso às informações em tempo curto, prover ferramentas ao usuário, treinamento de usuários, suporte ao desenvolvimento de aplicativos para microcomputadores, apoio à escolha de software para microcomputadores, orientação na utilização dos micros na empresa.

Objetivo da auditoria:
• Análise das funções do CI;
• Avaliação das atividades de treinamento;
• Avaliação das atividades de controle de utilização de hardware e software;
• Avaliação da estrutura do CI;
• Análise de normas e procedimentos do CI (backup, linguagens de programação, utilização de editores de texto, planilhas, documentação de programas, contratação de hardware e software, atendimento aos usuários).

5.4.2. Auditoria dos microcomputadores e seus usuários
• Envio de questionários aos usuários para levantamento de dados de seu micro (hardware, software, interfaces, procedimentos de segurança, backup, etc.);
• Recebimento de respostas para levantamento de usuários que mereçam uma auditoria mais detalhada.

Técnica utilizada: questionário.

5.5-Auditoria em ambiente de Teleprocessamento e Bancos de Dados

O Banco de Dados deve conter as informações a serem tratadas pelos sistemas aplicativos da organização, com os conceitos de unicidade do dado.

Aspectos importantes:
• Existência do administrador de dados;
• Existência de um dicionários de dados;
• Existencia de um SGBD;
• Existência de um analista de banco de dados;
• Existência de controle de acesso ao BD.

Problemas encontrados:
• Leitura extração de dados por entidade não autorizada;
• Alteração dos dados ou procedimentos de programas;
• Adição ou exclusão de dados estranhos aos arquivos;
• Utilização de equipamento ou software sem autorização;

Controles a serem verificados pelo auditor:
• Verificação de password;
• Verificação da autorização de acesso aos dados;
• Confirmação da digitação de dados antes da atualização do BD;
• Verificação da integridade do Banco de Dados;
• Verificação da última transação processada versus a última transação recuperada no BD, quando da queda do sistema;
• Verificação de protocolos de arquivos (header e trailler);
• Verificação dos protocolos de linhas;
• Verificação da utilização de terminais.

Procedimentos de segurança:
• Criação da função de administrador de dados (descrição do BD, manutenção do dicionário, monitoramento da utilização do BD, controle de acesso, etc);
• Segurança física dos terminais;
• Definir normas para uso de passwords.

Técnicas utilizadas: Questionários, visita in loco, entrevistas.

5.6-Auditoria em segurança física e ambiental do Centro de Computação

• Infra-estrutura do Centro de computação (elétrica, hidráulica, ar condicionado, segurança contra fogo, inundação, etc.);
• Acesso físico (porteiro, catraca, etc.);
• Segurança da rede de comunicação de dados;
• Segurança fisica de recursos humanos e materiais;
• Plano de contingência.

Técnicas utilizadas: Questionários, visita in loco, entrevistas.

5.7-Auditoria de segurança lógica e da confidencialidade

Segurança lógica : modificação inadequada dos recursos tecnológicos, informações e softwares.
Confidencialidade: captação indevida dos recursos tecnológicos, informações e softwares.

• Programas de crítica e consistência: verificam integridade do dado e sua compatibilidade com as informações contidas no cadastro;
• Programas de processamento: verificam a correção do funcionamento do sistema e a alimentação dos arquivos corretos;
• Programas de saída: evitam a passagem de informações erradas aos usuários.

5.8-Auditoria do Plano Diretor de Informática

Documentação que formaliza o planejamento estratégico de informática para uma organização:
• Estabelece a filosofia de PED para a empresa;
• Define os objetivos e a estrutura da área de informática;
• Apresenta o plano de sistemas a serem desenvolvidos e mantidos;
• Estabelece critérios para aquisição de software e hardware;
• Define a necessidade de recursos humanos;
• Apresenta um orçamento de custos na área de informática;
• Enumera os benefícios a serem alcançados e as restrições previstas.

O auditor deve:
• Discutir se os novos sistemas a serem desenvolvidos estão priorizados segundo a gravidade da fraqueza do controle interno;
• Acompanhar se os relatórios de auditoria serviram de base para a elaboração do PDI;
• Verificar a adequabilidade do plano de sistemas as fraquezas detectadas pelo relatório de auditoria;
• Acompanhar o cumprimento dos objetivos definidos para o PDI;
• Analisar a metodologia aplicada e o conteúdo do PDI;
• Avaliar a qualidade do planejamento do PDI.

5.9-Auditoria no ambiente de Inteligência Artificial

Sistemas especialistas:
• Novos conceitos de computação – banco de dados do conhecimento, software de inferência, software com regras de decisão (sistemas especialistas);
• Aparecimento de duas novas funções: engenheiro do conhecimento (para estruturação dos sistemas especialistas de do software de inferência) e especialistas (para alimentação do banco de dados do conhecimento e criação das novas regras de decisão).

Desafios do auditor:
• Dificuldade de manter a documentação atualizada;
• Constante mudança nos objetivos dos sistemas especialistas;
• Caráter extremamente interativo de manutenção e uso do sistema especialista.

ANEXO 1 – Bibliografia/Webliografia

. GIL, Antônio de Loureiro. Auditoria de Computadores 5ª Edição. Atlas, 2000.
. IMONIANA, Joshua Onome. Auditoria de Sistemas de Informação 1ª Edição. Atlas, 2005.
. http://michaelis.uol.com.br/
. http://busca.unisul.br/pdf/88277_Abilio.pdf
. http://www.lyfreitas.com/artigos_mba/arttrilhaauditoria.pdf
. http://www.vemconcursos.com/opiniao/index.phtml?page_ordem=assunto&page_id=233&page_parte=2
. http://ix.congresso.iscap.ipp.pt/resumos/brasil/a_contabilidade_de_gestao/sistema_integrado_de_informacao.pdf
. http://www.inf.pucrs.br/~jaudy/audit%20face%20modulo%204%20definicoes%20e%20gestao%20da%20area%20de%20AS.pdf
. http://www.portaldomarketing.com.br/Artigos/Fatores_Criticos_de_Sucesso.htm
. http://tecspace.com.br/paginas/aula/asi/aula01.pdf
. http://www.reitoria.rei.unicamp.br/auditoria/documentos/mod2_ap_dia9.pdf
. http://www.fes.br/disciplinas/cic/ASC/012-%20Relatorios%20de%20auditoria.pdf
. http://www.qualidade.eng.br/auditoria_alta_direcao.htm
. http://www.qualityservicesconsultoria.com.br/faq2.html
. http://www.deloitte.com/assets/Dcom-Brazil/Local%20Assets/Documents/auditoria%20interna.pdf
. www.apcontabilidade.com.br/artigos/auditoria.htm
. http://tecspace.com.br/paginas/aula/asi/aula05.pdf
. http://tecspace.com.br/paginas/aula/asi/aula06.pdf
. http://www.trf4.jus.br/trf4/upload/editor/apg_ROGER_CANDEMIL.pdf
. AUDITORIA E SEGURANÇA DE SISTEMAS - Sandra Regina da Luz Inácio (arquivo da Internet).
. Normas e Técnicas de Auditoria I - Henrique Hermes Gomes de Morais (arquivo da Internet).