UNIVERSIDADE FEDERAL DO CEARÁ.
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO,
ATUÁRIA E CONTABILIDADE.

CURSO DE CIÊNCIAS CONTÁBEIS.

AUDITORIA EM SISTEMAS INFORMATIZADOS E A RELAÇÃO ENTRE EMPRESAS E A INTERNET.

ADRIANO DORTA DE MENEZES.

FORTALEZA, FEVEREIRO/1999.

AUDITORIA EM SISTEMAS INFORMATIZADOS E A RELAÇÃO ENTRE EMPRESAS E A INTERNET.

ADRIANO DORTA DE MENEZES.

Orientador: Vicente Lima Crisóstomo.

Monografia apresentada à Faculdade de Economia, Administração, Atuária e Contabilidade, para obtenção do grau de bacharel em Ciências Contábeis.

FORTALEZA-CE

1999.

Esta monografia foi submetida à Coordenação do Curso de Ciências Contábeis, como parte dos requisitos necessários à obtenção do título de Bacharel em Ciências Contábeis, outorgado pela Universidade Federal do Ceará – UFC e encontra-se a disposição dos interessados na Biblioteca da referida Universidade.

A citação de qualquer trecho desta monografia é permitida, desde que feita de acordo com as normas de ética científica.

Média

Adriano Dorta de Menezes — 9,1

Nota

Prof. Vicente Lima Crisóstomo — 9,5

Nota

Prof.(a) Fátima de Souza Freire — 8,25

Nota

Prof. José Alberto Soares ~~de Sousa~~ — 9,5

Monografia aprovada em 03/07/09

RESUMO.

O presente trabalho visa analisar e elucidar os principais fatos que influenciam o processo de conscientização dos administradores e auditores quanto à necessidade do desenvolvimento e difusão de técnicas para controle e auditoria de Sistemas Informatizados.

A Auditoria em sistemas informatizados resultou basicamente da necessidade de se garantir maior segurança na utilização dos computadores, fato que se tornou evidente a partir da constatação gradativa dos principais problemas existentes em uma empresa que trabalha com sistemas de processamento de dados. A essas constatações devem ser acrescentadas a dependência cada vez maior das empresas em relação ao bom funcionamento de suas instalações de processamento de dados, e também a alta concentração de informações no computador e num grupo reduzido de pessoas.

Muitas organizações dependem tanto de seus CPD's que qualquer paralisação acarretaria sérios prejuízos e em muitos casos seria impossível a própria existência da empresa. Esta importância estratégica cria a necessidade de se dedicar maiores atenções à segurança e controle das atividades de processamento eletrônico de dados. Essa paralisações e conseqüentes prejuízos são causados na maioria das vezes por: falhas no desenvolvimento e implantação de sistemas; redução da evidência para auditoria; falhas na utilização de sistemas, tanto por parte de usuários, como de processamento; fenômenos naturais e acidentes; fraudes e sabotagens por parte do pessoal interno; invasão de internautas; utilização indevida de sistemas em ambientes integrados por redes ou ligados a Internet; obsolecência tecnológica no que diz respeito à segurança dos sistemas; instalação de vírus no CPD da empresa por meio magnético ou pela rede mundial de computadores, entre outros. O trabalho analisa como os procedimentos da Auditoria de Sistemas podem minimizar estas falhas e contribuir para um aprimoramento das condições de funcionamento da empresa.

AGRADECIMENTOS.

A DEUS que me deu vida e inteligência, e que me dá força para continuar a caminhada em busca dos meus objetivos.

Ao Professor Vicente Lima Crisóstomo pela dedicação na realização deste trabalho, que sem sua importante ajuda não teria sido concretizado.

Aos meus pais e a minha namorada, que me ajudaram a transpor os diversos obstáculos que a vida nos impõe.

E aos demais que de alguma forma contribuíram na elaboração desta monografia.

SUMÁRIO.

1. INTRODUÇÃO.

Auditoria em sistemas informatizados é a revisão e avaliação da qualidade de controle interno de uma instalação de processamento de dados, cobrindo os aspectos de planejamento, iniciação, execução e registro de transações.

A preocupação da auditoria em verificar os elementos contábeis e em determinar a exatidão e a fidelidade das demonstrações e relatórios contábeis é mantida na auditoria em processamento eletrônico de dados.

A utilização dos recursos de processamento eletrônico de dados em uma empresa não se limita exclusivamente a dados contábeis, podendo abranger funções de controle e planejamento de dados de outras naturezas.

A revisão e avaliação de controle interno de um Centro de Processamento de Dados (CPD) poderá ser efetuada em aplicações não contábeis, desde que sejam significativas para a empresa, embora no decorrer deste trabalho a ênfase seja dada às aplicações contábeis.

Controle interno compreende "todos os procedimentos adotados coordenadamente em uma empresa com o objetivo de salvaguardar seus ativos, assegurar a exatidão e a confiabilidade das informações, promover eficiência operacional e encorajar a adesão à política administrativa estabelecida".

A Auditoria de Sistemas é o controle das ações desenvolvidas no planejamento, iniciação, execução e registro de transações. O controle é prescrito pelo estabelecimento de políticas e métodos que regulam as ações e é evidenciado principalmente através da documentação dos procedimentos das ações tomadas.

Os conceitos apresentados têm o objetivo de familiarizar o auditor com os principais pontos a serem analisados na revisão de controle interno em uma instalação de processamento de dados, procurando minimizar o grau de subjetividade na análise dos procedimentos existentes.

Este trabalho compõe-se da introdução e mais cinco capítulos principais, além das considerações finais. Os cinco capítulos principais estão dispostos da seguinte forma: 1) *Necessidade de Auditoria de Sistemas Informatizados*, que disserta sobre as principais causas de problemas em Sistemas Informatizados; 2) *Auditoria de Sistemas*, que explica o que é, e de que é composta uma Auditoria de Sistemas, mostrando também a subdivisão da Auditoria de Sistemas de acordo com a aplicação do computador; 3)*Revisão de Controle Interno*, define

quais os procedimentos usuais dentro de uma Auditoria de Sistemas, estes procedimentos estão subdivididos em seis áreas a serem verificadas (Documentação da Aplicação, Controles de Entrada, Controles sobre o Processamento, Controles de Saída, Controles de Segurança e Organização e Pessoal); 4)*Utilização de Computadores para fins de Auditoria*, demonstra como o equipamento de processamento de dados pode se tornar uma ferramenta muito importante para o auditor; 5) *Sistemas Integrados*, analisa a complexidade de se controlar sistemas interligados, não somente pelo aspecto técnico, mas também por envolver controle de indivíduos estranhos à organização, além disto procura fornecer dados sobre serviços privados de comunicação e seus benefícios junto às organizações, e avalia os aspectos da vulnerabilidade das empresas que dispõem de serviços na Internet. Assim dispostos os capítulos, forma-se o corpo do texto, que de maneira clara e objetiva procura atingir o seu objetivo maior, que é fornecer ao leitor dados suficientes para um bom entendimento do tema abordado.

2. NECESSIDADE DE AUDITORIA EM SISTEMAS INFORMATIZADOS.

Este capítulo apresenta os principais fatos que influíram no processo de conscientização dos administradores e auditores quanto à necessidade do desenvolvimento e difusão de técnicas para controle e auditoria de Sistemas Informatizados.

As principais causas de problemas em Sistemas Informatizados podem ser classificadas em :

a) Falhas no desenvolvimento e implantação de sistemas;

b) Redução da evidência para auditoria;

c) Falhas na utilização de sistemas, tanto por parte de usuários, como de processamento ;

d) Fenômenos naturais e acidentes;

e) Fraudes;

f) Sabotagem; e

g) Utilização indevida de sistemas em ambientes integrados por redes ou ligados à Internet.

A Auditoria em sistemas informatizados resultou basicamente da necessidade de se garantir maior segurança na utilização dos computadores, que se tornou evidente com os seguintes fatos:

- Serviços manuais constituídos de uma série de fases, ao serem implantados em computador, passam a ter apenas os documentos de entrada e relatórios de saída, perdendo-se assim a evidência da execução de cada fase intermediária.
- A evidência para Auditoria de muitos sistemas quase desapareceu ou foi afetada, em função da falta de participação dos auditores no desenvolvimento de sistemas e também da falta de conhecimentos contábeis por parte dos técnicos em sistemas informatizados. Essa falta de envolvimento do auditor no projeto de sistemas resulta muitas vezes em sistemas não auditáveis, por serem projetados sem considerar as necessidades de auditoria quanto a acesso posterior a arquivos e amostragem para verificação.
- Prejuízos resultantes de sistemas mal projetados.
- Negligência no estabelecimento de controles internos no desenvolvimento de sistemas, resultando em relatórios errados e altos custos de reprocessamento e reconstrução de arquivos.

- Documentação incompleta e inadequada, necessitando de conhecimento técnico para seu entendimento, deixando a empresa na dependência do conhecimento de um número reduzido de pessoas.
- Alterações constantes de programas sem documentação, resultantes de evolução natural do processamento de dados ou para refletir necessidades da empresa, assim como resultantes de programas mal concebidos , exigindo constante manutenção.
- Nível anormal de rotação de pessoal na área de processamento de dados.
- Incidência alarmante de má utilização e má administração do computador.
- Tendência generalizada para redução do registro dos dados de entrada e emissão de relatórios escritos em função de técnicas e equipamentos avançados de registro desses dados.
- Avanços tecnológicos rápidos na área de processamento de dados e freqüentes substituições de equipamentos, nem sempre necessárias e adequadas.
- O advento de sistemas "on-line" e "real-time", com a eliminação dos tradicionais totais de controle de lote e evidência para auditoria.
- Má utilização dos sistemas por parte dos usuários, em função de instruções inadequadas.
- Má qualidade dos dados de entrada.
- Possibilidades de perda e destruição de arquivos de dados sem condições de recuperação, causadas por:
  - Manuseio indevido e erros de operações;
  - Destruição de arquivos gravados em meio magnético;
  - Acesso a arquivos e extração de informações através de linhas telefônicas;
  - Erros esporádicos de "software" e de "hardware" e queda de energia;
  - Sabotagem;
  - Fenômenos naturais, tais como: incêndio e inundações;
- Fraudes executadas através do computador
- Orçamento para a atividade de processamento de dados representando uma percentagem significativa do orçamento de uma empresa.
- Alta concentração de informações de caráter pessoal na área empresarial e governamental, ameaçando os direitos individuais de privacidade.

A essas constatações devem ser acrescentadas a dependência cada vez maior das empresas em relação ao bom funcionamento de suas instalações de processamento de dados e também a alta concentração de informações no computador e em um grupo reduzido de pessoas.

Muitas organizações dependem tanto de seus CPD's que qualquer paralisação acarretaria sérios prejuízos e em muitos casos seria impossível a própria existência da empresa. Esta importância estratégica cria a necessidade de se dedicar maiores atenções de segurança e controle às atividades de processamento eletrônico de dados.

3. AUDITORIA EM SISTEMAS INFORMATIZADOS.

A auditoria em sistemas informatizados é a revisão e avaliação da qualidade de controle interno de uma instalação de processamento de dados, cobrindo os aspectos de planejamento, iniciação, execução e registro de transações.

Da revisão de controles pode-se destacar, para efeitos didáticos, a auditoria de aplicações de computador, que envolve o processo de verificação dos procedimentos e controles de uma determinada aplicação, sua lógica, assim como conteúdo dos arquivos mantidos. A revisão de aplicações de computador se destina tanto para sistemas já implantados, como para aqueles que estejam em desenvolvimento.

É essencial que os auditores façam revisão de cada nova aplicação de computador durante seu estágio de projeto e especificação. Os comentários da auditoria sobre controles devem ser apresentados enquanto eles ainda podem ser considerados durante a etapa de projeto. As recomendações da auditoria raramente podem ser implantadas sem um considerável custo extra e inconvenientes, após o sistema ter entrado em operação.

A administração deve pedir aos auditores para efetuar uma pré-auditoria das aplicações propostas, pois esta é uma área onde os auditores podem apresentar observações construtivas.

3.1 AUDITORIA DE APLICAÇÕES DE COMPUTADOR.

A análise de uma aplicação de caráter contábil selecionada tem a finalidade de rever e avaliar sua integridade, adequação e eficácia, partindo-se da premissa de que o auditor é responsável por auditar também os sistemas que produzem as informações de caráter financeiro.

Podem ser usados dois enfoques para revisão e avaliação dos procedimentos de controle de uma aplicação:

Auditoria "ao redor" do computador e

Auditoria "através" do computador.

3.1.1 Auditoria "ao redor" do Computador.

Na auditoria "ao redor" do computador o auditor não toma conhecimento do equipamento, analisando apenas documentos de entrada e relatórios de saída da aplicação escolhida, sem verificar os programas utilizados no processamento e os procedimentos adotados no setor de processamento de dados. Ela é realizada consultando-se apenas os usuários.

A aplicação deste método está baseada na premissa de que o sistema utilizado não é importante, desde que se consiga validar os dados de entrada e conferir os resultados de saída contra os mesmos.

Este método é válido nos casos em que uma parte muito pequena de um sistema é implantada no computador, de maneira que a auditoria "ao redor" do computador implica em um risco muito pequeno.

3.1.2 Auditoria "através" do computador.

Na auditoria através do computador são examinados também os procedimentos e controles de cada programa e os arquivos correspondentes, exigindo conhecimento detalhado na área de processamento de dados, que não é necessário no primeiro caso.

Os sistemas devem estar adequadamente documentados, através de descrição dos programas e controles existentes, que de maneira geral deve estar isenta de termos técnicos, para facilitar seu entendimento.

O auditor deve começar pela obtenção de um entendimento completo da aplicação de computador e seus procedimentos burocráticos correspondentes. Este entendimento é adquirido através de:

- Obtenção de exemplares de todos os documentos de entrada, formato dos livros de controle e relatórios de saída. Esses modelos devem ser arquivados junto com os papéis de trabalho de auditoria.
- Utilização de fluxograma e/ou forma narrativa para descrever:
  - Preparação dos dados de entrada;
  - Conferência e aprovação dos dados;
  - Controles;
  - Distribuição dos relatórios de saída.

A avaliação e teste de um sistema informatizado são feitos pelo auditor através de:

— Preenchimento de questionários de controle interno específicos para aplicação de computadores. Estes questionários abrangem os controles sobre procedimentos, transações e arquivos mestres. Ênfase especial deve ser colocada sobre os controles para assegurar que:

- Os dados de entrada são completos e precisos e, quando necessário, devidamente autorizados.
- Os resultados de saída são conferidos para verificar que estão baseados somente em dados de entrada verdadeiros.
- Os dados de entrada são processados corretamente.
- Os dados de saída são completos.
- O ciclo de processamento é preciso.
- A segurança e as condições de *backup* existentes são adequadas.

— Preparação de testes de auditoria para verificar os aspectos de controle.

— Desenvolvimento de procedimentos alternativos de auditoria quando a evidência para auditoria for inadequada.

— Preparação de um relatório sobre deficiências de controle.

4. REVISÃO DE CONTROLE INTERNO.

A revisão de controle interno é a aplicação de um conjunto de procedimentos que permitem a avaliação dos controles existentes num setor de processamento de dados. É também o assunto de interesse principal do auditor no campo de processamento eletrônico de dados, porque apesar de alta confiabilidade inerente às máquinas e da aplicação de técnicas avançadas no desenvolvimento de programas de computador, não se deve assumir que o bom controle interno se mantém automaticamente ao se transferi-lo para o computador. Apesar de não haver razão para que o controle em um sistema em computador não seja ao menos tão efetivo como em qualquer outro sistema, as modificações que acompanham uma implantação de processamento de dados podem apresentar problemas de controle que não existem em sistemas menos sofisticados.

A revisão de controle interno em sistemas informatizados requer normalmente um certo nível de conhecimento técnico nesta área e envolve a verificação de:

- Documentação em Sistemas Informatizados;
- Controles de Entrada;
- Controles sobre Processamento;
- Controles de Saída;
- Controles de Segurança, e
- Organização e Pessoal.

Outro tipo de revisão efetuada sobre um centro de processamento é a Revisão Técnica, que visa avaliar aspectos técnicos da instalação, tais como:

- Equipamento utilizado, sua configuração e limitações,
- Nível de utilização desse equipamento e do "software" disponível para o mesmo.
- Qualidade da programação, e
- Capacidade do pessoal envolvido.

4.1 DOCUMENTAÇÃO EM SISTEMAS INFORMATIZADOS.

Documentação de sistemas informatizados consiste primariamente de diagramas de bloco e fluxogramas descrevendo as operações de máquina, mas inclui também instruções de

operação do equipamento e manuais de procedimentos para o pessoal que opera e controla o sistema.

Em resumo, a documentação representa toda a evidência que pode ser lida sobre:

- O fluxo de dados através de uma série de operações manuais e de máquina, e
- As operações correlatas de preparação de equipamento e controle dos resultados do processamento.

Em sistemas informatizados a documentação é classificada em três partes:

- Documentação da aplicação
- Documentação de procedimentos
- Evidência para auditoria

4.1.1. Documentação da aplicação.

A documentação da aplicação é o registro de cada uma das etapas de desenvolvimento de um sistema e tem o objetivo de transmitir as características de projeto, fornecendo condições para a manutenção da aplicação.

É, em grande parte, voltada para o pessoal de processamento de dados para possibilitar a manutenção do sistema e o desenvolvimento de outros sistemas que possam ter ligações (sistemas integrados).

Assim, mesmo variando conforme a empresa, esta documentação deve conter pelo menos os seguintes itens:

- Histórico do desenvolvimento - necessidades que motivaram o desenvolvimento, entrevistas e levantamentos realizados, objetivos, alcance e limitações do sistema.
- Fluxos de documentos - anterior ao sistema, o proposto e o aprovado.
- Plano detalhado de trabalho - contendo os recursos necessários e cronograma.
- Aprovação formal - com as alterações solicitadas, se houver.
- Relatórios de acompanhamento - elaborados no decorrer do desenvolvimento.

Esta documentação, preparada durante a fase de desenvolvimento da aplicação, pode ser mantida como um registro histórico para eventuais consultas.

A documentação a seguir deve necessariamente ser preparada e mantida atualizada:

- Descrição do sistema - desde a preparação dos documentos base até a emissão dos resultados finais, contendo todos os programas, arquivos utilizados, controles e relatórios emitidos.

- Pasta de *lay-out* de todos os arquivos
- Pasta de programas contendo sua descrição, compilações e testes, massa de dados, alterações efetuadas e paradas programadas.
- Pasta de instruções operacionais contendo todas as instruções para a utilização do sistema para cada usuário, instruções de digitação, de operação e de controle de qualidade.

4.1.2 Documentação de Procedimentos.

Esta documentação é constituída pelos manuais que contêm as instruções de utilização do sistema, preenchimento de formulário, conferência de totais, fluxo de informações e outros elementos necessários conforme cada situação.

4.1.3 Evidência para Auditoria.

Na terminologia de processamento eletrônico de dados, a evidencia para auditoria compreende toda a documentação encontrada sobre as entradas e saídas das operações do computador.

A modificação no aspecto visível da evidência para auditoria é um entre os vários efeitos aparentes de uma conversão para computador.

Os documentos de entrada são geralmente redesenhados e algumas vezes eliminados completamente, assim como o formato de relatórios de saída pode ser alterado consideravelmente, incluindo livros diário e razão.

4.1.3.1. *DOCUMENTOS DE ENTRADA.*

Um documento de entrada é um meio de iniciar transações e acumular dados para efeitos contábeis e gerenciais, assim como um instrumento de controle interno.

Sendo um meio físico, ele mostra evidência visível da autenticidade de uma transação e a aprovação dos respectivos passos no processamento. Como formulário de trabalho, ele regula atividades operacionais e assegura a acumulação e processamento dos dados correlatos. Um documento de entrada deve ser desenvolvido de tal maneira que force o cumprimento dos procedimentos estabelecidos.

DIÁRIOS

Os livros diários preenchem duas funções importantes; eles fornecem um meio de acumulação de totais de transações similares para lançamento nas contas individuais do razão geral e fornecem uma referência cronológica para pesquisa de uma determinada transação.

Em processamento eletrônico de dados, estas funções podem ser executadas de forma bastante diferente do diário tradicional. Totais de contas podem ser acumulados internamente, eliminando completamente a necessidade destes livros, que no Brasil devem ser produzidos, entretanto, para efeitos legais.

A preservação da função de referência do diário requer procedimentos especiais em contabilidade através do computador, uma vez que a impressão de registros detalhados de transações não é uma parte natural de um sistema mecanizado.

Na maioria dos sistemas isto afeta a eficiência do processamento por requerer tempo adicional do equipamento na preparação dessas listagens. As impressões são demoradas, havendo uma tendência para eliminação do diário nos países em que a legislação permite tal providência.

FICHAS DE RAZÃO.

As fichas de razão cumprem funções diversas, incluindo as seguintes:

- Fornecem saldos das contas para preparação de relatórios financeiros;
- Controlam o processo de contabilização através da totalização de débitos e créditos;
- Fornecem contas de controle para utilização de razões subsidiários;
- Fornecem registros históricos da atividade de cada conta.

As três primeiras funções podem ser mecanizadas, sem qualquer problema particular de controle interno ou manutenção da evidência para auditoria.

A quarta função implica na existência de um registro permanente e visivel, independentemente do seu processo de preparação. Isto apresenta um problema em sistemas eletrônicos de processamento de dados, porque a manutenção de livros razão em fitas ou discos magnéticos ou outro meio de computador exigiria o armazenamento de grandes

volumes de informações históricas, com custos adicionais. A alternativa de impressão desses arquivos também envolve tempo substancial de utilização do computador, com custos também significativos.

NOTIFICAÇÕES DE ALTERAÇÕES EM ARQUIVOS MESTRES.

Uma adequada evidência para auditoria deve incluir relatórios preparados pelo computador sobre as alterações no conteúdo de arquivos mestres, tais como mudanças de nome e endereço, alterações de preços, salários, taxas de comissões, etc.

Há vários métodos de reportar tais informações. Pode-se preparar, por exemplo, um relatório mostrando a situação do arquivo antes e depois da alteração, ou apenas após a alteração.

Pode-se imprimir o conteúdo do registro inteiro ou apenas os dados que foram alterados. O método utilizado não é importante, desde que ele garanta um meio de se verificar que as alterações foram feitas corretamente.

LISTAGENS DE ERROS.

A passada inicial de uma aplicação de computador inclui freqüentemente uma verificação minuciosa dos dados de entrada.

Algumas transações são normalmente rejeitadas em tais passadas, por não preencherem as qualificações estabelecidas para sua aceitação. Outras transações podem ser rejeitadas em passadas subsequentes, por outras razões, tais como a impossibilidade de localização de um registro correspondente.

As transações rejeitadas devem ser reportadas ao departamento interessado para investigação e, se necessário, correção e nova entrada para processamento. Estas transações são geralmente impressas em um relatório separado, chamado de "listagem de erro" ou "de consistência", que é parte da evidência para auditoria, por conter as transações não processadas.

4.2 CONTROLES DE ENTRADA.

Os controles de entrada estão relacionados com os estágios de obtenção e transmissão de dados, abrangendo, portanto, todas as operações até o ponto em que o processamento passa para o computador.

Sua finalidade é garantir a exatidão das operações preliminares envolvidas na apresentação dos documentos para processamento, que são:

- Autorização de documentos de entrada;
- Manuseio de documentos de entrada; e
- Conversão dos dados para linguagem de máquina.

Por conveniência de apresentação, a verificação dos dados de entrada pelo computador está classificada como um controle de processamento em vez de um controle de entrada.

Alguns dos controles de entrada são quantitativos, no sentido de que procuram garantir a introdução no computador de todos os documentos a serem processados. Outros controles são qualitativos, servindo como verificações da validade das informações.

4.2.1 Necessidade dos Controles de Entrada.

A área de entrada em processamento de dados é definida como incluindo todas as operações até o ponto em que o processamento passa para o computador, sob direção de um ou mais programas.

A qualidade dos resultados depende diretamente da qualidade dos dados de entrada.

Em sistemas não eletrônicos é possível corrigir e completar a informação de entrada à medida em que ela é processada. Por exemplo, qualquer código faltante em um documento pode ser completado por um dos funcionários envolvidos com seu processamento em um sistema manual.

Em processamento eletrônico de dados, o equipamento pode ser programado para detectar a ausência da informação, mas, na maioria dos casos, ele irá rejeitar o documento de entrada e imprimir uma mensagem para seu acerto, após o que ele poderá ser novamente apresentado para processamento.

A intervenção humana para correção de erros é relativamente ineficiente em sistemas eletrônicos de processamento de dados e deve ser evitada sempre que possível.

Na área de entrada de dados, este princípio é observado pelo estabelecimento de controles rígidos no ponto em que os dados são criados, em lugar de tentar detectá-los em um ponto mais avançado do processamento.

Desta forma, devem ser produzidos dados precisos, aceitáveis para as máquinas e acompanhados de totais de controle de lotes ou outros tipos de controle.

4.2.2 Autorização de Documentos de Entrada.

A primeira questão a ser examinada, no assunto geral de controle de entrada, é a autenticidade dos dados que entram no sistema, quer sejam transações ou alterações em arquivos mestres.

Sem a garantia dessa autenticidade não há razão para efetuar qualquer outro controle sobre a validade dos dados de entrada.

TRANSAÇÕES.

O controle da emissão e preparação dos documentos fonte é exercido principalmente através da separação de tarefas. Como estes controles são externos ao processo de mecanização, eles não são afetados pelo uso de computadores.

ALTERAÇÕES EM ARQUIVOS MESTRES.

Em um sistema eletrônico de processamento de dados, vários fatores usados para cálculo e processamento são mantidos em arquivos mestres e devem ser modificados de tempos em tempos, para acompanhar as mudanças nas condições existentes.

Como exemplos podem ser mencionados:

- Arquivos de clientes - faixas de preços de venda, limites de créditos e prazos de venda.
- Arquivos de folha de pagamento - salário hora ou mensal, códigos de adicionais, taxas de comissões.

Como os arquivos não podem ser lidos sem o uso de computador e, portanto, não são passíveis de inspeção imediata, devem ser estabelecidos controles para evitar a introdução de alterações não autorizadas, instituindo-se geralmente procedimentos formais de documentação e processamento das alterações.

Uma técnica eficaz é exigir que cada solicitação de alteração seja autorizada por escrito; o computador deve, em correspondência, preparar um relatório, mostrando a situação do arquivo antes e depois da alteração, que é a seguir conferido pelo departamento usuário, para garantir que todas as alterações foram processadas corretamente, sem que tenham sido introduzidas alterações não autorizadas.

4.2.3 Manuseio de Documentos de Entrada.

Após a emissão, os documentos de entrada podem ser trabalhados ou utilizados por várias pessoas antes de serem entregues para processamento. A seguir, os documentos são perfurados ou convertidos a outro meio de entrada antes de sua introdução no computador.

Desta forma, devem ser estabelecidos controles para detectar a perda de cartões ou documentos à medida em que são passados de uma operação para a seguinte.

A seguir estão descritas as técnicas mais comuns de controle sobre os documentos de entrada.

REGISTRO.

Pode-se manter um registro sobre o estado de processamento de cada documento. Um registro típico mostra a data de preparação ou recebimento, data em que passa em cada operação e data em que é arquivado ou devolvido ao departamento de origem.

Um registro mais elaborado é usualmente mantido pela seção de controle de um centro de processamento, registrando-se as seguintes informações:

- Documento ou lote de entrada
  - Descrição ou número de identificação
  - Departamento de origem
  - Data de recebimento

- Contagem de documentos e totais de controle
- Data de retorno ao departamento de origem

- Listagem de erros:

- Número de erros (algumas vezes analisados por tipo)
- Data de liberação ao departamento de origem

- Relatório:

- Data de emissão
- Data de distribuição

O formato do registro e seu conteúdo dependem dos requisitos de cada instalação em particular, preparando-se geralmente registros separados por aplicação.

CONTROLE DE SEQÜÊNCIA.

Quando os documentos são numerados consecutivamente, eles podem ser controlados mediante sua classificação em seqüência numérica, que permite a verificação de que todos os documentos foram entregues para processamento e facilita consultas em caso de erro, assim como seu arquivamento.

CONTAGEM DE DOCUMENTOS.

Contagem de documentos é uma técnica básica de controle quando os documentos são processados em lote.

O procedimento consiste em realizar uma contagem do número de documentos em cada lote e verificar essa contagem inicial, em estágios apropriados no transporte e manuseio de documentos.

Como uma contagem isolada não fornece uma indicação para localização dos documentos faltantes, esta técnica é freqüentemente usada em conjunto com outros métodos de controle.

TOTAIS DE CONTROLE EM VALOR.

Totais de valores extraídos dos documentos fonte são utilizados para controle das várias operações por que passam os documentos.

Esta é uma das técnicas mais comuns, por ser simples e ser em muitos casos uma parte necessária do processo contábil e não apenas uma providência isolada de controle.

TOTAIS DE CONTROLE.

Os totais de controle podem ser estabelecidos a partir de qualquer campo de dados que seja comum a todos os itens, como, por exemplo, horas trabalhadas, quantidade de produtos e de empregados.

"HASH TOTALS".

Quando não há dados quantitativos comuns a todos os itens, pode ser necessário acumular um "hash total". Isto significa a acumulação de números que não são normalmente somados, tais como números de conta, números de faturas ou clientes.

"Hash totals" são raramente usados para controle de documentos mas são freqüentemente utilizados para controle durante o processamento.

4.3 CONTROLES SOBRE O PROCESSAMENTO.

Controles sobre o processamento, conhecidos também como controles programados, são parte das instruções armazenadas que dirigem as operações de um computador.

Dependendo da extensão com que estes controles são utilizados, um sistema eletrônico de processamento de dados se torna auto auditável, sendo esta capacidade superior à que se pode esperar de qualquer outro sistema de processamento.

4.3.1 Funções dos Controles Programados.

A extensão de utilização dos controles programados é principalmente uma questão de economia. Os custos do controle devem ser confrontados com os custos de não detectar erros. Esta comparação, de formulação simples é, entretanto, difícil de ser efetuada.

Os custos de efetuar o controle incluem:

- Tempo adicional de desenvolvimento e programação do sistema e
- Maior tempo do computador para processamento, que são afetados pelos requisitos de memória de uma rotina de conferência.

Quando há bastante memória disponível, os custos podem ser insignificantes. Caso contrário, os custos podem ser elevados em função de uma programação mais elaborada e da necessidade de passadas adicionais de computador.

Os custos de não detectar erros incluem:

- Procedimentos manuais de detecção, investigação e correção dos erros e
- Vários fatores de difícil avaliação precisa, que são peculiares a um dado tipo de erro, tais como os efeitos sobre a eficiência da administração da empresa ou sobre a imagem junto a clientes.

Alguns destes custos ou possíveis efeitos são difíceis ou impossíveis de medir. Assim, a extensão em que devem ser empregados os controles programados é grandemente uma questão de julgamento.

Na prática, os possíveis efeitos de não detectar erros são, algumas vezes, sumariamente desprezados e, como conseqüência, os controles são minimizados. A seguir estão apresentados alguns métodos de controle programados.

4.3.1.1 *CONTROLES QUANTITATIVOS.*

Conforme já mencionado no tópico "Controles de entrada", normalmente se estabelecem dados de controle, tais como número de documentos ou um total de controle em valor, antes de introduzir os dados no computador. Isto permite controlar as operações de máquina e possibilita aos departamentos usuários manter o controle sobre os dados de entrada.

Falhas no estabelecimento de tais controles podem resultar em deficiência fundamental de controle interno, embora se deva reconhecer que é impraticável estabelecer controles ideais sobre os dados de entrada.

É responsabilidade do centro de processamento processar todos os dados recebidos e devolver aos usuários o resultado do processamento. Os registros de controle preparados pelos usuários evidenciam a transferência da responsabilidade sobre os dados ao centro de processamento e dão segurança de que não se perdem registros durante o processamento.

CONTAGENS DE REGISTROS.

Contagens são bastante usadas para controlar o manuseio de documentos e cartões perfurados. A necessidade de contagem de quantidade é evidente nas operações de entrada, porque há sempre a possibilidade de extravio de um ou mais itens no seu transporte de uma operação para a seguinte.

Contagens são também bastante usadas para controlar informação (normalmente chamada de "registros") gravada em fita magnética. Esta necessidade, apesar de não ser tão evidente, porque os registros individuais gravados em arquivos magnéticos não podem ser trocados de lugar, é uma necessidade real, pois pode acontecer, entretanto, perda de registros durante o processamento.

Embora seja verdadeira a afirmação de que um programa vai processar todos os registros esperados (e apenas esses), é uma prática salutar incorporar aos programas um sistema automático de conferência da quantidade de registros de transações.

A contagem de registros é usada também para controlar arquivos mestre, gravando-se no final do arquivo um registro com o número total de registros contidos no arquivo. Cada vez que o arquivo é processado, a contagem de entrada é verificada, estabelecendo-se uma nova contagem de controle, que leva em conta os registros adicionados e eliminados durante o processamento. Desta maneira, qualquer perda de registros é automaticamente indicada nas mensagens ao operador do console.

Esta contagem de registros não pode ser usada nos casos em que certos critérios de organização de arquivos permitem a atualização do arquivo mestre sem exigir sua leitura integral.

As contagens de registros podem ser usadas também para controlar os registros de saída, tais como número de cartões perfurados ou número de linhas impressas.

Contagens de registros não controlam a qualidade da informação nos registros e não isolam os registros errados. Assim sendo, são freqüentemente necessárias outras técnicas para complementar a contagem de registros.

TOTAIS DE CONTROLE.

Estes são os controles quantitativos mais comumente usados, estabelecendo-se um total de controle para cada lote de transações nas operações de entrada, para governar todo manuseio e processamento subseqüente.

Totais de controle em valor são normalmente usados quando possível; caso contrário, se acumula outro dado, tal como horas trabalhadas ou quantidades produzidas. Ocasionalmente se utilizam "hash totals" a partir de códigos de produtos ou de clientes ou outro dado descritivo, a fim de permitir a verificação da exatidão das operações subseqüentes.

Nas operações de entrada, as transações individuais devem ser verificadas contra um total de controle antes de serem aceitas para processamento, o que é feito em uma passada preliminar de "consistência" dos dados de entrada. Se as transações passam a seguir por várias passadas adicionais - classificação, processamento, formatação dos dados de saída - os totais de controle são transportados de um arquivo para outro através de todo o sistema.

Em muitas aplicações se desenvolvem totais de controle adicionais durante o processamento. Por exemplo, em um sistema de folha de pagamento, o total de controle inicial pode ser estabelecido em termos de horas; a partir do ponto em que as horas de cada empregado são multiplicadas por seu salário hora, se estabelecem usualmente novos controles a partir dos valores resultantes.

CONTROLES DE SEQÜÊNCIA.

Os computadores podem verificar a seqüência dos registros à medida em que são lidos no início do sistema e também em vários pontos no processamento para assegurar que a seqüência desejada está sendo mantida.

Quando os registros tem numeração consecutiva, o controle de seqüência fornece um meio rápido para detectar itens faltantes ou em duplicidade.

4.3.1.2 *CONTROLES QUALITATIVOS.*

Os controles qualitativos se relacionam com o conteúdo dos dados dos registros. Eles testam a consistência do formato do registro, a presença ou ausência de certos dados, a exatidão de dados que podem ser conferidos aritmeticamente e a razoabilidade de certos tipos de informação.

Quando os testes se relacionam com os dados de entrada, eles são freqüentemente chamados de edição ou de consistência de entrada.

Quando eles se relacionam com o manuseio dos dados ou com a geração dos registros de saída, eles são chamados de controles de processamento.

CONSISTÊNCIA DE ENTRADA.

Os dados de entrada são normalmente "consistidos" de forma bastante completa no computador antes de serem submetidos a processamento.

Os computadores, entretanto, não têm a possibilidade de detectar dados fictícios que satisfazem os controles de consistência estabelecidos. Eles podem detectar somente os itens que não conseguem satisfazer os requisitos do sistema.

As verificações de consistência variam amplamente, porque se relacionam com requisitos de aplicações específicas e com o conteúdo de determinados registros de entrada. Elas não testam a exatidão de funcionamento do equipamento, porque sua função se relaciona somente com os dados de entrada.

A seguir estão apresentadas algumas das verificações comumente utilizadas cuja terminologia, entretanto, não está estabelecida de forma padrão:

- Verificações de codificação
- Verificações de combinações
- Dígitos de controle
- Verificações de correspondência em arquivos mestre
- Verificações de conteúdo

As verificações de codificação rejeitam códigos que estão em desacordo com listas de códigos pré-estabelecidos, não permitindo, entretanto, detectar que um código válido foi utilizado indevidamente.

As verificações de combinação são uma extensão das verificações de codificação. Nestes casos, o programa de computador reconhece as combinações válidas entre dois campos de códigos e rejeita as combinações erradas; um exemplo deste caso é a relação usualmente existente entre vendedores e zonas de venda.

A finalidade dos dígitos de controle foi explicada no tópico de "Controles de Entrada".

As verificações de correspondência detectam números errados de transações em arquivos, quando processados contra um arquivo mestre. A lógica básica das operações está na suposição de que o arquivo de transações e o arquivo mestre estão, ambos, na mesma seqüência ascendente. A determinação de que o número da transação é menor que o número mestre, seguida da determinação de que a transação não representa um registro novo a ser incluído no arquivo mestre, é indicação de algum tipo de erro. A investigação de cada caso irá indicar se o número de transação está fora de seqüência, se o registro mestre para a transação deveria ter sido previamente incluído no arquivo ou se o número da transação está incorreto.

As verificações de conteúdo testam a adequação dos dados de diversas maneiras: pode-se, por exemplo, testar a existência da informação e presença de caracteres alfabéticos em campos exclusivamente numéricos.

CONTROLE DE PROCESSAMENTO.

Após os registros serem analisados e aceitos para processamento subseqüente, podem ser aplicados certos controles para assegurar a exatidão do manuseio dos dados. Tais controles são usados com pouca freqüência, porque a confiabilidade do equipamento fornece segurança suficiente da exatidão do processamento na maioria das situações.

As verificações de lançamento são utilizadas para evitar atualizações erradas de arquivos, quando há possibilidade de um número de identificação ser anotado errado na informação de entrada.

Por exemplo, em uma aplicação de contas a receber que utiliza um arquivo mestre de itens em aberto, os registros de entrada e o arquivo mestre podem ser comparados inicialmente com base no número do cliente e do documento; em alguns casos pode ser útil comparar também o valor e a data de vencimento.

Considera-se, em geral, desnecessário verificar as operações aritméticas efetuadas pelos computadores. Entretanto, certas verificações aritméticas são freqüentemente programadas como meio de conferir a razoabilidade do processamento em geral. As verificações mais comuns são as verificações de limite, verificações de somas horizontais e verticais e verificações de sinal.

As verificações de limite testam a razoabilidade dos dados, fazendo sua comparação com limites estabelecidos de tolerância.

Os testes podem ser aplicados aos registros de entrada à medida em que os mesmos são lidos, e podem também ser aplicados aos resultados do processamento à medida em que são gravados ou utilizados para atualização de um arquivo mestre. Por exemplo, em uma aplicação de faturamento de uma companhia de eletricidade a razoabilidade do consumo medido (entrada) pode ser testada pelo cálculo de limites superiores e inferiores para cada conta, com base em consumo histórico, variações sazonais e outros fatores. Da mesma forma, os cálculos de folha de pagamento podem ser comparados com valores máximos pré-determinados, valores totais de notas fiscais acima de um certo valor podem ser evidenciados para análise, assim como saídas de mercadorias dos depósitos em quantidade fora do normal podem ser caracterizadas para consideração.

Teoricamente, as verificações de limite podem ser aplicadas a qualquer sistema envolvendo prazos, valores ou quantidades. Na prática, sua aplicação é bastante restrita, apesar dos benefícios resultantes sob o aspecto de controle.

As verificações de somas horizontais e verticais permitem provar a exatidão aritmética de um registro ou conjunto de registros, da mesma forma que nos casos em que se executa manualmente este tipo de verificação. Esta técnica é um meio simples de garantir que o serviço foi completamente executado e de maneira correta, ela é particularmente eficaz na conclusão de serviços demorados, que podem estar sujeitos a interrupção por razões mecânicas ou de programação dos serviços, sendo portanto vulneráveis a erros de retomada do processamento.

As verificações de sinal, como seu nome sugere, testam o sinal algébrico de um campo de dados. As máquinas podem, por exemplo, detectar saldos negativos de estoque ou troca do saldo de uma conta de débito para crédito.

Estas verificações são freqüentemente utilizadas para indicar falha no recebimento dos dados, sendo, muitas vezes, a troca de sinal resultante de chegada dos dados de entrada ou de processamento fora da seqüência pré-estabelecida.

Computadores operando em "real-time apresentam problemas específicos de controle; quando há vários terminais ligados a um computador central, é necessário prevenir a introdução a introdução de dados errados, modificação incorreta a arquivos mestres, assim como acesso não autorizado a informações. Os controles programados constituem um dos métodos mais efetivos de controle da utilização dos dispositivos de entrada "on-line".

4.4 CONTROLES DE SAÍDA.

Os controles de saída fornecem meios de comparar os resultados do processamento com informação de controle pré-determinada. Os controles de saída não visam a verificação da exatidão do processamento em si, que é função dos controles do sistema nos estágios de entrada e processamento.

4.4.1 Revisão Externa dos Relatórios de Saída.

Sempre que a natureza da aplicação permitir, é recomendável que a informação de saída seja revista por alguém externo ao centro de processamento para verificar a exatidão ou razoabilidade dos resultados.

Normalmente, a revisão pode ser restrita aos resultados de forma geral, aceitando-se a premissa de que se os totais estão corretos os detalhes também estão.

Totais de controle, contagens de registros e outros dados fornecidos pelos departamentos de origem devem ser comparados com os resultados sempre que possível. Quando não há controles com base em valores, quantidades ou contagens, a razoabilidade dos dados pode ser verificada por comparação com valores médios, tendências ou outros dados correlatos.

4.4.2 Manuseio dos Relatórios.

Vários procedimentos seguem a emissão dos relatórios de saída. Os relatórios e listagens em formulários contínuos devem ser descarbonados, destacados e passados aos usuários designados, assim como os documentos devem ser retornados aos departamentos de origem.

Estes procedimentos são geralmente executados pelo pessoal do centro de processamento, devendo-se estabelecer controles que garantam o manuseio rápido e correto.

Um registro de saída pode ser usado para anotar as datas em que os relatórios foram preparados e liberados, ou estes dados podem ser confrontados com dados de entrada e anotados em um registro combinado de entrada e saída.

4.4.3 Controle de Dados com Erro.

Quando um erro é detectado por um controle programado, o processamento desvia para uma rotina de erro que, conforme o caso, pode processar o item após a determinação do tipo de erro envolvido e sua inclusão em um arquivo de erros, ou então o erro é suficientemente crítico, sendo interrompido o seu processamento.

Nestas condições torna-se importante a necessidade de assegurar que os erros detectados são sempre devidamente investigados e reprocessados, quando necessário.

Não há uma forma única de garantir estes procedimentos; os erros são geralmente listados utilizando-se a listagem de erros para revisão dos casos apontados; muitas vezes os erros são gravados e apontados em todos os processamentos posteriores do mesmo serviço até que sejam corrigidos.

Em geral o centro de processamento não procura se assegurar de que os erros e itens rejeitados foram submetidos novamente para processamento, não devendo ter a responsabilidade pelos acertos de forma nenhuma, a menos que sejam devidos a erros de sua responsabilidade, tais como erros de perfuração; o centro de processamento pode ser, entretanto, bastante útil na interpretação dos erros quando solicitado pelos usuários.

4.5 CONTROLES DE SEGURANÇA.

Os controles de segurança consistem de políticas e regras estabelecidas para operação do equipamento de processamento de dados, que visam proteger o equipamento, dados e programas contra perigos conhecidos, incluindo fogo, queda de energia, excesso de umidade e outros perigos físicos, assim como contra destruição deliberada ou acidental ou alteração de informações pelos operadores do equipamento.

O principal interesse do auditor na área de controles de segurança se relaciona com as providências que estabelecem ou limitam as atividades dentro da sala do computador, enfatizando-se, como parte do sistema de controle interno, a importância das medidas que fornecem controle sobre a console e restringem o acesso a arquivos de programas e dados.

4.5.1 Segurança de Operação.

Os computadores são equipados com botões, *dials* e luzes que são utilizadas para operação do sistema e que se encontram agrupados convenientemente na console. A console é o único meio de iniciar e interromper as operações, examinar o conteúdo de áreas escolhidas na memória e determinar o estado do computador e das unidades de entrada e saída em um dado ponto do programa. Em alguns sistemas, ainda, ela permite ao operador rodar o equipamento a baixa velocidade, o que é útil na verificação das instruções do programa. A console indica ainda informações para efeito de manutenção.

Infelizmente, estes usos múltiplos da console possibilitam ações do operador que constituem uma exposição do ponto de vista de controle interno.

O operador da console tem controle completo sobre a máquina a todo instante, podendo interromper sua operação em qualquer momento desejado e modificar o conteúdo da memória. Desta forma, ele pode alterar uma transação ou um registro de arquivo mestre, modificar os respectivos totais de controle, inserir uma transação fictícia ou também pular uma transação válida.

A única forma de coibir uma intervenção irregular deste tipo é adotar as seguintes medidas:

- Separar o pessoal de processamento de dados de funções contábeis, de autorização de documentos e de funções de custódia.
- Estabelecer controles de sistema que permitam aos departamentos de origem detectar falsificações dos dados.
- Aplicar controles de segurança para prevenir uso não autorizado da console e restringir o acesso aos programas e arquivos de dados.

4.5.2 Registros de Utilização do Equipamento.

É recomendável que sejam mantidos registros sobre a utilização do computador. Para cada programa de produção, os registros devem ser complementados com a porção utilizada do equipamento (unidades de fita ou disco, impressoras, etc) e hora de início e término, Os registros devem indicar ainda todos os tempos não produtivos devidamente classificados em testes, reprocessamento, manutenção, tempo parado, etc.

Os registros de utilização do equipamento servem a várias finalidades, incluindo:

- Preparação do cronograma de operação;
- Acumulação de dados estatísticos sobre o desempenho do equipamento;
- Controle do tempo não produtivo; e
- Débito do valor dos serviços aos usuários.

Além disso, estes registros fornecem evidência que pode ser útil para efeitos de controle interno e auditoria.

Nas instalações em que se controla o tempo de máquina de forma contínua, uma passada irregular irá requerer algum tipo de anotação no registro, que pode servir de indicação para o auditor ou gerente do departamento. Além disso, é razoável considerar que qualquer manipulação indevida em uma passada regular vai resultar em aumento evidente do tempo de máquina.

4.5.3 Rotação do Pessoal.

Dentro das possibilidades práticas, o pessoal de operação deve ser trocado de função e de turno, numa tentativa de minimizar os riscos envolvidos em permitir ao operador tornar-se muito familiarizado com certos programas e as respectivas rotinas de contabilização.

Não deve ser descuidada também a necessidade de férias periódicas para o pessoal de operação do computador.

4.5.4 Investigação de Erros.

Os operadores não devem ter funções relacionadas com a investigação e correção de erros de dados e outros itens rejeitados.

As listagens de erros preparadas pelo computador devem ser devolvidas ao departamentos de origem, acompanhadas dos respectivos documentos de entrada; nos casos em que a urgência necessária ao processamento exija ou exista conveniência em função de grandes distâncias, esta função pode ser executada pela seção de controle do centro do processamento, cujos funcionários são completamente independentes da operação do equipamento.

Os controles administrativos necessários para assegurar o reprocessamento devem ser também executados pelo pessoal de controle.

4.5.5 Segurança Física.

SEGURANÇA DO EQUIPAMENTO.

Devem ser tomados cuidados para garantir a máxima disponibilidade e bom desempenho do computador, o que envolve um adequado programa de manutenção e a existência de instalações alternativas.

MANUTENÇÃO.

Há dois tipos de manutenção - preventiva e corretiva - que em condições normais de aluguel do equipamento são de responsabilidade do fabricante; nos casos de compra também se pode obter manutenção do fabricante, sob contrato.

É importante que o gerente de processamento de dados obtenha um bom serviço de manutenção, que muitas vezes é negligenciado por falta de tempo dos técnicos do fabricante, em virtude de demanda excessiva sobre seus serviços ou por falta de consciência de manutenção preventiva do próprio usuário em geral motivada por excesso de serviço.

INSTALAÇÕES ALTERNATIVAS.

Se a natureza das operações de uma empresa é tal que a perda de um ou dois dias de tempo de processamento possa trazer conseqüências sérias, devem ser promovidos entendimentos com um *bureau* de serviços próximo ou com outro usuário para utilização do seu equipamento quando necessário, dentro de determinadas condições.

Isto envolve localizar um computador com uma configuração similar de fitas, discos e impressoras e também com capacidade de memória suficiente para processar os serviços mais urgentes.

4.5.6 Segurança dos Dados.

O uso de arquivos magnéticos como um meio de registro de informações contábeis apresenta riscos que são peculiares a instalações de processamento de dados. O risco principal é a destruição não autorizada de dados, uma vez que uma das características de processamento eletrônico é apagar a informação de uma fita no processo de gravação de nova informação.

A proteção de dados está baseada em dois fatores básicos:

- Segurança física - sistemas de proteção física devem ser aplicados para proteger todos os dados quando não estiverem sendo usados pelo computador. Devem estar incluídos nesta categoria os procedimentos de controle da distribuição de relatórios confidenciais.
- Educação do usuário - os usuários devem ser instruídos quanto à importância de se manter a confidencialidade da informação. Eles devem também se preocupar com as ações disciplinares a serem tomadas contra qualquer pessoa que viole as diretrizes nesta área.

A seguir, são apresentados os controles mais comuns para proteção de dados gravados em fita magnética:

4.5.7 Política de Retenção de Fitas.

Um plano sistemático de retenção de fitas é desejável por várias razões:

- Prevenir a acumulação desnecessária de um grande número de carretéis,
- Assegurar a preservação das fitas necessárias à reconstrução dos dados, caso seja preciso, e
- Prevenir a destruição acidental ou intencional de dados vigentes.

É usual que uma grande instalação tenha um estoque de centenas ou milhares de carretéis de fita. Quando não há uma política específica de retenção, a tendência normal é salvar as fitas por prazos longos, para eventuais necessidades indefinidas de reprocessamento; um plano sistemático de retenção pode reduzir consideravelmente o investimento em fitas.

Por outro lado, pode haver conseqüências sérias quando uma fita de dados é liberada prematuramente. Dados em vigor podem ser destruídos, requerendo procedimentos de reconstrução que demandam tempo de máquina; pior ainda é a destruição de dados vigentes, se necessários.

Um plano básico de retenção é conhecido como o método "avô", que envolve três gerações de fita, em que a primeira (avô) e a segunda (pai) são a segurança contra perda ou

mal funcionamento da terceira (filho) no processo de gravação da fita seguinte. Em outras palavras, uma fita não pode ser liberada para uso até que passe da condição de avô. Este método funciona com arquivos mestres e as fitas correspondentes de transações de entrada.

Esta regra não se aplica a fitas de relatório que devem ser mantidas até que o relatório emitido seja aceito pelo destinatário; por outro lado, arquivos de trabalho utilizados em passadas de classificação podem ser liberados para uso imediatamente.

Um plano apropriado de retenção deve designar uma data ou qualquer outra base para expiração de cada fita utilizada. Todo o esquema de retenção deve ser revisto periodicamente para avaliar se os critérios de retenção requerem modificação e para decidir quanto à necessidade de compra de carretéis adicionais de fita.

Os dados de retenção devem ser registrados para fins de consulta. Além disso, a descrição de cada carretel de fita pode ser anotada no seu *label* externo para verificação visual; isto deve ser evitado, entretanto, no caso de arquivos de dados confidenciais, em que a descrição externa possa facilitar o roubo da informação.

As datas de expiração podem ser gravadas também nos *labels* internos das fitas, sendo calculadas pelo computador com base no seu período de retenção e na data de gravação. Este procedimento visa basicamente evita a destruição de dados que ainda estejam em vigor. A data de expiração é verificada pelo computador antes de se efetuar qualquer gravação na fita para evitar sua destruição, caso seja montado um carretel não expirado em uma unidade de fita para gravação.

Para que este plano funcione efetivamente, entretanto, todos os programas devem incluir uma rotina de verificação de *labels* para as fitas de saída; caso contrário, existirá a possibilidade de uma fita com dados em vigor ser montada em uma unidade de saída em um programa que não contém a rotina de verificação de *label*.

FITOTECA.

Os carretéis de fita devem ser guardados de maneira ordenada para facilitar sua localização e garantir sua proteção.

As fitas devem ser guardadas em uma sala próxima ao computador ou até mesmo em outro recinto, com controle de temperatura, umidade e poeira.

Deve haver uma pessoa responsável pelos carretéis de fita, operando como bibliotecário em tempo integral ou parcial, que deve ter instruções rígidas para não liberar fitas de programas ou de dados para analistas de sistemas, programadores ou outros elementos não autorizados.

Em geral mantém-se um controle em fichas por carretel e por arquivo. O primeiro fornece o conteúdo do carretel a qualquer momento e evidencia seu desempenho na operação; o segundo indica o carretel em que o arquivo está gravado para facilitar sua localização.

Os riscos contra fogo podem ser minimizados armazenando-se certas fitas fora do centro de processamento, incluindo-se uma geração de arquivos mestre e fitas com cópias de programas.

Cofres contra fogo são freqüentemente utilizados para guarda de arquivos no centro de processamento e em localidades fora do mesmo.

4.5.8 Segurança de Dados Confidenciais.

Cuidados especiais devem ser tomados para proteção de dados confidenciais, constituindo o que se chama de segurança lógica, que estabelece que a informação confidencial deve estar disponível em texto claro somente para certos programas de computador devidamente autorizados.

A segurança lógica deve estar baseada na filosofia de que todos os dados sensitivos armazenados fora da memória principal (por exemplo, em fitas e discos) devem ser cifrados.

A decodificação desta informação deve ocorrer somente durante a execução dos programas autorizados.

A seguir está apresentado um enfoque para implantação de controles projetados visando a segurança lógica. A preocupação pública sobre a privacidade da informação armazenada em sistemas computadorizados faz com que seja particularmente importante um maior envolvimento dos auditores.

OBJETIVOS DA SEGURANÇA LÓGICA DOS DADOS. CRIPTOGRAFIA.

Um plano de segurança lógica dos dados deve ser projetado para atingir os seguintes objetivos:

- Dados sensitivos em texto claro devem estar disponíveis apenas para programas autorizados.
- A responsabilidade por todos os aspectos de privacidade e segurança dos dados deve ser atribuída a uma autoridade central.
- Os aspectos de segurança dos dados devem ser transparentes aos programas de aplicação.
- Os requisitos de segurança devem causar pouco ou nenhum *overhead* de processamento.

Obviamente, alguns arquivos de dados não são particularmente sensitivos e não requerem proteção especial. Cada organização deve determinar a sensitividade relativa de seus dados; os tipos de arquivos de dados que necessitam de proteção são aqueles cuja divulgação criaria uma desvantagem competitiva, resultaria em uma perda para a empresa ou causaria qualquer outro prejuízo sério.

Várias instalações insistem que mesmo os arquivos de teste derivados de arquivos de produção sejam codificados de alguma forma, para protegê-los contra divulgação não autorizada ou inadvertida de informação sensitiva.

Um administrador de dados deve ser nomeado e encarregado da manutenção dos dados que identificam os arquivos sensitivos.

Um sistema de cifragem/decodificação deve manter a seguinte informação para cada arquivo sensitivo:

- Uma descrição dos campos a serem cifrados
- A chave específica que será usada para cifrar os dados (deve ser atribuída uma chave para cada operação)
- Nomes dos *jobs* (tarefas) que estão autorizados a acessar os dados sensitivos
- *Passwords* (senhas) atribuídas aos *jobs* autorizados (um *job autorizado* pode acessar o arquivo, mas não consegue decodificar os campos sensitivos)

Estas informações são o elemento mais importante no processo de cifragem/decodificação .

Controles estritos de segurança devem regular todo o acesso às mesmas e isto é imperativo.

Além disso, é claro que o administrador de dados cumpre um papel importante em assegurar que esses dados estão completos, assim como a precisão e autenticidade de seu conteúdo.

4.5.9 Segurança de Programas.

Um certo cuidado deve ser tomado para prevenir alteração acidental ou intencional de programas de computador.

Diagramas de bloco, dados de teste, jogos de cartões de programas, fitas e listagens de programas devem ser devidamente identificados e guardados convenientemente; cópias dos programas devem ser guardados em segurança, em local separado.

Os arquivos de programas e de dados devem ser guardados em local cujo acesso seja controlado por algum funcionário, seja este acesso no horário de expediente ou não. Durante o expediente devem ser liberados aos operadores do equipamento somente em concordância com o cronograma de operação.

As alterações de programas devem ser autorizadas por escrito pelo encarregado da equipe de desenvolvimento de sistemas e devidamente documentadas.

Dentro das políticas de controle adotadas, a manutenção de programas é uma das atividades mais vulneráveis em qualquer departamento de processamento de dados.

Os programas de produção, que parecem não conter erros e estar de acordo com os requisito dos usuários, são freqüentemente modificados para atender a novas solicitações. Durante este processo de manutenção, devem ser aplicados controles estritamente administrativos e organizacionais, para assegurar que as modificações são solicitadas, aprovadas, codificadas, testadas, documentadas e liberadas para produção de maneira apropriada.

Estes controles irão também auxiliar na prevenção de alterações autorizadas e potencialmente fraudulentas.

Cada etapa do processo de manutenção, desde sua iniciação até implantação, requer seus próprios procedimentos ou diretrizes para proteger a integridade da aplicação de computador.

Este tópico analisa o processo de manutenção de programas, identifica as áreas de possível exposição e descreve os controles que podem ser usados para minimizar os riscos correspondentes.

Os gerentes de sistemas mais prudentes devem implantar controles adequados nesta área em suas instalações; os auditores internos e externos também devem analisar estes controles durante sua avaliação de controle interno de uma determinada instalação.

SOLICITAÇÕES DE ALTERAÇÕES.

Os usuários devem emitir uma "ordem de serviço", "solicitação de manutenção" ou "solicitação de alteração", devidamente autorizada para requisitar modificações em sistemas já implantadas. Esse formulário deve conter a seguinte informação:

- Data de solicitação
- Data em que a alteração deve estar finalizada
- Motivo para alteração do programa
- Impacto da alteração, se conhecido, em outras partes do sistema
- Descrição detalhada da alteração, incluindo, quando for o caso, modelos de relatórios ilustrando o impacto da modificação
- Assinatura do usuário requisitante
- Assinaturas autorizadas, indicando aprovação do usuário

Esta informação ajudará o pessoal de processamento de dados a entender a natureza da solicitação, estimar necessidade de pessoal e tempo, assim como garantirá que a solicitação foi cuidadosamente considerada e devidamente aprovada pelo usuário.

O usuário retém uma via da solicitação e encaminha as vias restantes ao processamento de dados, onde são registrados e recebem um número de controle.

O departamento de sistemas deve analisar a solicitação e estimar o custo para efetuar a modificação, incluindo programação, teste e documentação. Todas as alterações cujo custo ultrapassar um valor mínimo pré-estabelecido devem ser devolvidas ao usuário requisitante para nova aprovação, antes de se executar qualquer serviço adicional.

Este procedimento deve ser seguido mesmo nas instalações que não debitam os custos de processamento de dados aos usuários.

Estes controles administrativos minimizam a probabilidade de implantação de solicitações não autorizadas ou que não sejam justificáveis do ponto de vista econômico.

PROGRAMAÇÃO.

A solicitação de alteração, após aceita, se transforma em um projeto para a equipe de manutenção, que é alocado a um programador para detalhamento e codificação.

Os programadores de manutenção , para executarem seu serviço, devem ter acesso à documentação de sistemas e de programas, assim como à codificação fonte do programa.

Em conseqüência, eles tem a maior parte das ferramentas necessárias para analisar uma série de programas, projetar uma fraude e inserir instruções não autorizadas sem levantar suspeitas.

Para reduzir esse risco, são necessários alguns controles adicionais, mais adiante discutidos.

TESTE.

É necessário um teste completo de cada sub-rotina e do programa inteiro, para que a alteração possa ser aceita. Estes testes têm a mesma importância dos procedimentos de teste aplicados durante o desenvolvimento inicial de um sistema.

Uma alteração em um módulo de um sistema pode freqüentemente afetar vários outros módulos. Se limitarmos o teste às instruções que foram alteradas, sem tentarmos comprovar os demais componentes do sistema, isto pode resultar em falha séria do sistema.

DOCUMENTAÇÃO.

A documentação dos programas afetados deve ser completada com um formulário "Registro de revisão de programa" para que a modificação seja aprovada e implantada.

Este registro de revisão deve conter todos os detalhes da alteração e estar suportado por um *list* atualizado do programa e uma cópia da solicitação original de alteração.

Alguns *package* para manutenção de biblioteca fonte fornecem uma evidência das alterações de programas que, quando disponível, deve ser incluída na documentação de alteração.

A documentação de manutenção de programas é muitas vezes negligenciada, devido à pressão para se completar o serviço. Este enfoque serve apenas para aumentar o tempo total necessário à manutenção de programas, porque a documentação imprecisa e incompleta irá prejudicar a atividade de manutenção no futuro.

CONTROLES.

O processo de manutenção de programas aqui descrito mostra algumas áreas vulneráveis, como, por exemplo, alterações sem documentação e programas não testados.

Os seguintes controles podem ser usados para assegurar que as alterações de manutenção são efetuadas de maneira apropriada e para reduzir as possibilidades de erros e de fraude:

- Autorização do usuário - a evidência escrita de que a alteração solicitada foi apropriadamente iniciada e aprovada pelo departamento usuário reduz a possibilidade de que solicitações não autorizadas sejam apresentadas através dos canais normais de manutenção. Cada solicitação deve requerer duas assinaturas do usuário, o solicitante e um supervisor, como mínimo, nos casos de alteração simples. É desejável que as alterações mais importantes sejam aprovadas por outras pessoas, pois a autorização exclusiva do usuário, como é usual em algumas organizações, pode conduzir a resultados catastróficos como, por exemplo, uma deterioração séria no tempo de resposta do sistema. A alta administração da empresa deve estar envolvida na aprovação das modificações de maior vulto, podendo requerer, em alguns casos, que modificações dessa magnitude sejam tratadas como novos sistemas.

A auditoria interna é também um candidato à aprovação de modificações de sistemas; as alternativas para a participação da auditoria na manutenção de programas estão discutidas em seção específica.

- Controle organizacional - pessoal de supervisão componente da equipe de manutenção deve rever e aprovar todas as alterações por escrito.

Embora um supervisor talvez não tenha tempo para revisar cada linha do programa modificado, um mecanismo formal de aprovação auxiliará a desencorajar as tentativas de manipulação imprópria.

- Aplicação independente das alterações e programas - a integridade das alterações ao programa fonte pode ser melhorada se os programadores tiverem de submetê-lo a um grupo de garantia de qualidade (GQ), após terem sido testadas.

O grupo de garantia de qualidade deve rever as alterações e aplicá-las contra cópias dos programas em produção. Este grupo mantém também uma evidência para auditoria das mudanças efetuadas e a inclui na documentação.

Embora o grupo GQ não possa rever e entender todas as alterações de programas, sua presença minimiza a possibilidade de que instruções não autorizadas sejam inseridas nos programas fonte da biblioteca de produção.

Se um centro de processamento não possui formalmente um grupo de GQ, as funções aqui atribuídas ao mesmo tempo devem ser assumidas por alguma outra entidade independente da atividade de manutenção de programas.

- Teste independente para aceitação - o teste para aceitação do sistema modificado deve ser efetuado pelo grupo de garantia de qualidade.

Para implantar esta técnica de segurança, o *staff* de GQ deve desenvolver um arquivo de teste para um caso base que percorre cuidadosamente a lógica do sistema.

Após terem sido efetuadas as alterações de manutenção, o sistema atualizado é testado, utilizando-se este arquivo de teste do caso base. Quaisquer divergências entre os resultados de testes anteriores do caso base e aqueles obtidos com o sistema modificado devem ser atribuídos à atividade de manutenção.

Este enfoque pode resultar em muito tempo aplicado; é aconselhável, portanto, limitar o teste de caso básico dos sistemas de baixa prioridade. Por exemplo, tais sistemas podem ser testados a cada trimestre, enquanto os sistemas de alta prioridade e alto risco seriam testados após cada manutenção.

- Controle da documentação - o grupo de garantia de qualidade deve ser responsável pela revisão das atualizações de documentação resultantes da manutenção de programas.

Antes da implantação do sistema modificado, todas as alterações de documentação necessárias, incluindo uma descrição do programa revisado e o registro de revisão do programa, devem ser submetidos a GQ e aprovados. Sem esta aceitação formal da documentação que foi atualizada, a modificação do sistema não deve ser considerada completa.

- Controle da biblioteca - os funcionários de GQ devem ser os únicos elementos autorizados a efetuar as alterações de programa nas bibliotecas de produção e catalogar nas mesmas os programas atualizados. Este procedimento impede os programadores de modificar os programas fonte de produção e de compilar e substituir um programa objeto de produção por outro.

Estas restrições nas bibliotecas fonte e objeto são essenciais para garantir a eficácia dos demais controles aqui mencionados.

Os auditores internos são usualmente responsáveis por assegurar que o departamento GQ está funcionando de maneira adequada e eficaz.

Devido à sua responsabilidade de controlar a manutenção de programas, a atividade do grupo de GQ deve estar sujeita a uma revisão profunda a cada ano.

4.6 ORGANIZAÇÃO E PESSOAL.

4.6.1 Qualificação do Pessoal.

Em sistemas eletrônicos de processamento de dados é evidenciada a necessidade de competência do pessoal envolvido.

Quando as máquinas fazem a maior parte do serviço, a competência do pessoal significa a diferença entre o sucesso ou insucesso do processamento.

Podem ocorrer erros em qualquer ponto do fluxo de dados em que se requer assistência humana, desde a preparação dos documentos até o manuseio dos relatórios e documentos de saída, passando pela perfuração, operação do equipamento e investigação de erros detectados pelo computador.

A competência da equipe de programação contribui bastante para uma conversão suave e ordenada de um sistema manual para o computador e é importante para o desenvolvimento de um sistema adequado de controle interno. Analistas de sistemas e programadores com conhecimentos contábeis têm, em geral, mentalidade de controle mais desenvolvida do que funcionários sem preparo na área de contabilidade e, por esta razão, as aplicações desenvolvidas por esses funcionários oferecem melhores condições de controle.

Há uma série de providências que auxiliam no desenvolvimento e manutenção de uma equipe qualificada. A determinação cuidadosa dos requisitos educacionais e de experiência de cada cargo fornece uma base sólida para admissão de novos empregados. Os programas de treinamento no serviço auxiliam os funcionários a atingirem os níveis requeridos.

Além disso, os registros de desempenho do pessoal são úteis na determinação da situação de um funcionário quanto a promoção.

PROGRAMADORES E OPERADORES.

A separação entre os programadores e os operadores de console geralmente não apresenta problemas nos estágios iniciais de desenvolvimento de uma aplicação. É usual que estas equipes se reportem a supervisores distintos, subordinados ao gerente do centro de processamento

Nos estágios finais da programação torna-se mais difícil manter a separação. As linhas de subordinação dentro da organização se mantém, mas os requisitos de teste de programas e processamento paralelo reúnem os programadores e operadores em um esforço comum. Não há objeções a isto do ponto de vista de controle, porque os programas não estão em operação normal neste ponto. Entretanto, esta prática não deve ser continuada após o funcionamento do sistema.

Consideração especial deve ser dada ao cargo de operador de console. Geralmente este operador desenvolve considerável conhecimento de programação através de sua participação em testes de programas. Mesmo embora ele não tenha fuções específicas de programação, seus conhecimentos de programação e operação combinados exigem um controle estreito de suas atividades.

PESSOAL DE CONTROLE E PERFURAÇÃO.

Os documentos de entrada devem ser manuseados somente por funcionários administrativos e da perfuração, isto é, funcionários diretamente envolvidos com a recepção de documentos e verificação de que os resultados de saída conferem com os totais de controle de entrada e também com a transcrição dos dados para cartões, fita magnética ou outro meio de entrada.

Obviamente estes funcionários não devem ter quaisquer atribuições em relação a programação ou processamento, assim como os operadores não devem manusear documentos de entrada.

BIBLIOTECÁRIO.

A custódia das fitas magnéticas é atribuída a um bibliotecário, cuja função principal é receber, guardar e liberar carretéis de fita, de acordo com um sistema organizado de arquivo e identificação.

Quando se utilizam centenas ou milhares de carretéis de fita, devem ser seguidos procedimentos bem definidos para evitar destruição acidental de arquivos e melhorar a eficiência dos procedimentos de preparação do computador.

A liberação dos arquivos deve ser feita com base em requisições ou em um cronograma de operação do computador. A separação das funções de programação e operação pode ser melhorada com a liberação de arquivos exclusivamente para o pessoal de operação.

5. UTILIZAÇÃO DE COMPUTADORES PARA FINS DE AUDITORIA.

O equipamento de processamento de dados pode ser uma ferramenta muito importante para a auditoria e o auditor deve conhecer as formas de utilização do computador para fins de auditoria e as vantagens resultantes.

No passado, a maioria dos dados relativos a transações se encontrava sob a forma de documentos escritos para uso do contador e para revisão do auditor. Atualmente estes dados estão armazenados em meios magnéticos e para sua utilização é necessária a aplicação de programas de computador, o que implica na necessidade de conhecimentos de processamento de dados.

O problema é agravado pelo fato de que o volume de informações armazenados é muito maior do que em sistemas manuais, de maneira que uma análise adequada do conteúdo dos arquivos magnéticos só pode ser feita com a utilização do computador.

A fim de que o auditor possa cumprir seus objetivos de analisar o conteúdo de arquivos magnéticos da mesma que em sistemas manuais, ele tem duas alternativas:

- Desenvolver programas de computador para atender a necessidades específicas, ou
- Utilizar programas generalizados de computador especialmente desenvolvidos para fins de auditoria.

A primeira alternativa irá envolver em cada caso as mesmas providências necessárias para desenvolver qualquer sistema de computador, a saber:

- Definir os objetivos e procedimentos a serem seguidos.
- Desenvolver o fluxograma do sistema.
- Desenvolver os diagramas de bloco de cada programa.
- Codificar, montar e testar cada programa.

Estas tarefas podem ser atribuídas ao centro de processamento mas, de qualquer forma, a utilização dos programas está condicionada e uma revisão detalhada de sua documentação por parte do auditor, que deveria também participar do desenvolvimento e teste do sistema.

Os sistemas ou *packages*, que constituem a segunda alternativa, não exigem conhecimentos especializados de computador ou linguagem de programação, ou tem como pré-requisito apenas um curso de conceitos básico de processamento de dados; sua utilização requer um curso de treinamento de três dias em média.

Estes sistema foram desenvolvidos inicialmente pelas firmas independentes de auditoria, para utilização nos seus serviços, tendo sido posteriormente colocados à disposição de seus clientes.

Outros sistemas semelhantes foram desenvolvidos, em uma segunda etapa, por firmas de *software* e colocados no mercado.

Essencialmente esses sistemas permitem executar as seguintes operações com arquivos em meio magnético:

- Extração - permite efetuar análises especiais, através da inclusão de registros com base em determinados critérios especificados.
- Apuração de subtotais - permite obter subtotais de arquivos com base em códigos estabelecidos, tais como zona de venda, código de filial, mês, etc.
- Impressão ou perfuração - o arquivo resultante de cada rotina pode ser impresso e/ou perfurado. No caso de impressão, as colunas de informações podem ser dispostas na seqüência mais conveniente, imprimindo-se opcionalmente os cabeçalhos descritivos de cada coluna.
- Resumo - esta rotina resume os registros de um arquivo com base em uma característica de identificação, tal como um número de cliente, código de peça, exigindo-se que os registros do mesmo cliente ou da mesma peça estejam agrupados.
- Operações matemáticas - esta rotina permite executar adição, subtração, multiplicação ou divisão com base em campos quantitativos e também com valores constantes especificados.
- Classificação - algumas vezes os arquivos não se encontram na seqüência mais adequada à aplicação de uma determinada rotina; os programas de classificação permitem colocar o arquivo na seqüência desejada.
- Comparação - dois arquivos podem ser comparados com base no mesmo campo de controle, selecionando-se apenas os registros que se encontram em um dos dois arquivos, ou em ambos, para processamento posterior.
- Amostragem estatística - esta rotina calcula o tamanho da amostra necessária para obter a segurança desejada e seleciona os itens que serão incluídos na amostra a ser examinada pelo auditor.

A seleção do *package* de programas generalizados de auditoria a ser utilizado em cada empresa deve ser precedida de uma análise detalhada dos sistema disponíveis no

mercado, em nenhum caso deve-se supor que um sistema deste tipo possa substituir esforço normal do centro de processamento no desenvolvimento de sistemas e preparação dos programas que serão utilizados rotineiramente.

Os programas generalizados podem ser utilizados rapidamente por não exigirem praticamente tempo de análise e programação; o tempo de processamento, entretanto, é maior do que o tempo necessário à execução de programas desenvolvidos com finalidades específicas.

Estes programas podem entretanto ser utilizados pelo próprio pessoal de processamento de dados para apuração de relatórios especiais.

6. SISTEMAS INTEGRADOS.

Até então vimos a Auditoria de Sistemas no que tange ao controle sobre sistemas de produção e sistemas de desenvolvimento.

Desde a década de 80, iniciou-se o processo de interligação de sistemas computacionais em redes. Esta nova realidade permitiu o surgimento das redes corporativas e também da interligação de redes de organizações distintas. Este processo passa por interligação de organizações que tenham parcerias em negócios, e chega ao seu apogeu nos dias de hoje com a Internet.

Neste novo quadro, os controles que apresentamos ao longo do trabalho permanecem, e outros fazem-se necessários. Controles no uso de sistemas interligados apresentam um maior grau de complexidade, não somente pelo aspecto técnico, mas também por envolver controles de indivíduos estranhos à organização.

O auditor deverá então ter conhecimento da situação dos sistemas corporativos e de suas interconexões internas e externas. A partir daí, será capaz de estabelecer controles neste ambiente. Neste novo contexto, é aconselhável que o auditor tenha algum conhecimento da tecnologia de redes de computadores, da arquitetura cliente-servidor, Internet e os aspectos de segurança envolvidos em tais ambientes.

Enumeramos a seguir alguns controles a serem adotados em tais circunstâncias:

- Controles com relação ao acesso a componentes físicos, que deve ser o mais restrito possível, além de instalações adequadas para comportar tais componentes;
- Controles rigorosos relacionados com a segurança lógica. Estes estão relacionados com o uso de sistemas e recursos computacionais. Aí estão inseridas atitudes como o uso de sistemas operacionais e sistemas gerenciadores de banco de dados com requisitos de segurança adequados, sistemas que permitam o controle de acesso e uso de recursos, além de outros cuidados.

Realizamos uma pesquisa sobre serviços de comunicação privados utilizado por algumas organizações e os benefícios oriundos dos mesmos. Além disto, estudamos também a Internet e seus aspectos de vulnerabilidade, que exigem grandes cuidados das organizações que a utilizam.

6.1 A REDE POR SATÉLITE E SEUS BENEFÍCIOS.

A Internet vem se transformando em um instrumento de avanço tecnológico de várias empresas no Brasil e no mundo graças às suas constantes inovações. No Brasil, o mercado está ficando cada vez mais aceso devido às mudanças ocorridas na lei das telecomunicações e com a privatização do sistema Telebrás.

Esta nova lei de telecomunicações, aprovada no ano passado, promove alterações importantes nesse cobiçado setor da economia brasileira. Uma das mais significativas mudanças diz respeito à participação da iniciativa privada em atividades antes restritas à Embratel como, por exemplo, a de comunicação por satélite, considerado um dos meios mais eficazes e confiáveis de transmissão, apresentando como principais vantagens a alta disponibilidade e baixa incidência de erros. Indicado para regiões de difícil acesso e que exigem linhas de comunicação (*links*) de alta velocidade, o satélite desponta como uma alternativa para conexões em grandes centro urbanos onde a instalação de meios terrestres de comunicação, como por exemplo a fibra ótica, se torna difícil. A quebra do monopólio estatal cria as condições para o estabelecimento de um modelo de mercado onde a concorrência, até então inexistente, é parte intrínseca do jogo e pode favorecer a proliferação de novos serviços a preços acessíveis.

A comunicação por satélite é enquadrada na legislação em vigor como uma modalidade de "serviços de telecomunicações especializados", e como tal, somente pode ser explorado mediante concessão da ANATEL (Agência Nacional de Telecomunicações), criada para atuar como órgão regulador de todas atividades relacionadas ao setor. A boa notícia, contudo, é que, ao contrário do que ocorria antes, uma vez obtida a outorga, as empresas poderão prover serviços de comunicação compartilhados, interligando vários clientes simultaneamente na mesma rede de satélite. Para tanto, terão que fazer investimentos na montagem da estrutura, que abrange desde a contratação do segmento espacial (capacidade de satélite), até a instalação dos equipamentos que integram a estação terrena de comunicação, conhecida no jargão da área como teleporto, a partir do qual monitoram e gerenciam o tráfego de dados de todos os seus clientes, podendo inclusive identificar e corrigir quaisquer eventuais interferências na transmissão dos sinais.

Os equipamentos que integram o teleporto são a HUB, que concentra os sinais enviados ao satélite, multiplexadores, moduladores e antenas parabólicas, entre outros. Se a

rede for baseada na tecnologia VSAT (*Very Small Aperture Terminal*), o investimento inclui instalação de estações remotas. No caso de antenas, as dimensões são compatíveis com a faixa de freqüência da transmissão. Quanto ao segmento espacial, as empresas autorizadas a prestar serviços compartilhados, ficam com a incumbência de contratar a capacidade espacial. Nesse campo a legislação em vigor também apresenta novidade ao permitir o emprego de satélite estrangeiro, desde que "sua contratação seja feita com empresa constituída segundo as leis brasileiras e com sede e administração no país, na condição de representante legal do operador estrangeiro". Isso significa que a partir de agora as empresas poderão alocar banda de outros satélites com cobertura sobre o território nacional que venham a ser lançados por outros consórcios. Na tentativa de ampliar a capacidade de satélite para uso doméstico, a ANATEL prepara licitação para exploração de satélite brasileiro, sendo que nas novas regras, até três grupos poderão lançar satélites – antes só podia um.

Uma das vantagens do compartilhamento da rede é a redução dos custos de comunicação, principalmente das redes baseadas na tecnologia VSAT, desenvolvida para aplicações de baixo tráfego, tais como transações financeiras, correio eletrônico, transações de ponto-de-venda, sistema de reservas, controle de estoque e segurança e sistema de supervisão em ambientes com pontos distribuídos geograficamente. Além destes aperfeiçoamentos gerados pelo compartilhamento de rede, que são os mais importantes, existe uma gama de serviços que facilitam e dinamizam a operacionalização das empresas, por exemplo, o TeleCampus, oferecido pela empresa Impsat do Brasil, destinado a empresas que promovem cursos e de treinamento à distância que permite a transmissão de aulas e palestras geradas em estúdio de um ponto central e podem incluir recursos tais como desenhos gráficos e vídeos complementares.

Uma das empresas que interligaram sua rede com satélite via sistema VSAT, foi a *Volkswagen*, empresa que já começa a usufruir da dinamicidade deste meio de comunicação. Um ano após a montagem de uma *intranet*, que teve como objetivo garantir a comunicação entre os setores industrial, comercial e de compras e vendas, a *Volkswagen* acaba de finalizar a implementação de sua rede *VWNet*, baseada no sistema de comunicação via satélite (VSAT), que permitirá o tráfego de dados, voz, e imagem entre todas as unidades. Ao todo, o sistema interliga todas as suas fábricas com os 13 escritórios regionais, 22 escritórios de serviços financeiros e 820 revendedores espalhados pelo país. O objetivo da *Volkswagen* com a *VWNet*, de acordo com o diretor de tecnologia de informação, Carlos Roberto Boschetti, em entrevista

a revista LanTimes, foi dinamizar o fluxo de informações entre os diversos setores, facilitando os negócios de *leasing*, financiamento e compra de automóveis, além de treinamento da rede, com atendimento durante 24 horas, sete dias por semana. De acordo com Boschetti, a comunicação via satélite foi a saída encontrada para garantir a alta qualidade nas transmissões, facilidade de conexão e excelente relação custo/benefício num país onde a tecnologia ISDN (*Integrated Services Digital Net*) ainda está dando os seus primeiros passos.

A economia de custos, segundo Boschetti, será sentida tanto pelas montadoras como pelos revendedores com a videoconferência e o *broadcasting*, que eliminarão despesas com treinamento, viagens e a realização de negócios com clientes que dependem de liberações do departamento financeiro. O diretor da *Volkswagen* explica que com o sistema de *broadcasting* o revendedor poderá treinar seus mecânicos através de vídeo em tempo real ou gravar para que eles possam assistir os cursos conforme o tempo disponível. Ele reforça que o foco, portanto, está em como preparar o treinamento da rede, lançar novos programas de vendas, desenvolver nova política de comercialização da *Volkswagen*, observando que o país tem uma dispersão geográfica muito grande, além de uma qualidade de comunicação bastante heterogênea.

A grande vantagem salientada pelo diretor da empresa é que a *Volkswagen* e as concessionárias não investiram nenhum centavo no empreendimento, pagando apenas mensalmente pelo serviço prestado, independente da utilização. Segundo Boschetti, também foi formado um consórcio para montar e gerenciar toda a infra-estrutura, já que ficaria muito caro investir no VSAT. Desse modo, a Embratel ficou responsável pelo segmento aeroespacial do satélite, a NEC, pelo equipamento terreno e antena provedora da tecnologia, a comunicação voz e videoconferência ficou por conta da Equitel, com tecnologia da Siemens, e a IGS (*IBM Global System*) é a gestora do serviço. Segundo Boschetti, a Volkswagen está gastando muito menos investindo em uma empresa especializada na tecnologia de comunicação como a IGS, do que se ela montasse o seu próprio sistema de fluxo de informações. "Se fôssemos implementar por conta própria o sistema, faríamos o melhor dentro da nossa óptica, mas o pior no ponto de vista do cliente. Afinal, nosso negócio é fabricar carros e caminhões", finaliza Boschetti.

Analisando os aperfeiçoamentos que podem ser realizados através de um sistema de comunicação eficiente, como vimos neste caso da *Volkswagen*, através da redução dos custos, da qualificação profissional, da rapidez no fluxo de informações e no dinamismo da produção,

entre outras melhorias, notamos a importância da tecnologia nas empresas, não só nas grandes, mas também nas pequenas e médias empresas, que na medida do possível devem se modernizar-se e procurar novas formas de negociação, medidas que facilitem a comercialização do produto ou do serviço e muito mais. Os empresários brasileiros devem estar atentos para não pararem no tempo e sempre buscarem inovações que melhorem a qualidade do serviço e incentivem a demanda por seus produtos.

Observamos aí um bom aspecto de segurança, já que o serviço de comunicação por satélite tornou-se quase que privativo para a empresa que utiliza-o. Uma outra situação observa-se na Internet, na qual o aspecto de segurança que é crucial.

6.2 INTERNET: ATÉ ONDE ISTO É SEGURO?

Muitas vezes ser um cliente nos leva a uma experiência aborrecida. Basta precisar de algum bem ou serviço para ter de conformar-se em despender muito tempo para encontrar aquilo que se necessita. No final, o golpe de misericórdia é tornar-se cliente em um processo qualquer dentro da empresa. Mas poderia ser pior, pois se contratarmos algum tipo de serviço, murmúrios de descontentamento começariam a zunir pela nossa cabeça. "Eu quero um empréstimo, não um quilo de formulários para preencher". Ou ainda: "Eu quero leite na geladeira, não permanecer uma hora na mercearia".

Num país cartorial como o Brasil, será que estaremos preparados para o bombardeio de *telemarketing* que está por vir, convidando-nos a mudar algo para ganhar? Hoje infelizmente, empresas correm para a Internet somente a fim de seguir os passos de um concorrente para não ficar para trás, por puro modismo e não pela melhoria e comodidade de atendimento aos seus clientes, que acaba tendo que telefonar para a empresa a fim de tentar desvendar como ela subdivide o atendimento pelos seus diversos departamentos e descobrir o processo por trás de cada requisição.

No passado não era assim. As compras eram efetuadas em sua maioria nos poucos e próximos fornecedores ou mercadinhos, que geralmente possuíam poucas opções, menos vendedores e muito menos transações. Mas em compensação, a relação cliente e fornecedor era muito mais íntima, os fornecedores já conheciam as suas preferências, a quantidade

habitual, podendo adivinhar muitas vezes qual a novidade que você compraria caso ela tivesse na prateleira.

O uso intensivo da tecnologia vem permitindo combinar o bom e o ruim do passado. Vejamos o que se consegue, por exemplo, com a Internet. Temos uma vasta lista de produtos para escolher, mas perdemos muito tempo em pesquisas, além de expormo-nos a estranhos ao dizer o que queremos e quem somos. Contudo, a tecnologia servirá para transformar o aborrecimento de ontem na oportunidade de hoje. O fundamento comercial se baseia em saber exatamente quanto o cliente quer, aonde e quando, sem perda de tempo e nem muito esforço. A Internet está bem posicionada para fortalecer a tendência à eliminação dos intermediários em atividades de rotina, como o fornecimento constante de mercadoria a clientes. Ao se comunicar diretamente com eles, as empresas não apenas eliminam intermediários mas aumentam a fidelidade. A Internet pode se delinear como uma ferramenta crítica de coleta de dados, com a qual consumidores podem enviar críticas ou comentários em relação aos produtos e serviços. A simples monitoração fará com que as empresas possam aprender novas maneiras de personalizar seus produtos e melhorar o atendimento que prestam a seus clientes, fundamentos básicos para uma empresa aumentar sua participação no mercado.

Desta maneira, o ato de comprar será novamente uma atividade social dentro do cenário comercial. Os negócios são orientados para os clientes, ao invés de produtos ou divisões, e com foco para os valores individuais ao contrário de rentabilidade cega. Este será o estratagema maior, o investimento de longa duração de todas as empresas de sucesso.

Com tudo o que já foi dito a respeito da Internet, em relação aos seus benefícios e facilidades e a sua inevitável proliferação no mundo empresarial, devemos também atentar para os perigos advindos desta nova forma de comercialização e divulgação de produtos e serviços. A rede mundial de computadores acaba se tornando um "prato cheio" para pessoas mal intencionadas, que se utilizam de má fé para realizar operações indevidas em seu favor tais como: destruir arquivos e programas, efetuar transações financeiras em favor próprio ou de terceiros, sabotar dados, e muito mais causando prejuízos gigantescos em algumas empresas.

O volume de negócios realizados pela Internet em 1997, foi cerca de US$8 bilhões ao ano, e deve chegar aos US$330 bilhões até o ano 2002, segundo dados do instituto americano *Forester Research.* O dado relevante é que estas cifras astronômicas carregam consigo uma dicotomia: à medida que cresce as expectativas de negócios na Internet, aumentam também os problemas com a segurança das informações. Ou seja, ao mesmo tempo que a rede mundial

abre muitas portas para negócios, abre muitas outras para pessoas mal intencionadas, os chamados invasores ou *hackers*. Por isso, qualquer empresa que esteja pensando em montar um *site* de comércio na rede mundial deve antes de tudo estabelecer uma política de segurança, bem planejada e implantada, para evitar ou ao menos reduzir os riscos de invasões e violações aos seus sistemas de informações.

Uma recente pesquisa realizada pelo *Computer Security Institute* (CSI), dos Estados Unidos, revela quão é crítica a questão da segurança. Os resultados são bastante preocupantes, dos 520 profissionais de segurança de empresas, governos, instituições financeiras e universidades americanas entrevistados, 64% responderam que sofreram violações na segurança nos últimos doze meses, um percentual 16% maior que o do ano passado. Dentro deste universo, 72% dos entrevistados reconheceram que tiveram perdas financeiras com a quebra na segurança, mas somente 46% souberam quantificar essas perdas. O prejuízo devido a essas invasões chegou a US$136 milhões.

As principais causas detectadas pelo CSI foram ataques por meio de acessos não autorizados de funcionários (44%), negligência com serviços (25%), invasão através de sistemas externos (24%), roubo de informações confidenciais (18%), fraudes financeiras (15%), e sabotagem em redes e dados (14%). Diante disso, especialistas observam que fica claro a deficiência das empresas tanto na forma de implantação quanto na divulgação de uma cultura global de segurança junto aos seus funcionários. Daí, a defesa de alguns de que sejam estabelecidas punições no sentido de fazer com que os usuários cumpram as medidas de segurança estabelecidas pela empresa.

O número de violações de segurança no mercado americano é assustador, nos demais países a situação não é diferente. Uma prova disso são os resultados da primeira pesquisa internacional sobre segurança da informação realizada pela Ernest & Young no ano passado. De acordo com Celso Leite, diretor de desenvolvimento de negócios na área de segurança de sistemas de informações da empresa, a pesquisa foi realizada com 4.320 empresas em 29 países, incluindo o Brasil. Apesar de 82% das empresas entrevistadas terem considerado importante a segurança das informações, 74% reconheceram que houve um crescimento dos riscos nos últimos anos. Mesmo assim, 63% delas disseram que expandiriam o uso da Internet para realização de negócios, desde que houvesse um nível maior de segurança. No tocante a perdas financeiras com violações internas e externas, ficou demonstrado que 51% delas foram

causadas por desastres não-naturais, que paralisaram os sistemas ou interromperam as ligações por problemas de telecomunicações.

A ênfase dada atualmente na implementação de uma política de segurança diz respeito à sua integração aos negócios da empresa e ao envolvimento dos vários departamentos. Nesse sentido, o administrador da rede passa a funcionar como uma peça-chave do processo, o qual será responsável por procedimentos e padrões de configurações das redes. "Por ser estratégica, a política de segurança deverá envolver diversas áreas na sua elaboração como a de informática, O&M, e diretoria de tecnologia da informação, além da alta direção da empresa, afirma Rubens Nicolluzzi, gerente de marketing da Prolan, uma empresa integradora de redes e de sistemas de segurança.

Numa visão ampla da realidade das invasões, a política de segurança das informações deve conter um conjunto de medidas não somente para proteger a rede, mas a própria empresa, já que há várias portas de entrada e de fluxo de informações fora do ambiente de informática. Conforme explica Fernando Nery, diretor-presidente da Módulo Consultoria e Informática, existem três tipos de prejuízos para as empresas causados por invasões: o patrimonial, que ocorre quando há um ataque direto ao caixa da empresa; o operacional, quando os negócios são interrompidos, no caso de um *site* da Internet sair do ar; e a imagem, cuja preservação está à cargo da equipe de comunicação e dos executivos.

Da série de procedimentos a serem observados para a definição da política de segurança, a primeira ação a ser feita é a análise de riscos físicos, lógicos e administrativos da rede e das aplicações críticas – como protegê-las e qual o seu valor –, bem como a identificação das pessoas que poderão ou não ter acesso aos dados e quais as informações acessíveis. Na política de segurança serão determinadas as formas de certificação e de autenticação com uso de chaves públicas, assinaturas digitais, senhas e hardware e software responsáveis pela geração de informações de identificação e certificação do usuário, incluindo métodos de proteção do acesso à rede, como os *firewalls*. Estipuladas as regras, inicia-se a formatação da sua implementação, identificando-se as ferramentas adequadas. A gerente de redes e comunicações da Hitech, Maria Tereza Aarão, explica que as empresas que utilizam políticas de senhas, deverão ter muito cuidado para que as mesmas sejam bem construídas e substituídas periodicamente, devido aos custos de administração e gerência, que poderão tornar-se elevados, como no caso do *help-desk* – muito utilizado quando o usuário esquece a

senha, entre outros problemas – causando um custo de US$80 por cada senha ao ano, segundo um dado extraído de estudos internacionais.

Para uma política mais complexa, um conjunto de outras ferramentas irão defender a rede contra ataques. Existem no mercado uma série de empresas que oferecem essas ferramentas que se baseiam em diversas variantes de defesa da rede. Aparelhos como roteadores, *firewalls, proxies*, sistemas de criptografia, produtos de certificação, são algumas destas ferramentas. Além destas ferramentas, algumas empresas utilizam táticas de defesa como a proteção em vários pontos da rede, a segurança nas estações e o gerenciamento da segurança nos servidores. Mesmo com todas estas inovações tecnológicas, o risco de invasão é grande e os empresários devem estar atentos para estas inovações e sempre procurarem utilizar normas de segurança bem definidas para a sua empresa, pois do contrário, o prejuízo pode ser incalculável.

7. CONCLUSÃO.

Por tudo que se tem dito e pela evolução que tem ocorrido, passou a ser peça fundamental para o auditor seu conhecimento e aplicação em processamento eletrônico de dados.

À primeira vista, o processamento eletrônico de dados com sua mistura enriquecida de jargões técnicos, o conjunto dos programas aplicativos operacionais, os equipamentos de computação e seus periféricos apresentam-se como um obstáculo aparentemente intransponível aos olhos da auditoria convencional.

Contudo, o processamento eletrônico de dados é parte presente, e cada vez em maior escala, da organização, fazendo com que mais setores, áreas e atividades sejam por ele auxiliadas e controladas.

Dessa forma, a iniciação da auditoria na área de processamento de dados deve obedecer a um critério, baseado na posição em que esteja na organização e suas necessidades reais.

A auditoria em processamento eletrônico de dados encontra-se ainda em fase de desenvolvimento, na busca de pessoal que reuna condições técnicas adequadas do perfil do auditor convencional, acrescido do conhecimento técnico suficiente na área de processamento de dados.

A definição do que representa a auditoria em processamento de dados é importante para desenhar a configuração do composto do auditor, seu aprendizado e aplicação real na empresa. É imprescindível que este setor de auditoria conduza-se no exame de adequação dos sistemas computadorizados e no subsídio às tarefas das áreas de auditoria convencional.

O trabalho de auditoria, mesmo na área de processamento de dados, está com sua preocupação voltada para a adequação do sistema de controles internos, quer sejam estes computadorizados ou não. Por outro lado, a administração da empresa necessita de que alguém lhes diga que as informações recebidas dos computadores são confiáveis e obtidas de acordo com critérios adequados, planejados de forma econômica e salvaguardados os direitos da própria empresa.

Antes de mais nada, os auditores devem perder a "fama" de que eles só servem para detectar falhas na operacionalização da empresa, isto não é verdade, e somente eles podem provar isto. Os auditores devem assumir um papel de assessor da alta administração da

empresa, não só identificando os problemas da empresa, mas sim prestando informações que sirvam como prevenção dos mesmos. Além disto, os auditores possuem informações suficientes para sugerir medidas que acarretem em melhorias para a empresa. À medida que estas informações forem repassadas e adotadas dentro da empresa, os empresários passarão a ter uma nova visão do auditor e da profissão contábil.

8. REREERÊNCIAS BIBLIOGRÁFICAS:

• VERHALEN, Berthold./ DOMINGUES, Diva T. M./ SOUZA, Hamilton E. L./ COSTA, João C. F./ MIRANDA, José C./ FONTANA, Júlio C./ MACIEL, Luiz A. C./ ROZIN, Luiz A./ NAVARRO, Nelson C. ***Procedimentos de Auditoria Informática.*** Instituto dos Auditores Internos do Brasil. (1992)

• **Revista LANTIMES Brasil:**

LT.1 (Vol.4, Ed. 29, pág. 34 e 35, 22.06.98)

LT.2 (Vol.4, Ed.27, pág. 18, 19, 32 e 33, 25.05.98)

LT.3 (Vol.4, Ed.42, pág. 42, 17.08.98)

LT.4 (Vol. 4, Ed. 32, pág. 26, 17.08.98)

• COULOURIS, George./ DOLLIMORE, Jean/ KINDBERG, Tim. ***Distributed Systems, Concepts and Design.*** (Edit. ADDISON-WESLEY. Ed.2ª, Págs. 484 a 487, 1992)

• RAMOS, Tagil O. O *call center* cai na Internet. ***Revista INFOEXAME.*** Ano 13, Nº151, págs. 122 e 123, Outubro/1998.

• **SITES:**

1) www.modulo.com.br

2) www.infoexame.com.br

3) www.auditoria.com.br

4) www.receitafederal.gov.br