UNIVERSIDADE DE SÃO PAULO
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE
DEPARTAMENTO DE ADMINISTRAÇÃO

DISSERTAÇÃO DE MESTRADO

SEGURANÇA EM PROCESSAMENTO DE DADOS

EDSON LUIZ RICCIO

ORIENTADOR: PROF. DR. NICOLAU REINHARD

SÃO PAULO
1981

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE ECONOMIA ADMINISTRAÇÃO E CONTABILIDADE
DEPARTAMENTO DE ADMINISTRAÇÃO

SEGURANÇA EM PROCESSAMENTO DE DADOS

EDSON LUIZ RICCIO

Dissertação apresentada ao
Departamento de Administração
da Faculdade de Economia,
Administração e Contabilidade da
Universidade de São Paulo para
a obtenção do Título de Mestre
em Administração.

Orientador: Prof. Dr. Nicolau
Reinhard.

São Paulo
1981

AGRADECIMENTOS

Quero expressar ao Prof. Dr. Nicolau Reinhard, meu reconhecimento pela sua inestimável colaboração e apoio, fundamentais para a execução e finalização deste trabalho.

À Amália pelo incentivo e apoio na realização de mais esta etapa.

DATA PROCESSING SECURITY

EDSON LUIZ RICCIO

The business community and the Data Processing and Information Systems professionals are facing today a new kind of challenge: the Computer threat.

The increasing number of installed computers and the large utilization of teleprocessing and networking techniques are pushing the organizations to be greatly dependent on the Information Processing Facility and its final product: the computerized information systems and the associated environment. It is not very difficult to verify that the impact of this fast growing technology has been only partially absorbed not only by users but also by the computer professionals. In fact, the computer development is not being followed by the corresponding development of the Data Processing Administration Principles.

This means that the control and administration guidelines for this type of activity are not in the desirable stage, i.e., no final conclusions have been set up on how to obtain a completely secure and reliable Data Processing Installation. This "open Window" is, as a consequence, the shortest way for criminal practices and generalized errors which will result in the damage of the organization's assets and operations.

The concept of security largely used today refers mostly to the physical security and does not cover all the components of the Data Processing Installation as it should be understood:

- a) The Physical Installation - including the hardware, software, lay-out, auxiliary equipment, telephone lines , etc..
- b) The computerized information system (formal batch system)

c) The computerized information systems using advanced techniques such as Data Base and Data Communication.

d) The Process of Information Systems Development (Methodology)

In this study, we propose that the concept of security be extended to all the elements of the Data Processing environment, as a basic factor which contributes to its integrity and effectiveness.

As a contribution to the study of the Data Processing Administration, we present, for each element, the most critical causes of exposures and the most important controls which may reduce the impact of these causes.

ÍNDICE

I - ESTRUTURA DESTE TRABALHO.....	6
II - O INVESTIMENTO PRESENTE EM UMA INSTALAÇÃO DE PROCESSAMENTO DE DADOS	7
III- O CONCEITO DE SEGURANÇA EM PROCESSAMENTO DE DADOS.....	10
IV - OS ELEMENTOS DE UMA INSTALAÇÃO DE PROCESSAMENTO DE DADOS	14
V - OS RECURSOS FÍSICOS DE PROCESSAMENTO DE DADOS	16
VI - O SISTEMA DE INFORMAÇÃO VIA COMPUTADOR	32
VII - O SISTEMA DE INFORMAÇÃO QUE UTILIZA TÉCNICAS AVANÇADAS.	53
VIII - O PROCESSO DE DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO (PDSI).....	67
IX - O PLANO DE EMERGÊNCIA E RECUPERAÇÃO (PER).....	81
X - CONCLUSÃO.....	90
XI - BIBLIOGRAFIA	93

I - ESTRUTURA DESTE TRABALHO

Este trabalho está organizado de forma a apresentar para cada Elemento componente da Instalação de Processamento de Dados os seguintes tópicos:

- Descrição do Elemento: subentende-se, aqui, que o leitor está familiarizado com o assunto “Processamento de Dados”. Portanto, esta descrição destina-se, tão somente, a posicionar os aspectos mais importantes de cada um.
- Causas de Ameaças: Relacionamos as principais causas que geram ameaças aos recursos de cada Elemento.
- Controles de Segurança: Estão indicados aqueles que possam ter maior efeito sobre as Causas de Ameaças.

II - O INVESTIMENTO PRESENTE EM UMA INSTALAÇÃO DE PROCESSAMENTO DE DADOS

O investimento em uma instalação de Processamento de Dados é o montante de recursos monetários e não monetários que a empresa emprega com a finalidade de obter adequados sistemas de informação. Os sistemas de informação representam a estrutura formal estabelecida para o fluxo e o Processamento de Dados.

Ao decidir pela implantação de Processamento de Dados, uma empresa leva em consideração, antes de qualquer coisa, suas necessidades de informação mais rápidas e objetivas.

Após algum tempo, as atividades de desenvolvimento de projetos somados às de manutenção dos sistemas já implantados, bem como a operação do conjunto de Processamento de Dados, passam a absorver recursos financeiros gradativamente maiores.

As aplicações destes recursos podem ser classificadas em duas categorias:

a) Despesas com a instalação da área de Processamento de Dados, envolvendo os seguintes tópicos:

- Encargos iniciais de contratação do equipamento;
- Custos das instalações físicas - ar condicionado, sistema elétrico, sistema de prevenção e combate a incêndio;
- Móveis e equipamentos auxiliares.

b) Despesas mensais com a operação normal da área

- Aluguel do equipamento (ou leasing);

- Despesas com a manutenção dos equipamentos (em caso de serem adquiridos ou na forma de leasing);
- Gastos com formulários contínuos, cartões, disquetes, fitas de impressão, material de escritório, em geral;
- Linhas telefônicas para telecomunicações (linhas urbanas privadas, canal de voz Embratel ou Rede Transdata);
- Amortização mensal dos encargos iniciais de contratação do equipamento, das instalações físicas e dos móveis e equipamentos auxiliares.

c) Custo do desenvolvimento de um projeto

Este ponto encontra-se ainda pouco discutido dentro da comunidade de Processamento de Dados. O que se tem verificado na prática é que, em grande parte das empresas, a maior preocupação com custos ocorre na fase inicial da instalação da área e, principalmente, no aspecto de máquina e construção da área física para funcionamento do computador, ar condicionado , etc..

Em segundo plano, assume certa importância o controle dos gastos com a mão-de-obra especializada que compõe a totalidade da instalação.

Pouca ou quase nenhuma ênfase, no entanto, é dada ao custo do sistema pronto, e por conseguinte, às análises de custo-benefício (a priori), tão importantes para a decisão final sobre a validade deste ou daquele projeto.

Para os objetivos deste trabalho é, de qualquer forma, fundamental efetuarmos as seguintes perguntas: *“Quanto vale cada um dos sistemas que estão implantados na empresa?”* ou *“Quanto representam para a sobrevivência de uma empresa, as informações e os dados gerados e manipulados pelos sistemas A, B e C?”*

Muito embora as respostas a estas perguntas possam situar-se, em grande parte, no plano da especulação em torno dos diferentes critérios de avaliação do custo da informação, existe, pelo menos, um aspecto que pode ser abordado com grande grau de certeza: os sistemas de informação de uma empresa representam um ativo de alto valor estratégico.

Por outro lado, eles não podem ser tratados separadamente dos elementos da instalação, onde eles foram desenvolvidos e onde atuam.

Assim, o investimento feito em um sistema de informação é formado não apenas pelo número de horas de análise e programação, treinamento e de máquina despendidos em seu desenvolvimento, mas também pelo alto valor intangível dos benefícios que ele gera.

Portanto, ao enfocar o estudo da segurança em Processamento de Dados nas organizações não podemos limitar-nos à consideração simples de que os gastos com esta atividade se situam entre 1 e 2% do faturamento bruto da empresa, de acordo com os *standards* definidos para isto. Na realidade, estas quantias atingirão níveis bem mais elevados se lhes acrescentarmos os valores intangíveis ou não monetários representados pelo uso da informação na manutenção da continuidade da empresa.

Outro aspecto importante que queremos ressaltar é que sendo a instalação de Processamento de Dados uma área tipicamente prestadora de serviços, os resultados de sua ação penetram e se agregam às áreas usuárias, criando uma relação de co-responsabilidade quanto aos recursos financeiros aplicados, bem como aumentado o nível de interesse pela proteção e segurança da área de Processamento de Dados.

III- O CONCEITO DE SEGURANÇA EM PROCESSAMENTO DE DADOS

Muito mais do que se possa pensar, a dependência das operações normais de uma empresa, em relação a sua área de Sistemas e Processamento de Dados é cada vez mais crítica e merecedora de análise adequada.

A segurança em Processamento de Dados é assunto que justifica, não só a atenção de Administradores de P.D., Auditores, Gerentes Financeiros, Usuários em geral, mas também da Alta Administração. Isto porque o risco recai não apenas em equipamentos e sistemas, representando vários milhões de reais, mas, também sobre dados e informações que, se não são mais importantes, têm a característica mais crítica, que é a quase total impossibilidade de reposição.

As medidas aplicadas pelas empresas, na sua maioria, visam impedir a ocorrência de um desastre e são, via de regra, tradicionalmente conhecidas como medidas de prevenção de incêndio. Pretendemos ampliar este conceito de segurança dizendo que: “qualquer que seja o controle adotado, as chances de serem ineficazes são bastante grandes e, portanto o risco estará sempre presente”.

Além disso, não é somente o fogo que representa uma ameaça ao Processamento de Dados. Outros agentes, internos e externos, são igualmente importantes e não devem ser relevados.

O crime por computador é uma ameaça cada vez mais constante a todas as organizações que usam o Processamento de Dados e dele dependem para a realização de seus objetivos maiores.

Assim, propomos que o termo Segurança tenha um enfoque mais abrangente que a simples proteção aos recursos físicos.

Decorre daí, portanto, que uma instalação segura é aquela que consegue garantir uma atuação eficaz e gera os benefícios esperados pela organização, apesar das ameaças constantes, a que está sujeita.

Os Tipos de Controles de Segurança

Na parte final de cada Elemento, passaremos a enumerar os tipos de Controles que são recomendados para uma Instalação de Processamento de Dados. Segundo a maioria dos autores pesquisados, os controles podem ter características diversas quanto à sua aplicabilidade e ação sobre uma ou mais causas de ameaça.

Como decorrência da análise destas características, a classificação dos controles que nos parece mais oportuna é a que considera o tipo de ação obtida por cada um, em relação a cada elemento de uma Instalação.

Desta forma, temos a seguinte categorização de controles:

- Controle Preventivo - É o que age como guia para que certas operações se desenvolvam na forma desejada. Não representa uma barreira intransponível, mas contribui eficazmente para a redução das causas de ameaças.
- Controle Detectivo - Embora não previna a ocorrência de um problema, tem condições de alertar a organização para que sejam adotadas as medidas corretivas necessárias a tempo de evitar que o problema evolua para uma ameaça, na qual o prejuízo seria maior.
- Controle Corretivo - Uma vez detectado um problema, sua correção ou eliminação é fator essencial para a continuidade das atividades da Instalação. Este tipo de controle age no sentido de conduzir à normalização do problema.

Grau de Eficácia dos Controles

Queremos chamar a atenção para o fato de que a caracterização dos controles preventivos, detectivos e corretivos é feita segundo critérios subjetivos e, tendo em vista, a tendência de cada um agir em relação a este ou aquele tipo

de problema. O “mix” ideal de controles a serem selecionados para uma dada Instalação deve ser resultante de cuidadosa análise de custo-benefício, em que se leve em consideração os tipos de risco relacionados à empresa específica.

Poderá, também, de uma empresa para outra, surgir uma situação na qual um ou mais dos controles, aqui apresentados, não sejam aplicáveis, dada à natureza da Instalação ou da empresa.

AS CAUSAS DE AMEAÇAS DE UMA INSTALAÇÃO DE PROCESSAMENTO DE DADOS

Uma vez estabelecido que toda a instalação de Processamento de Dados representa para a empresa um recurso de alto valor, não só financeiro como estratégico, devemos iniciar uma análise dos possíveis tipos e formas de causas de ameaças a que ela esteja sujeita.

Para isto, necessitamos definir o conceito de ameaça a uma empresa que se utiliza dos serviços de Processamento de Dados.

Achamos bastante apropriada a conceituação proposta pelos autores William Mair, Donald Wood e Keagle Davis em seu livro *“Computer Control and Audit”*, ao dizer: *“Uma ameaça é o efeito de uma causa (expressa em dólares), vezes a sua frequência possível de ocorrência ..... O fogo, por si só, não é uma ameaça. Uma ameaça é a destruição que o fogo pode causar”*.

Assim, as ameaças não surgem espontaneamente ou simplesmente pela ausência de controles. Podemos afirmar que, sem dúvida, as ameaças são causadas.

O estudo da Segurança em Processamento de Dados destina-se a definir controles apropriados que possam atenuar ou, às vezes, eliminar estas causas.

Outras relações são importantes de serem observadas entre controles, ameaças e causas.

Muito embora os controles sejam estabelecidos no sentido de eliminar ou reduzir as ameaças eles agirão de fato sobre as causas.

As Categorias de Ameaças que Afetam as Empresas Como Decorência de Falhas na Segurança de suas Instalações de Processamento de Dados:

- Registros que não refletem a real situação dos recursos;
- Informações contábil-financeiras não confiáveis;
- Interrupção parcial ou total nas operações da empresa;
- Decisões Gerenciais não adequadas;
- Sanções fisco-legais;
- Incremento nos custos de operação;
- Perda ou destruição de arquivos estratégicos;
- Desvantagens em relação à Competição.

IV - OS ELEMENTOS DE UMA INSTALAÇÃO DE PROCESSAMENTO DE DADOS

Os elementos de uma instalação de Processamento de Dados que são, aqui apresentados, baseiam-se em uma situação mais freqüentemente encontrada nas nossas empresas.

Existem, atualmente, grandes dificuldades na determinação de tipos de classificação do porte de equipamentos, uma vez que fatores de utilização de computação, tais como: complexidade das aplicações, volume, forma de processamento, forma de agrupamento dos dados e recursos de software envolvidos formam, na prática, um número bastante grande de combinações possíveis.

A classificação rígida, baseada em um ou mais dos aspectos acima, por sua vez, não se revela indispensável para os efeitos deste trabalho, pois os princípios de segurança são igualmente válidos para todos.

Assim sendo, chamaremos de instalação típica de Processamento de Dados o conjunto que passamos a descrever, o qual será utilizado para a abordagem dos aspectos de segurança e controle mais relevantes:

- Os Recursos Físicos de Processamento de Dados;
- O Sistema de Informação Via Computador;
- O Sistema de Informação que Utiliza Técnicas Avançadas;
- O Processo de Desenvolvimento de Sistemas de Informação.

Organização da Função de Processamento de Dados

A estrutura organizacional da área pode sofrer grandes variações em seu porte e subdivisão interna, conforme o tamanho da empresa e, quer se trate de órgãos públicos, indústrias, instituições financeiras, comércio ou institutos de pesquisa.

De qualquer jeito, no entanto, o organograma seguinte indica a forma mais usual de disposição das suas várias funções.

Queremos observar que embora a estrutura organizacional seja um dos elementos de uma Instalação de Processamento de Dados, achamos mais apropriada a menção de suas causas de ameaça e de controles de segurança em cada um dos capítulos seguintes.

Figura 1 – Organização da função de processamento de dados

V - OS RECURSOS FÍSICOS DE PROCESSAMENTO DE DADOS

1- Equipamentos

Referimo-nos aqui ao conjunto de equipamentos que compõem o comumente chamado CPD (Centro de Processamento de Dados). No transcorrer deste trabalho, os termos “computador” e “configuração de processamento de dados” serão utilizados com o mesmo significado.

Assim, os principais tipos de equipamentos de Processamento de Dados estão divididos em:

a) Computador, composto por:

- Unidade Central de Processamento;
- Unidade de fita magnética;
- Discos magnéticos;
- Impressora;
- Leitora de Cartões;
- Vídeo de Controle do Sistema;
- Terminais de vídeo e impressores, locais e remotos.

b) Equipamentos de entrada de dados (off-line) (on-line).

c) Meios de retenção e arquivamento de Dados:

- Discos;
- Fitas.

d) Equipamentos auxiliares e de sustentação:

- Gerador e/ou Sistemas de suprimentos de energia de emergência (*No break*);
- Reguladores de Voltagem;
- Ar Condicionado e respectivos controles.

e) Equipamentos de Comunicação e Telecomunicação:

- “*Modems*”;
- Dispositivos de comutação;
- Telefones e linhas privadas.

2 - Suprimentos:

- Formulários *standard* e especiais;
- Cartões, disquetes, cassetes;
- Fitas para impressora, perfuradoras , etc..

g) Documentação interna:

- De Sistemas;
- De Programação;
- De Operações;
- De Controle e Administração do CPD.

h) Dados (embora sempre se encontre contidos em fitas ou discos, o destaque é importante para efeitos desta análise).

i) Móveis e acessórios:

- Mesas, armários, cadeiras, móveis especiais da sala de Operações;
- Máquinas cortadoras e descarbonadoras.

CAUSAS DE AMEAÇAS

1- Erros Humanos

- 1.1 - Erro de digitação e/ou de conferência
- 1.2 - Comandos indevidos via Vídeo de Controle do Sistema
- 1.3 - Uso indevido de arquivos e programas
- 1.4- Danos causados a arquivos reais (eliminação indireta de registros, atualização imprópria, perda de situação (pai, filho))

2- Falhas nos Equipamentos, Software de Controle do Sistema e Utilitários

- 2.1 - Interrupção do processamento por defeito técnico do equipamento, variação ou falta de energia.
- 2.2 - Perda de dados durante o processamento.
- 2.3 Processamentos corretos, porém indevidos.

3- Ações desonestas

Nesta categoria, encontramos os tipos de causas que visam à prática de atos criminosos com o uso do computador ou em relação aos dados que são por ele manipulados. O estudo do crime por computador, com a finalidade de estabelecer correlações entre os atos praticados, o mecanismo adotado e as condições em que ocorrem, é ainda bastante precário. A obtenção completa dos fatos, por motivos, os mais diversos, é muito difícil e não permite ao pesquisador a elaboração de conclusões generalizáveis. No entanto, é importante abordar os tipos mais comuns, segundo os dados colhidos até o momento:

3.1 - Fraude: uso do computador com objetivo de distorção, modificação ou geração de informações falsas que resultem no benefício ilícito para uma ou mais pessoas ou organização.

3.2 - Invasão de Privacidade: ocorre quando é executada a penetração não autorizada nos arquivos de informação do CPD de uma empresa, com a finalidade de colher dados ou informações que serão usadas ilegalmente pelo executor. O uso ilegal destes dados ou informações pode, por exemplo, ser utilizado para beneficiar competidores da empresa ou para serem “vendidos” a outros interessados. A Invasão de Privacidade pode também representar o passo inicial para uma ação de Fraude posterior. Esta penetração é feita pela leitura dos arquivos existentes em fitas ou discos magnéticos.

3.3 - Ações de Roubo e Sabotagem: Ocorrem quando objetos ou meios magnéticos de gravação de dados são retirados do CPD com a intenção clara de provocar interrupções no processamento ou para serem utilizados externamente (ex.: roubo de fitas magnéticas, disquetes, cartões , etc..)

4 - Catástrofes em Geral

Nesta categoria de causa, incluímos todos aqueles que podem atingir de forma contundente o elemento “Recursos Físicos” e onde encontram-se, não só os equipamentos, mas também, os dados manipulados pela Instalação. Como resultado de uma Catástrofe, teremos sempre a paralisação total ou parcial das atividades da Instalação, que por sua vez, pode provocar a interrupção de boa parte das operações da empresa.

As causas de Catástrofe são:

4.1 - Fogo - Como sabemos, todos os componentes de um CPD são altamente sensíveis ao fogo e a altas temperaturas. Mesmo quando o fogo não atinge diretamente os equipamentos, fitas e discos magnéticos poderão ser completamente danificados pela exposição à alta temperatura.

4.2 - Água - A penetração de água, quer seja por inundação ou vazamentos em condutores, pode causar curtos-circuitos que resultarão na destruição dos equipamentos.

4.3 - Tempestades - Obviamente, este tipo de catástrofe pode não só atingir diretamente a instalação mas, principalmente, certos meios de suporte do CPD. Por exemplo, uma tempestade pode danificar a empresa e paralisar a Operação do Computador. Igualmente poderá haver a interrupção de linhas de comunicação, gerando a paralisação na transmissão de dados, quando esta existir.

4.4 - Atos de vandalismo ou desordem civil - Como se sabe, as Instalações de Processamento de Dados são portadoras de alta concentração de informações estratégicas para a empresa. Este fato, já bastante difundido popularmente, pode conduzir as ações de vandalismo ou desordem civil, no sentido de atingir os locais onde se situa a Instalação, com a finalidade de sua destruição e, conseqüente paralisação da empresa.

CONTROLES DE SEGURANÇA

Os objetivos dos Controles de Segurança, em relação a este Elemento, são:

- Detecção de erros em geral;
- Evitar o acesso não autorizado à área de operações e o uso indevido do equipamento e dos dados;

- Registro e análise das atividades desenvolvidas pela área de Operações.
- Manter a continuidade dos serviços de Processamento de Dados.

Controles Preventivos

1- Segregação de funções

Este controle, bastante tradicional em todas as áreas da organização, tem suma importância no Processamento de Dados. Trata da separação em subáreas apropriadas, de funções que, se reunidas em um único setor, dariam margem a ações não autorizadas em relação à Instalação. Desta maneira, são as seguintes as principais características da segregação de função:

- Área de Processamento de Dados deve ser independente de áreas usuárias, onde sejam iniciados qualquer tipo de transação e também não deve tomar a iniciativa de criação de transações.
- A operação de Computador deve ser totalmente independente da biblioteca e do controle de entrada e saída.
- Os Programadores e analistas não devem ter acesso à operação do equipamento para testes e compilações de programas.
- Operadores de computador não devem ter acesso à Biblioteca de fitas e documentação de programas e devem estar separados das funções de controle de entrada e saída.
- O controle de biblioteca deve ser independente da operação de computador.
- Os funcionários de Processamento de Dados não devem ter acesso a funções financeiras ou acesso ao controle dos bens da companhia.
- Periodicamente, deve ser feita a rotação de pessoal.
- Pessoal de Operações não deve tomar a iniciativa para correção de erros em programas ou dados.

2 - Definição de cargos

Deve ser claramente estabelecida e divulgada a cada um dos funcionários da área.

3- Seleção de pessoal competente

Age diretamente no nível de qualidade dos serviços da área.

4 - Manutenção e limpeza da área de operação do Computador

Deve ser evitada, na área do computador a presença de lixo, alimentos, materiais em desuso, cigarro , etc.. A limpeza da área deve ser feita constantemente, uma vez que resíduos e poeira podem provocar danos aos equipamentos.

5 - Manutenção dos equipamentos

A Manutenção preventiva, efetuada pelos técnicos do fabricante, tem função importante na confiabilidade do funcionamento do equipamento.

6 - Ar condicionado

É uma condição básica exigida pelo fabricante dos equipamentos. A manutenção da Temperatura da Sala dentro dos limites recomendados evita a paralisação do equipamento e aumenta sua vida útil.

7 - Planejamento das atividades de operação

A utilização do Computador é uma atividade que pode e deve ser planejada para dar o melhor tratamento da demanda de serviços. Este planejamento é

perfeitamente possível, uma vez que para os sistemas em produção normal, sabe-se com grande grau de certeza, o tempo estimado de processamento de cada um. Desta forma, com certa antecedência (um mês, pelo menos), tem-se uma visão da carga de horas a serem consumidas. Como resultado, o atendimento aos usuários pode ser feito com grau de eficiência desejável. O tempo restante de cada dia, pode assim ser melhor distribuído para atendimento a: solicitações adicionais dos usuários, testes de desenvolvimento, reproprocessamento , etc..

O controle preventivo incrementa o nível de qualidade dos serviços e melhora o “*timing*” de emissão de relatórios aos usuários.

8 - Controle do acesso à área física do CPD

Controlar os meios de acesso ao CPD é uma maneira de evitar o surgimento de tentativas de uso indevido ou sabotagem. Este controle pode ser feito por meio de:

- Fechaduras especiais;
- Cartões magnéticos;
- Sistemas de identificação eletrônicos;
- Guardas.

9 - Restrição na divulgação de informações

Como meio de controle, o pessoal de operação deve ter apenas o conhecimento necessário sobre o Sistema, programação e documentação que permita a perfeita execução de suas atividades.

10 - Guarda de arquivos

A guarda das fitas componentes da Biblioteca é um importante controle preventivo. Qualquer movimentação de fitas (arquivos) deve ser feita sob rígido controle e relacionado com o Planejamento diário de Serviços. O retorno de fitas também deve ser controlado. Para tal, dois conjuntos de controles devem ser mantidos: ficha individual para cada fita, relacionando o conteúdo de cada uma e os dados de utilização, desde sua inicialização.

Quando possível deve ser adotado um sistema computadorizado de controle de Biblioteca de fitas, o qual manterá o controle automático das fitas conjugado com a ficha individual.

11- *Label* externo

Permite a identificação usual do arquivo e evitará a sua utilização indevida.

12 - *Label* interno

Permite a identificação pelo sistema dos dados do arquivo quanto a sua validade, data de expiração conteúdo e utilização.

13 - Anel protetor

Usado nas fitas magnéticas, protege as mesmas contra “deleções” ou regravações acidentais. Quando colocado na fita, o anel aciona um dispositivo que permite a gravação de dados. Ao ser retirado, não existe a possibilidade de gravação.

14 - Proteção do disco magnético

Existem dispositivos no equipamento de disco magnético que permitem controlar as possibilidades de gravação indevida. Este controle é feito pelo operador, de acordo com instrução de operação apropriada.

15 - “Containerização” da área do CPD

É um controle que minimiza as possibilidades de acesso à área e facilita a aplicação de medidas de segurança. Significa, que na época da construção da área, definir um layout, onde a área toda seja naturalmente circundada por paredes e possua um mínimo de pontos de entrada. A sala do Computador deverá estar no centro dessa área.

16 - Treinamento

A constante reciclagem do pessoal técnico com cursos de atualização em suas respectivas funções reduz as possibilidades de erros por falha ou incompetência.

17 - Autorização para entrada

Qualquer que sejam os meios de controle de acesso, deve existir uma relação freqüentemente atualizada onde constem os nomes das pessoas autorizadas a entrar neste ou naquele setor. A utilização de cartões identificadores para cada tipo de acesso é bastante oportuna.

18 - Características dos equipamentos e software básico (CPU e Periféricos)

Este ponto, é decidido quando da escolha do tipo de equipamento. No entanto, os fabricantes incorporam cada vez mais em seus produtos,

dispositivos de controle que asseguram completos diagnósticos em caso de problemas e que permitem rápida análise e normalização.

19 - Localização física

Embora este controle seja instalado quando do planejamento da instalação, os seguintes princípios devem ser observados:

- Evitar áreas de fácil visibilidade ou próximas a janelas.
- Não utilizar paredes com vidros.
- Evitar proximidade de Tubulação de água ou vapor.
- Evitar subsolos ou áreas inundáveis.
- Evitar lugares onde materiais combustíveis sejam estocados.
- Não identificar a área com letreiros ou anúncios chamativos.
- Evitar locais onde haja excessiva vibração e poeira.

Controles Detectivos

1- Supervisão sobre as atividades do CPD.

Significa atribuir claramente responsabilidade ao chefe da área em relação aos seguintes pontos:

- Aprovação do planejamento de utilização no início de cada turno.
- Fiscalizar o decorrer das operações.
- Analisar as atividades que ocorrem durante as “pausas” e interrupções.
- Controlar e verificar os “logs” diários.
- Analisar os resultados da operação de cada turno contra o planejamento feito e determinar as causas dos desvios.

2 - Controle orçamentário

Neste controle, devem ser analisadas as discrepâncias entre o planejado e o real como fonte de constatações de problemas na operação da Instalação.

3 - Relatórios Gerenciais

Devem ser estabelecidos, pelo menos, em bases mensais, onde estejam reportados e analisados os seguintes aspectos:

- Horas de máquina gastas em Compilação, testes reprocessamento, manutenção e Produção normal;
- Para maior confiabilidade, estes relatórios devem ser gerados com base nos dados de “*Job Accounting*”, originados pelo Sistema Operacional.

4 - Relatório de Operador

Deve ser instituído como rotina da função de operação de Computador. Após o término do seu turno, cada operador deve apresentar o relatório de suas atividades, reportando as condições ocorridas desde interrupções de equipamentos até problemas no processamento provocados por programas ou outro fator.

5 - Relatório da Console

Emitido pelo Sistema Operacional, com base nas ações executadas pelo Computador no período, tais como: identificação dos *Jobs*, instruções dadas pelo operador e mensagens do sistema operacional, arquivos processados, indicação de todas as condições de anormalidades ocorridas e mensagens dos sistemas processados.

Diariamente, o relatório da Console deve ser examinado pela chefia de operações e comparado com o relatório do operador para constatação de possíveis anormalidades.

6 - Relatório de Biblioteca de arquivos (fitas e discos)

Este tipo de controle deve estar organizado da seguinte maneira:

- Relatório listando os arquivos de acordo com seu conteúdo ou identificação, para assegurar que *backup* do arquivo esteja disponível em qualquer tempo;
- Relatório que indique para cada fita ou disco, o seu conteúdo:
  - localização atual;
  - Nome do arquivo conforme requerido pelo Sistema;
  - Identificação de volume;
  - Datas de criação, de liberação;
  - Local externo onde se situa o *backup*.

7 - Relatório do Setor de Controle

Este relatório contém informações sobre o comportamento dos dados de entrada e saída do CPD, ou seja, de cada lote recebido e processado e seus respectivos totais de controle.

8 - Verificação de perfuração/digitação

Como controle detectivo, age no sentido de localizar erros de conversão que ocorram na operação inicial. Também esta atividade deve manter estatística de controle de produção evidenciando, por digitador, sua produção (por código de transação) em relação ao período de tempo.

9 - Controles de *Hardware* e de Sistema Operacional

O constante aperfeiçoamento dos equipamentos e dos sistemas operacionais, assegura, atualmente, elevado nível de confiabilidade às operações de processamento. Cada tipo de equipamento oferece uma enorme gama de controles que evitam a passagem de dados deturpados. Idêntica ação é provida pelos respectivos sistemas operacionais. Para entendimento e utilização adequada desses controles, devem ser estudados os Manuais de Equipamento dos fabricantes, bem como os Manuais do Sistema Operacional utilizado.

10 - Verificação de Saídas

O Setor de controle deve verificar visualmente os relatórios de saída antes de distribuí-los aos usuários. Deve ser feita a conferência contra listagens de distribuição de relatórios para verificação de omissões ou enganos.

11 - Sistema de detecção de fumaça

Age no sentido de alertar a segurança da Instalação contra a ameaça de incêndio.

Controles Corretivos

1. Plano de Emergência e Recuperação

Sem dúvida, permite corrigir uma situação de desastre na Instalação. (Ver capítulo especial)

2. Retenção de arquivos

Como forma de prevenir ou obter a Instalação de meios de correção e recuperação em situações de perda de arquivos, o sistema de retenção avô-pai-filho deve ser adotado.

Devem ser definidos todos os tipos de transações a serem retidos e a periodicidade de execução da retenção.

3. Estatística de erros

Devem ser preparadas abrangendo erros de digitação, de operação, de programa, de sistema , etc., para periodicamente, permitirem a ação específica sobre a causa dos erros.

4. Estatísticas de Incêndio

O sistema de combate a incêndio deve abranger não somente a Sala do Computador, mas também, as demais áreas da Instalação.

Os sistemas atualmente oferecidos pelos fornecedores são:

- Sistemas com utilização de gás halon;
- Sistema com utilização de CO₂;
- *Sprinklers* para dispersão de água;
- Combinação de dois sistemas.

5 - Backup local

Deve ser selecionado em local dentro da área da empresa e que tenha condições de abrigar o backup geral (Sistema Operacional, Biblioteca e arquivos). Esse local deve estar protegido contra incêndio e ter acesso fácil, para uso imediato, em caso de perda de dados no processamento.

6 - *Backup* externo

Como no caso anterior, com a diferença de que o *backup* estará guardado em local fora da Companhia, para ser usado dentro das mesmas condições.

7 - Seguro das Instalações

Obviamente, não age sobre a recuperação de informações como outros controles, mas será de grande valia na substituição dos equipamentos e outros recursos destruídos em caso de catástrofe.

8 - Sistema de emergência para fornecimento de energia (*No break*)

Assume papel de grande importância quanto maior for a dependência da empresa em relação aos serviços de processamento de dados.

Dado ao grande investimento que requer, sua aquisição deve ser feita criteriosamente.

A ação deste tipo de equipamento é muito importante, pois permite a Instalação reduzir ou eliminar os prejuízos causados pela interrupção do processamento, em caso de falta de energia.

VI - O SISTEMA DE INFORMAÇÃO VIA COMPUTADOR

Este elemento de uma Instalação de Processamento de Dados é também chamado de Aplicação. Significa o conjunto de operações de processamento ordenados, logicamente, e segundo objetivos comuns, que se incumbe do tratamento dos dados recebidos de outros Sistemas de Informações, com a finalidade de permitir aos seus usuários o controle e ação sobre os recursos a eles afetos. Cumpre esclarecer que a expressão “operações de processamento” não se refere apenas aqueles executados pelo computador, mas também às operações manuais desenvolvidas pelas pessoas dos departamentos afetados pelo sistema.

Para efeito de análise dos princípios de Segurança que se referem a este elemento necessitamos desmembrá-lo em partes menores e seqüenciais conforme segue:

Início - Surgimento dos eventos que são passíveis de tratamento pelo Sistema, a partir deste momento.

Registro- É o passo seguinte, em que o evento é convertido para uma forma documental. Poderá, como seqüência, ser executada alguma codificação e mesmo transcrição do documento original para outro.

Transmissão - O movimento dos dados, por qualquer meio de um local para outro.

Processamento - (pode estar sendo executado por meios manuais ou eletrônicos, total ou parcialmente). Dentro deste grupo, reconhecem-se as seguintes operações:

- Comparação dos dados em relação a testes lógicos ou condicionais para identificação de suas propriedades;
- Execução de operações aritméticas;
- Atualização de conjuntos de dados em arquivo;
- Manutenção de arquivo por meio da adição, “deleção” ou substituição de informações, tendo em vista a utilização futura do arquivo;
- Sumarização de dados usados como “chaves” comuns;
- Classificação dos dados do arquivo em uma dada seqüência.

Processamento de Dados - É a guarda das informações na forma de arquivo para posterior utilização.

Preparação de Informações de Saída - organização dos dados em forma de relatório para a comunicação dos resultados.

Consulta - É a obtenção de informação sem alterá-la.

Os elementos acima apresentados compõem o esquema básico de funcionamento de um Sistema de Informação.

Quanto as suas características internas, estas poderão ser simples, comum ou sofisticado.

Um Sistema de Informação, como aqui definido terá sempre a estreita ligação com os equipamentos de processamento em que é operado e com os respectivos usuários. Estes últimos desempenham importante papel na execução de controles de segurança, como veremos adiante.

CICLO DE PROCESSAMENTO DA INFORMAÇÃO NOS SISTEMAS POR LOTES

Figura 2 – Ciclo de processamento da informação nos sistemas por lotes

Figura 3 – Exemplo de um Sistema de Informação via computador

CAUSAS DE AMEAÇA

As causas de ameaças que atingem este elemento podem ser classificadas, segundo a composição de um Sistema de Informação em:

1. Operações e dados de entrada;
2. Operações de Processamento;
3. Operações e dados de saída;
4. Outros componentes.

Passamos a indicar cada uma das causas, segundo o grupamento acima.

Causas: 1 - Em Operações e Dados de Entrada

1.1 - Perda do dado - pode ocorrer na transmissão, na transcrição ou no reconhecimento do evento inicial.

1.2 - Duplicação de dados - geralmente ocorre no momento da substituição de pessoas no meio de uma transcrição ou digitação ou pela interpretação errônea de que tenha ocorrido o caso 1.1

1.3 - Dados errados - ocorrem pela inversão ou troca de números ou letras.

1.4 - Dados incompletos - os dados estão em desacordo, no seu conteúdo, em relação à necessidade do sistema.

1.5 - Omissão de dados - acidental ou proposital, esta causa pode conduzir a ameaças graves ao elemento, tais como: fraude e roubo.

1.6 - Falta de autorização nos dados - por razões de volume e tempo, alguns sistemas aceitam dados de entrada sem o “visto” ou “identificação” de quem a iniciar. Muito embora certas justificativas possam ser apresentadas para isto, subsiste o fato de que este caso representa causa de problema no processamento do Sistema.

1.7 - Transações que são criadas internamente pelo Sistema - são bastante comuns, pois os programas em computador freqüentemente relacionam dados diversos e criam uma transação resultante desse relacionamento e que aciona ações subseqüentes dentro do sistema. Entretanto, este aspecto é também, susceptível de causar danos ao sistema e às informações de resultantes.

2 - Em operações de Processamento

2.1 - Utilização de arquivos indevidos - os arquivos em computador são criados para utilização posterior, seja por consulta ou conjugação com novos dados de entrada. A sua retenção também é feita com o objetivo de reconstituição de situações anteriores. Assim, a utilização de uma versão anterior de um arquivo, quando não apropriada àquela execução ou à utilização

de outro arquivo, não relacionado com aquele processamento, resultam em um processamento indevido e erro nos resultados.

2.2 - Utilização de arquivo para processamento com registros indevidos - por erro de lógica no programa de atualização, as transações poderão ser processadas contra registros indevidos dentro do arquivo.

2.3 - Processamento incompleto - na confecção dos programas, estes poderão ter operações incompletas que deixam “gaps” na identificação dos resultados apresentados nos relatórios.

2.4 - Processamento errado - por falhas ocorridas em algumas fases do PDSI, certos programas podem não estar executando corretamente as operações a ele atribuídos durante a fase de desenho do sistema.

2.5 - Perda de Arquivos - ocorre quando uma operação de gravação é feita em cima de um arquivo, já existente, ou quando existe a deleção indevida do arquivo inteiro.

2.6 - Perda de programas - a eliminação acidental de um Programa da Biblioteca embora difícil, pode ocorrer por um erro de operação ou ação intencional.

3 - Em Operações e Dados de Saída

3.1 - Distribuição indevida de informação - quando os resultados do processamento são entregues às pessoas, que não os usuários definidos pelo sistema.

3.2 - Distribuição da informação fora do tempo previsto - neste caso, a Informação poderá ser considerada perdida, pois, sem dúvida, não prestará mais para as ações que daí sucederiam.

3.3 - Dados dos relatórios de saída errados - como maior consequência, a perda pelos usuários da confiança no Sistema de Informação. Resultarão daí prováveis atitudes de indiferença e a criação de operações manuais paralelas com incremento nos custos de operação das áreas usuárias.

3.4 - Excesso de pontos de verificação nos programas de consistência - ocasiona o aumento do volume de mão-de-obra por parte dos usuários para a correção dos erros indicados pelo sistema, às vezes, agravado pela freqüência de operação (ex.: diário). Esta situação acarreta resultados muitas vezes piores do que os que resultariam do não-processamento do sistema via computador.

4 - Em outros componentes

4.1 - Sistemas paralelos - são sistemas informais que surgem dentro do mesmo conceito que os sistemas formais, isto é, com entradas, processamento e saídas, e produzem os mesmos resultados que os gerados pelos sistemas autorizados. Muito embora possam ser tomados como sistemas auxiliares do principal, sua existência pode ser fonte de problemas, pois nele a participação dos usuários praticamente não existe.

4.2 - Não adesão ao Sistema pela Gerência envolvida - não obstante, todo Sistema de Informação seja divulgado formalmente é freqüente encontrarmos casos em que a média e alta Gerência “saltam” certos pontos do Sistema ou seus controles. Embora, isto possa ocorrer no sentido de “agilizar” ou “resolver” um problema urgente do dia-a-dia, pode representar uma abertura para atos não autorizados ou fraudes.

CONTROLES DE SEGURANÇA

Os objetivos dos Controles de Segurança em relação a este elemento são:

- Permitir que toda e qualquer transação do sistema seja processada, sem omissões ou duplicações;
- Assegurar que toda e qualquer transação seja validada e, ao ser processada, esteja correta e completa;
- Garantia de que o processamento do sistema seja executado conforme as características predeterminadas;
- Assegurar que as informações resultantes do sistema sejam utilizadas para os fins especificados;
- Permitir que o Sistema tenha condições de autonomia em relação ao seu funcionamento e não dependa de esta ou aquela pessoa ou condição para sua sobrevivência.

Controles Preventivos

1- Definição de Responsabilidade

No âmbito de ação do sistema, deve estar bem clara a definição das tarefas, das responsabilidades e da autoridade de cada área e função no desempenho das suas atividades - esta definição refere-se não só aos usuários como também para as pessoas dentro da Instalação.

2- Confiabilidade do Pessoal

As pessoas que desempenham funções dentro do sistema devem ser adequadamente confiáveis em relação ao grau de responsabilidade das tarefas que desempenhem.

3- Treinamento

O treinamento, tanto dos usuários como do pessoal de sistema, age no sentido de dotar a todos os envolvidos dos conhecimentos necessários sobre os detalhes de operação do sistema. Com isto, minimiza-se a ocorrência de falhas humanas ou erros por ignorância dos detalhes do sistema.

4- Adequação da Capacidade do Pessoal

Em certas atividades do Sistema, há necessidade de qualificação técnica do pessoal envolvido para a sua adequada operação. Exemplo: em um sistema de Controle de Produção, o usuário deve ter formação técnica em Administração Industrial.

5- Operação de Cálculo Aritmético

Em um sistema de informação, devem ser alocados para execução pelo Computador, uma vez que gerarão maior consistência e confiabilidade.

6- Correta agregação de responsabilidade

Trata-se de não atribuir a uma mesma pessoa ou função, atividades que possam representar conflito, como por exemplo: a requisição e a compra de um material não devem ser atribuídas a um mesmo indivíduo ou área.

7- Rotação de responsabilidade

Para sistema com alto grau de risco, é aconselhável que a cada período de tempo (1, 2 anos) seja efetuado o revezamento entre as pessoas e suas respectivas responsabilidades. Isto evita a formação de núcleos de controle informal que podem alterar a performance do Sistema.

8- Uniformização de procedimentos

Dentro de um Sistema, os procedimentos de cada área e função devem ser igualmente claros e completos e com idêntico grau de detalhes.

9- Limites de autoridade

Para muitas atividades do sistema, deve ser estabelecido claramente quem pode ou deve executar a operação. Ex.: Somente um Inspetor de Controle de Qualidade pode emitir documento de apuração de um material recebido.

10- Cofres para guarda de informações críticas

Informações, manuais e tabelas que possam representar risco para o Sistema quando utilizados, evidentemente, devem permanecer em locais sabidamente seguros. Exemplo: Manual de Tabelas Salariais.

11- Duplo controle da informação

Significa que a informação só será aceita pelo Sistema se contiver nítida aceitação por mais de um usuário envolvido. Ex.: O pagamento de uma compra de material implica na evidência de que o requisitante realmente solicitou o material e que o Recebimento realmente o recebeu.

12- Formulários auto-explicativos

É importante que os papéis usados pelo Sistema na vinculação de dados permitam fácil compreensão quanto ao seu preenchimento e conteúdo. Isto reduz as possibilidades de erro e interpretações pessoais indevidas.

13- Pré-numeração de formulários

Necessária quando dentro do Sistema se deseja controlar a veracidade da iniciação de cada informação e efetuar análises, *a posteriori*, sobre os respectivos detalhes de seu conteúdo. Também deve ser utilizado quando a informação estiver relacionada com outros conjuntos de informações.

14- Formulários pré-preenchidos

Sua utilização facilita e reduz erros de transcrição e digitação, pois, evita a reprodução ou reescrita de dados constantes. Pode também permitir a leitura direta por equipamentos, sem intervenção manual. Ex.: Caracteres óticos nas contas de energia.

15-Preparação simultânea

O uso de múltiplas cópias para um formulário, onde, cada uma seja utilizada para diferentes ações, com emissão simultânea, facilita as atividades de registro da informação e reduz erros de transcrição.

16- Pré-preparação de documento

Este controle refere-se à criação, pelo computador, de documento inicial, que circula dentro do Sistema voltando para posterior processamento com as informações complementares preenchidas pelos usuários. Exemplo: Requisição de material pré-preenchida pelo computador, que volta com a informação de qualidade, data e assinaturas preenchidos pelos usuários.

17- Cancelamento de informações já processadas

Para certas atividades, em que existe o risco de reentrada indevida de uma transação, este controle reduz as possibilidades de ocorrência do problema. Exemplo: O carimbo “Processado” aplicado a documentos fonte.

18 - Entrada por exceção

Neste caso, o Computador inicia o processamento interno assumindo certa condição em valor. Isto só será alterado se for recebida informação de entrada que indique condição ou valor diferente.

19- Opção “Default”

É um tipo de controle que deve ser examinado quanto a sua ação, pois pode, por outro lado, representar problemas futuros de flexibilidade do Sistema. Neste caso, certos dados nas transcrições são deixados em branco pelo usuário, conforme determinam os procedimentos. Nestas ocasiões, o Computador assume valor ou condição já previamente definida.

20- Códigos de passagem

Em certos tipos de processamento, pode ser conveniente a criação de códigos de passagem (*passwords*) que assegurem que certas condições foram cumpridas antes do início da transação. Exemplo: Certos tipos de lançamentos contábeis só são aceitos se contiverem código de passagem válidos.

Controle Detectivos

1- Fixação de Horário para o envio de informações aos usuários

Embora sutil, este controle permite a detecção de maneira simples, de problemas na emissão de informações pelo sistema.

2- Ficha de controle de lotes

É o formulário que explicita os documentos que estão sendo enviados em cada lote: quantidade, data, tipo e origem.

3- Controle de seqüência de lotes

O setor de Recepção de documentos do CPD controla a chegada dos lotes pelo seu número seqüencial mencionado na ficha. Qualquer omissão na seqüência é detectada e comunicada.

4- Registro de lotes

É o controle em registro formal, do recebimento de cada lote e suas características.

5- Totais de controle ou documentos ou arquivos

Organizados com base em totais monetários, serve para verificação do comportamento do conjunto de dados em relação aos mesmos valores obtidos em momentos anteriores.

6- Controle da quantidade de documentos

Serve para verificar se os documentos recebidos estão na mesma quantidade mencionada pelo usuários ou após processamento do total de registros processados.

7- Controle do número de linhas

Em documentos em que existe a possibilidade de múltiplas transações, cada linha representa um registro de entrada. Sua contagem tem a mesma finalidade que o controle citado em “6”.

8- Totais de controle não monetário

É a soma, de valores não monetários que servem para o controle de entrada e saída de dados. É geralmente usado onde não existem totais monetários.

9- Total de lote

É o estabelecimento de um total qualquer relacionado com uma certa quantidade de documentos recebidos em dado momento.

10- Controle de fechamento de lote

Serve para detectar se o total de transações processadas confere com os totais de controle anteriormente estabelecidos.

11- Verificação Visual

Quando possível de ser aplicado, o controle visual de documentos pode contribuir para a redução de erros mais gerais, como por exemplo: quando o documento está ilegível.

12- Verificação de seqüência

É a verificação da seqüência alfanumérica dos campos-chave em transações a serem processados.

13- Verificação de limites de área (*overflow*)

Permite constatar se a capacidade de uma área de arquivo será suficiente para acomodar os itens que serão processados.

14- Verificação de formato dos dados nos formulários

Permite detectar campos que estejam preenchidos de forma não apropriada, tanto para dados numéricos como para alfabéticos.

15- Verificação da complementaridade dos dados

É a constatação de que os campos obrigatórios foram preenchidos e para os quais não pode haver brancos.

16- Dígito de verificação

Usado para verificar a validade de dados numéricos. O dígito de verificação é calculado no momento de processamento e o resultado obtido é comparado com o dígito informado na transação. Tem grande ação na detecção de inversão de números.

17- Teste de características

É a comparação de vários campos da informação contra outras informações mestre ou variáveis, com o propósito de detectar a incoerência nos dados. Exemplo: Um material não existente não pode ser requisitado.

18- Verificação de limites de valores

Serve para se detectar possíveis erros ou ação ilegal em transações que envolvam a movimentação de recursos da empresa. O valor da transação é comparado com os limites inferiores e superiores e, se estiverem fora, serão rejeitados.

19- Verificação de validade

Os valores mencionados na transação são comparados contra arquivo, já existentes, verificando-se a igualdade entre ambos, não só quanto ao formato, mas, principalmente quanto à posição e conteúdo dos valores. Exemplo: O número do empregado constante no cartão de ponto deve coincidir com o número existente no arquivo Cadastro Pessoal.

20- Confirmação da informação

Neste controle os dados de entrada são “re-submetidos” ao usuário para confirmação. É comum, nos casos de transmissão oral, de dados via telefone.

21- Data de transação

É a retenção do dia, mês e ano, da transação na forma de calendário para permitir futura comparação de validade da informação em relação ao tempo ou utilização para análise históricas.

22- Limite de validade de transações

Este controle permite a comparação da data atual com data de validade da transação para efeitos de análise dos dados ou de sua expiração.

23- Verificação de perfuração (Cartões) ou de digitações (Terminais e Disquetes).

Pela reentrada da informação (no cartão é feita a comparação das perfurações), esta pode ser verificada contra a gravação original e estabelecer a exatidão ou não da operação de entrada do dado.

24- Aprovação em documentos

Significa que para os casos relacionados, a informação iniciada está de acordo com as normas da empresa. Poderá existir mais de uma aprovação para o mesmo documento.

25- Totais de controle entre processamentos

Grande parte do processamento de um sistema estabelece que os resultados de um *Job* sejam entrada para um *Job* seguinte. Este controle define a criação de totais intermediários que possibilitem a verificação de que o processamento foi feito corretamente. Ex.: Saldo de duplicatas a receber anterior (+) novas duplicatas (-) pagamentos = novo saldo de duplicatas a receber.

26- Balanceamento entre arquivos, detalhe e resumo

Neste controle, efetua-se a comparação dentre os valores apresentados pelo arquivo de detalhe e o de resumo para verificação da igualdade de totais.

Exemplo: O total monetário apresentado pela conta de Materiais está diferente do apresentado pelo arquivo de Materiais em Estoque (controle).

27- Reconciliação entre arquivos

É a identificação de divergências entre dois arquivos de mesma natureza ou entre resumo e detalhe para a correção de erros resultantes de defasagem entre o processamento dos dois conjuntos de dados.

28- "Aging"

Este tipo de controle tem sido mais associado a sistemas de Contas a Receber. Trata-se da classificação dos dados de um arquivo segundo certas Duplicatas de tempo (30, 60, 90 dias). No entanto, pode ser aplicado a qualquer caso que se queira detectar a existência de transações fora (ou dentro) de um período qualquer de tempo.

29- Arquivos aguardando complementação

Refere-se às Transações que não foram processadas em várias oportunidades e que ficam retidas neste tipo de arquivo para posterior correção e processamento.

30- Comparação entre informações

Nos casos em que diferentes sistemas utilizam a mesma informação, devido às características de cada um, várias situações de desigualdade poderão surgir entre os resultados de um e de outro. Este controle visa a identificação das desigualdades a fim de estabelecer qual dos sistemas omite qual informação.

31- Arquivo de Controle

Geralmente manual, este controle visa à formação de um arquivo (*tickler file*) ou seqüência cronológica com objetivos de *follow up* sobre determinado assunto.

32- Processamento em duplicatas

Pressupõe re-execução de uma atividade sem, no entanto, atingir todos os graus de detalhe mas, apenas cálculos mais importantes para confirmação de validade do processamento original.

33- Identificação (*Label*)

Significa a identificação interna ou externa de um lote de transações ou arquivo, em relação a datas, fontes, sistema a que pertence, companhia , etc.. É aplicável a arquivos em meios magnéticos.

34- *Trailer record*

É a criação de um registro que contem totais de controle que serão comparados com os totais obtidos durante o processamento.

Controle Corretivo

1- Relatórios de Exceção

São relatórios que indicam as transações que não atendem aos requisitos do sistema ou que contrariaram um ou mais controles detectivos e, portanto, requerem investigação adicional.

2- Detalhe das transações /Trilha de Transações / *Audit Trail*

É um dos controles mais importantes em sistemas computadorizados. Refere-se ao estabelecimento de relatórios que indicam claramente a evolução das transações (para frente e para trás), relativas a um item do sistema.

3- Análise de erros

Este controle tem como objetivo identificar para, um dado tipo de transação do sistema, o volume de erros ocorrido em certo intervalo de tempo. Visa conduzir à conclusão sobre as medidas necessárias para a redução do volume de erros.

4- Sugestão automática para correção de erros

Ao detectar alguma transação que viola algum controle detectivo, é emitida automaticamente uma informação solicitando a correção do erro.

5- “Re-submissão” de correções

Os dados errados rejeitados pelo Sistema, após correção, são submetidos novamente e sofrem outras verificações, além daquelas impostas às transações normais. Isto, obviamente, só deve ser aplicado em tipos de transações cuja manipulação da correção de um caso poderá dar margem a ações ilegais.

6- Plano de Emergência e Recuperação (PER)

Este tipo de controle corretivo destina-se aos casos de ameaças de paralisação da instalação. Situará como o único meio para a recuperação dos arquivos mestres e de transações dos sistemas de informação da empresa (ver capítulo especial, no final deste trabalho).

VII - O SISTEMA DE INFORMAÇÃO QUE UTILIZA TÉCNICAS AVANÇADAS

- Teleprocessamento
- Banco de Dados

Temos, aqui, uma variação bastante importante na forma de transmissão e tratamento dos dados de um Sistema de Informação.

Muito embora, grande parte dos autores de Auditoria e Segurança em Processamento de Dados isolem estes tipos de sistemas e os classifiquem como avançados, achamos que esta postura deve iniciar uma rápida alteração e o termo “avançado” possa, talvez, ser substituído por “de alto risco” ou “com alta possibilidade de conter ameaças à organização”.

Por outro lado, a aplicação das técnicas de Teleprocessamento e de Bancos de Dados vem crescendo em proporção bastante grande, em função das facilidades oferecidas pelos equipamentos, pelos serviços de Telecomunicação e pelos produtores de *Software*.

Assim, o seu uso, já não está mais associado às características de grande organização, grandes equipamentos, sistemas sofisticados ou alto custo de operação.

Por outro lado, a par da crescente vantagem de sua aplicação, as técnicas, aqui citadas, tornam, cada vez menos “visível”, para a Administração da Instalação os detalhes de cada uma das operações do sistema, as quais são quase que totalmente explícitas e controláveis nos sistemas que utilizam a forma de “*Batch*” simples.

Assim, podemos classificar estes tipos de sistema, segundo o grau de utilização destas técnicas, em:

- Transações em *Batch* remotos
  - *RJE* (*Remote Job Entry*)
  - Consulta
  - Atualização
  - Programação
  - Arquivos reunidos em Banco de Dados
- } tempo real

Nos quadros seguintes exemplificamos a forma geral de cada um.

Figura 4 - Ciclo de processamento da informação no sistema on-line

Figura 5 – Batch Remoto

Figura 6 – Consulta em tempo real

Figura 7 – Atualização em tempo real

Figura 8 – Programação em tempo real

**EXEMPLO DO CONCEITO BÁSICO DE
UM BANCO DE DADOS NA ÁREA INDUSTRIAL**

Figura 9 – Exemplo do conceito básico de um banco de dados na área industrial

CAUSAS DE AMEAÇAS

Como já vimos no capítulo que descreve os elementos de uma Instalação, os Sistemas que utilizam técnicas avançadas diferenciam-se dos sistemas em “*batch*”, pela maior abertura a problemas de segurança, em virtude dos componentes adicionais que incorporam.

Tendo em vista que os conteúdos dos sistemas são idênticos, chamamos a atenção do leitor para o fato de que as causas de ameaças, já indicadas para o Elemento, continuam a existir para este caso.

No entanto, causas adicionais são identificadas conforme a categoria utilizada. Assim, passamos a destacar, em seguida, apenas estas causas adicionais, por categoria.

1- Transações em *Batch* Remoto (Transmissão de lotes de transações apenas com retorno de inconsistência e dados aceitos também na forma de lotes, em períodos predeterminados).

1.1 - Perda parcial ou total de transações, possível de ocorrer durante a transmissão. Interferência nas linhas de telecomunicação provocam alteração nos dados.

2- RJE (*Remote Job Entry*)

Nesta modalidade, temos como resultante o que é chamado de “*open shop*”, quer dizer, grande possibilidade de acesso a dados, arquivos e equipamentos. Isto porque, nesta forma usam-se os terminais remotos (Leitoras, impressora e vídeo de controle) para a execução não apenas do processamento de transações, mas também, submissão de programas para compilação, alterações, depurações, etc.. Assim sendo, a exposição da instalação (de todos os elementos) é bastante grande e permite a prática de atos não autorizados como fraude, roubo de informações ou desvio de recursos. Também, aqui, podem ocorrer os mesmos problemas do “*batch* remoto”.

3- Consulta em Tempo Real

A característica principal nesta forma é a execução tão somente de consulta a arquivos situados no computador central. É o tipo de aplicação mais simples da forma “*Real Time*”. A possibilidade de consulta a esses arquivos, embora controlada, permite a execução de ações e penetração não autorizada e a obtenção de informações sobre este ou aquele sistema da empresa. Resumindo, podemos ter as seguintes causas de ameaças:

3.1- Invasão de Privacidade

3.2- Consulta a informações não atualizadas: em certas situações, a informação contida nos arquivos pode não estar atualizada como se supunha e o seu uso poderá gerar distorções nas ações dos usuários.

3.3- Informação consultada incorreta: por erro no programa de consulta o usuário poderá estar recebendo informação distorcida.

3.4- Distorções na transmissão de dados.

4- Atualização em Tempo Real

Como forma mais sofisticada que os anteriores, esta envolve operações de atualização em arquivos mestres e de transações com correção imediata de erros. Tendo em vista a amplitude de operações permitida nesta modalidade, as causas de ameaças possíveis são as mesmas de um Sistema de Informação tradicional com os seguintes agravantes:

4.1 - Acesso ilimitado

Semelhante ao da forma Consulta em Tempo Real com a diferença que transações inadequadas terão reflexo mais desastroso que a simples invasão de privacidade, uma vez que será possível, em tempo real, a modificação em arquivos e a correção de erros, por meio do que, uma ação desonesta, poderá ser praticada.

4.2- Falhas em equipamentos e *Software*

Poderão ocorrer enquanto uma operação estiver sendo executada. Ao reiniciar, poderão acontecer erros como duplicação de dados e perda da transação.

A ausência de relatório em que seja indicada a seqüência já executada também aumentará a chance de enganos.

4.3- Erros na entrada de dados

Podem ocorrer com os terminais da mesma maneira que nos sistemas em *batch*, isto é, omissão de dados, ausência de códigos, inversão de dados.

5- Programação em Tempo Real

Da mesma maneira que a forma de *RJE*, esta modalidade cria as condições de “*open shop*”. É como se tivéssemos o programador dentro da sala do Computador, executando suas atividades “diretamente” na máquina. Assim, todas as causas de ameaças às Operações do CPD, executando-se as referentes às Catástrofes, são passíveis de ocorrência nesta modalidade.

6- Arquivos reunidos em Banco de Dados

De certa maneira, todos os Sistemas, que usam técnicas avançadas de transmissão e processamento de dados, têm seus arquivos organizados dentro da técnica de Gerenciadores de Banco de Dados.

O Gerenciador é um *Software* específico que controla e estabelece as relações entre os subconjuntos que integram o Banco de Dados. Uma das características de um Banco de Dados é que a utilização de suas informações se faz pelo conhecimento da “chave” ou “chaves” que permitem percorrer cada um dos subconjuntos da rede e os seus registros pelo programa de aplicação.

Uma vez acessado pelo programa de aplicação, torna-se possível percorrer as cadeias internas do Banco e Dados e acessar dados que não os de interesse exclusivo daquele programa. Com isso, as seguintes causas de ameaças se destacam neste tipo de organização de dados:

6.1- Acesso ilimitado

Tendo em vista que os “controladores de biblioteca” praticamente não exercem controle sobre a forma de Banco de Dados, o acesso a uma “chave” na rede representa o acesso a toda a rede, ilimitadamente.

6.2- Perda de Arquivos

A organização de métodos de *backup* em Banco de Dados é mais difícil que na forma de arquivos independentes, será muito mais custosa e demorada na sua execução. Assim, falhas nos equipamentos ou nos programas de aplicação provocam perda de arquivos da rede com interrupção na operação do Sistema.

6.3- Baixo tempo de resposta

No funcionamento de um sistema de teleprocessamento, com Banco de Dados, o Sistema de informação tem que percorrer diversos arquivo da rede, para a seleção das informações que compõem determinada operação de processamento. Esta atividade consome tempo e também pode representar um ponto negativo na performance do sistema. Não quer dizer que a técnica de Banco de Dados causa desvantagens ao teleprocessamento, mas sim que sua adoção exige o planejamento cuidadoso quanto ao encadeamento dos diferentes grupos de dados para que a pesquisa, pelos programas de aplicação, seja a mais eficiente possível.

7- A Penetração nos Sistemas via Teleprocessamento

Citamos nas diversas causas de ameaças o termo penetração como ponto fundamental para a execução de ações desonestas.

Segundo R. D. Lackey (1), "Penetração é o ato de ganhar acesso não autorizado a dados, procedimentos ou recursos de máquina ... "A Penetração de um sistema pode conduzir a uma ou mais das seguintes ações não autorizadas:

- a) Observação - não altera os dados observados;
- b) Extração - os dados são copiados;
- c) Alteração - modificação nos dados, procedimentos ou equipamento (condições);
- d) Adição - inclusão de dados estranhos ao arquivo;
- e) Utilização - uso de equipamentos, *software* ou ambos.

Ainda, de acordo com R. D. Lackey, existem seis categorias de técnicas de penetração em sistema On-line, definidos pela análise de inúmeros casos de ações não autorizadas.

Tendo em vista a necessidade de estudo adicional para determinação dos termos em português que melhor se adaptem ao seu significado, preferimos denominar cada categoria com os termos originais, em inglês:

Browsing - é a pesquisa de resíduos de dados ou de áreas de armazenamento de dados para obtenção de informações. É também chamada de “*Waste basket threat*”. É feita, às vezes, com o intuito de conseguir penetração no sistema e, então, iniciar a busca. Às vezes, é usada para uma busca aleatória de *passwords* ou identificação de usuários.

Foible ou Trap door - é a facilitação acidental e não intencional que permite o acesso às informações ou o controle não autorizado do Computador. Pode ocorrer tanto com os equipamentos como o *Software*. Um caso comum seria a existência acidental de uma condição não prevista para a qual não é feito nenhum teste e que criará a condição de acesso.

Artifice (Trojan Horse) - é a introdução intencional de um código clandestino em um sistema, para ser usado em seguida em ações desonestas.

Pode ser introduzida na implantação do Sistema durante modificações posteriores. O “*Artifice*” pode estar contido em um programa Honesto, que desempenha as funções desejadas, mas que também executa, sem o conhecimento do usuário, operações não autorizadas.

Impersonation - é a ação desonesta conseguida quando o perpetrador faz-se por usuário autorizado ou faz seu terminal ser reconhecido como tal pelo sistema. Geralmente, esta ação é combinada com outra para a execução de ato ilegal. Exemplo: conseguir a identificação de um usuário por meio de “*browsing*” e então executar esta técnica.

Tapping - é o acesso a um Computador por meio da conexão direta de terminal, a uma linha de comunicação (ilegalmente) ou equipamento do próprio computador.

Radiation - é a obtenção de informações sem a conexão direta. Nesta forma, os dados são captados por sistema de detecção acústica ou de sinais eletromagnéticos, emanados pelo computador ou seus componentes. Estes sinais são captados em receptores, gravados e depois tratados para a obtenção de informações.

CONTROLES DE SEGURANÇA

Os objetivos dos Controles de Segurança, em relação a este elemento, são:

- Reduzir as possibilidades de penetração não autorizada nos sistemas de informação;
- Reduzir as falhas no processamento;
- Minimizar os riscos sofridos pela interrupção dos meios de transmissão.

Observação: De forma geral, os controles mencionados para os Sistemas de informação tradicionais, são, também, aplicáveis neste caso. Portanto, serão apresentados, em seguida, somente os controles adicionais relativos às formas avançadas.

Controles Preventivos

1- Código de passagem (*Password*)

Permite o controle do acesso ao sistema central. Sua formação pode variar, conforme o tipo de combinação e natureza da informação requerida.

Os *passwords*, quando transmitidos são analisados pelo sistema por meio de comparação com tabelas específicas, criadas com a finalidade de controlar o acesso aos dados.

Os *passwords* podem limitar o acesso a arquivos, limitar a operação a ser executada, as pessoas autorizadas e os terminais.

2- Segurança física dos terminais

Trata-se de dotar o local onde se situam os terminais de alguma forma de segurança que controle o acesso e impeça a utilização por pessoas não autorizadas. Além disso, os terminais possuem chaves de segurança para sua situação.

3- Tabelas de Autorização

Este controle utiliza-se de tabelas que referenciam quais as pessoas que podem fazer o que e em quais sistemas.

Exemplo: Em um sistema de Vendas On-line, o vendedor pode apenas entrar com pedidos (código e quantidade).

Controles Detectivos

1- Protocolos de transmissão

Permitem a identificação do transmissor e da validade da mensagem.

Incluem, ainda, as seguintes informações:

- Identificação do terminal;
- Número seqüencial de controle;
- Número da mensagem;
- Dia e hora;
- Códigos de ação;
- Indicador de fim de mensagem.

2- Verificação da informação

Este controle pode ser executado via terminal de forma imediata, incluindo a verificação de formato, complementaridade e validação da informação transmitida.

3- Controle de acessos

Tem a finalidade de registrar todas as tentativas, bem e mal sucedidas de acesso ao sistema, por todos os terminais que compõem a rede. Estes registros devem ser processados posteriormente para a obtenção de relatórios que permitam identificar possíveis tentativas de penetração não autorizada.

4- Arquivo de usuários autorizados

Para ser utilizado pelos *passwords*.

5- *Read Back*

Após a introdução da transação ou consulta, esta deve ser consistida e, então, informada novamente ao usuário para confirmação do que foi recebido.

6- Verificação de Redundância

Em um controle executado pelo equipamento de controle de comunicações integrante da configuração.

Serve para detectar distorções nos dados durante a transmissão. No entanto, seu emprego depende da existência desta capacidade no equipamento fornecida pelo fabricante.

7- Controle de Linha

Este controle pode tanto ser executado por equipamento ou por um *software* específico. Sua função é implementar os procedimentos de Protocolo de linha, produzir controles de acesso, executar verificação de redundância e outras possibilidades de controle de segurança.

Controles Corretivos

1- Rotação nos controles de acessos

Tendo em vista que os controles de acesso, com o passar do tempo, podem ser conhecidos por outras pessoas, que não as autorizadas, é importante promover sua constante revisão, ampliação ou substituição. Isto é válido não só para terminais, como também, para arquivos de autorização, fechaduras especiais, cartões de identificação , etc..

2- Arquivo paralelo de registro de transação

O risco de perda ou deterioração da situação de um Banco de Dados está sempre presente em sistemas on-line. Portanto, é altamente recomendável a manutenção paralela de um arquivo detalhado de todas as transações ocorridas. Este arquivo será utilizado para os procedimentos de recuperação da rede, em caso de interrupção.

3- Auto-treinamento on-line

Permite que o usuário, em caso de dúvida quanto à seqüência de operações no terminal, possa ser instruído no mesmo instante sobre os procedimentos a seguir para efetuar a contento a operação.

VIII - O PROCESSO DE DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO (PDSI)

Este é outro elemento presente em uma Instalação que, tanto quanto os demais, desempenha parte importante na eficácia de suas atividades.

Em termos formais, o PDSI representa o conjunto de “*standards*” ou princípios que a Instalação adota para o desenvolvimento de seus projetos de Sistemas de Informação.

Em relação ao seu conteúdo, o PDSI é expresso em forma de manuais que explicam em detalhes aos técnicos da Instalação, o “como” e o “porquê” cada atividade deve ser desenvolvida, desde a solicitação inicial do usuário, até a sua implantação em caráter definitivo.

Existe uma correlação bastante forte entre o PDSI adotado por uma Instalação e os Sistemas de Informação ali implementados. Em outras palavras, um PDSI não muito bem estruturado contribui à instalação e traz, em si, pontos que geram causas de ameaça à Organização.

Uma vez que não é o objetivo deste trabalho discorrer sobre as diversas metodologias de desenvolvimento de sistemas praticados atualmente, mostramos nos quadros seguintes, um exemplo de um PDSI clássico, e as suas fases intermediárias.

Quadro 1 – Fases clássicas de um projeto de sistemas

Quadro 2 – Definição dos objetivos - análise de viabilidade

Quadro 3 – Desenho básico do sistema

Quadro 4 – Desenho detalhado do sistema

Quadro 5 – Implantação

Como decorrência de sua aplicação, um PDSI gera não só o elemento chamado “O Sistema de Informação via Computador”, como também documenta o que foi executado durante o processo de desenvolvimento e como o Sistema Implantado deve agir.

Assim, a documentação de um Sistema representa condição fundamental para a avaliação do sinal de segurança destes dois elementos.

CAUSAS DE AMEAÇAS

1- Falta de Análise de Viabilidade ou Análise de Viabilidade Incompleta - esta causa ocorre quando a fase de análise inicial não expressa todos os pontos abordados pelo sistema e a qualidade dos dados levantados não permite uma avaliação completa dos recursos requeridos pelo projeto e os benefícios tangíveis e intangíveis que serão obtidos. Como resultado, uma decisão enganosa poderá ser tomada em prejuízo da empresa, por exemplo:

- Não executar um projeto devido a seu “alto custo” e sofrer futuramente as consequências de não ter informações para enfrentar as mudanças da competição.
- Executar o projeto, arcar com seus custos e verificar, posteriormente, que existiriam alternativas mais simples e baratas.

2- O PDSI não fixa claramente a necessidade e os pontos de participação dos usuários

Este tipo de problema geralmente vai de encontro a uma situação já latente nas organizações, que é a da total abdicação da alta Administração em relação à função de Planejamento e Desenvolvimento de Sistemas. A razão apresentada de que o trabalho de Sistemas é “técnico”, e por isso deve ser deixado aos profissionais da área, traz em si uma grande abertura para que se reduza a participação dos usuários em um nível de insuficiência.

3- Desenho do Sistema apresenta especificações inadequadas

Às especificações de um Sistema devem influir sempre da junção do trabalho dos usuários e do analista. As especificações inadequadas são aquelas que estão além ou aquém do necessário ou quando não são apropriadas ao sistema. Assim sendo, poderá acarretar o desenvolvimento de Sistemas de Informação com as falhas já adotadas.

4- Falhas no desenho do Sistema

Ocorrem mesmo quando existe correta especificação, pois são decorrentes das possibilidades de falha humana a interpretação das especificações.

5- Incompetência da equipe de projetos (pessoal de Sistemas e usuários)

A qualificação das pessoas que fazem parte da equipe é fator fundamental na qualidade da concepção do Sistema. Quando este requisito não é preenchido, o resultado será um Sistema com pontos vulneráveis, inadequados aos objetivos de sua criação e de difícil operação.

6- PDSI demasiadamente livre, permitindo soluções auto-gratificantes -

O desenvolvimento de um sistema é uma atividade técnica dirigida a objetivos precisos. Em casos como este, por ausência de controles de desenvolvimento, o técnico de sistemas pode tender a adotar soluções “geniais” que lhe causem auto-satisfação, mas que poderão causar também a inoperabilidade do Sistema,

Também o emprego de soluções tipo “estado de arte” poderá conduzir em certos casos, ao mesmo resultado. Antes de tudo, os usuários participantes do sistema são os que conviverão com ele no dia-a-dia. Portanto, o sistema deve estar adequado, acima de tudo, às necessidades e possibilidade operacional do ambiente, onde atuará.

7- Problemas de comunicação entre os técnicos de sistemas e usuários

No desenvolvimento de um projeto, a transparência das informações intercambiadas pelos técnicos e os usuários é fundamental para o desenvolvimento de sistemas adequados. Mal-entendidos ou definições incompletas causam erros fundamentais no desenho e também na operação do sistema.

8- O PDSI não obriga revisões periódicas entre fases

Em um projeto de sistemas, a finalização de uma fase não significa a garantia automática de que a fase seguinte deva ser executada sem alterações. A não execução de uma revisão ao término de cada fase leva à não consideração das prováveis mudanças organizacionais das necessidades dos usuários e dos custos do projeto.

9- Preparação para futuras Ações Desonestas

O desenvolvimento de um projeto é um dos pontos que apresentam maior abertura à perpetração de ações desonestas. Os detalhes de um sistema são passíveis de manipulação, não só pelo analista, mas, principalmente pelos programadores; no período do desenvolvimento dos programas.

A inclusão de desvios na lógica do programa permite a passagem de transações indevidas, no processamento de sistema, que encubram fraudes ou gerem transferência ilegal de recursos da empresa.

10- Sistemas Inflexíveis

São aqueles que não têm condições de acompanhar as mudanças nas necessidades da empresa, quer por razões técnicas ou econômicas. Sistemas com estas características chegam a impedir o desenvolvimento normal das áreas afetadas e são, por si só, uma causa de ameaça.

CONTROLES DE SEGURANÇA

Os objetivos dos Controles de Segurança em relação a este elemento são:

- Assegurar a existência de meios de comunicação que permitam o conhecimento da situação do projeto a qualquer tempo.
- Permitir o desenvolvimento de sistemas de informação adequados, no tempo designado e dentro dos recursos alocados.
- Identificar em tempo os problemas existentes em cada fase de desenvolvimento para a execução de prováveis mudanças.
- Assegurar a efetiva participação dos usuários não só no planejamento de Sistemas como no desenvolvimento de cada projeto.

Controles Preventivos

1. Adoção de um PDSI adequado

A definição de qual a metodologia de desenvolvimento de sistemas a ser adotada na empresa é uma das tarefas que exigem mais cuidado por parte do Administrador de Sistemas. Esta decisão significa, na realidade, a implantação do primeiro e mais importante controle sobre as atividades de desenvolvimento de sistemas.

A metodologia, como controle preventivo, deve ser selecionada com base nos seguintes critérios:

- Porte da empresa e tamanho da Instalação de Sistemas e Processamento de Dados.
- Detalhe das atividades de cada fase. Metodologias demasiadamente rebuscadas tendem a gerar desinteresse por parte do pessoal técnico e usuários.
- Utilização da metodologia por outras empresas, com razoável índice de satisfação.
- Qualidade da documentação gerada por cada fase combinada com objetividade e facilidade de execução.

- Versatilidade para adaptações às características da empresa e incorporação de técnicas avançadas de processamento de dados.

2- Gerenciamento de Projetos

Este controle é, na realidade, uma necessidade indiscutível para o desenvolvimento de uma Instalação dentro de padrões de profissionalismo e adequação às expectativas da empresa.

Destacam-se aqui os seguintes aspectos mais importantes:

- Planejamento de Projetos - Como ponto fundamental temos a execução do Plano Diretor de Sistemas, no qual estejam destacadas as prioridades da empresa como: resultado da discussão e da participação dos usuários, desde o mais alto nível hierárquico da empresa até o nível de Gerência Operacional.

Dentro do âmbito do Planejamento de Projetos, os seguintes aspectos que agirão como controles preventivos devem existir:

- a) Normas para definição e seleção de projetos.
- b) Divisão de tarefas em fases claras e homogêneas.
- c) Definição de datas de início e término de cada fase.
- d) Existência de Planos que definam as atividades para definição do Sistema, subsistemas e cada detalhe respectivo.

3- Controle de Projetos

Estas atividades devem estar previstas dentro do PDSI e referem-se a:

- Planejamento de curto prazo: englobando partes menores do sistema e detalhando-se até o menor nível possível (tarefas).
- Definição da responsabilidade pela execução das tarefas constando, não apenas o pessoal técnico, mas também os usuários.
- Relatórios de avaliação da situação de cada tarefa.
- Avaliação da situação do Projeto como um todo.

- Reporte das horas alocadas por analistas e programadores referentes a cada sistema, subsistema, tarefa ou programa.

4- Seleção e treinamento de pessoal técnico

Este controle prevê a existência de políticas claramente definidas para guiar a seleção e recrutamento de analistas, programadores e outros técnicos.

Estas políticas devem basear-se em adequadas descrições de cargos, tabelas, salários, planejamento de carreira e critérios de treinamento.

5- *Checklists* de fim de fase

O PDSI deve conter em seu detalhamento completa relação de itens que devem ser cumpridos até o final de cada fase para que sejam evitados o esquecimento ou a omissão proposital de qualquer atividade.

6- Documentação

Tendo em vista que a única forma de se conhecer um sistema de Informação e seus detalhes é pela correspondente documentação, reputamos como totalmente indispensável a sua definição clara dentro do PDSI.

A ausência de documentação adequada pode acarretar na perda total do controle sobre a operação de um CPD. Com o controle preventivo permite a constatação de avaliação econômica incompleta ou especificações inadequadas. Além disso, reduz a possibilidade de tentativas de fraude.

Controles Detectivos

1- Revisões e aprovações técnicas

O PDSI deve prever a execução de revisões e aprovações para cada etapa de desenvolvimento do projeto.

Estas revisões devem ser executadas formalmente (com assinaturas de envolvidos) e documentados por meio de atas de reunião.

Assim, o trabalho apresentado pelos analistas e programadores deverá ser revisto e aprovado pelos respectivos supervisores e, posteriormente, pelo Gerente de Sistemas.

2- Revisões e aprovações pela Alta Administração e Usuários

Da mesma maneira que no item (1), ao final de cada etapa, os supervisores e Gerentes das áreas usuárias deverão aprovar os resultados alcançados. As aprovações pela Alta Administração significam que os resultados obtidos pela equipe de projetos (técnicos e usuários) estão de acordo com os objetivos pré-definidos.

3- Participação da Auditoria no desenvolvimento do Projeto

Muito embora haja certa resistência por parte dos auditores na sua participação em projetos de sistemas, esta presença é de uma importância e de forma alguma chega a comprometer o princípio da “independência do auditor”. Este tipo de controle justifica-se pelos seguintes princípios:

- Os técnicos de sistemas são especialistas em desenvolvimento de projetos.
- Os usuários são especialistas na sua área de atuação.
- Os auditores são especialistas em controle interno.

Assim, a atividade que denominamos de auditoria preventiva representa um importante controle detectivo para o PDSI.

Pela sua participação, o Auditor verificará se o Sistema em criação possui os requisitos de controle mínimos aceitáveis e necessários a uma adequada performance.

4- Teste do Sistema

O teste do Sistema é uma das últimas atividades do projeto, antes da implantação definitiva. Sendo assim, representa importante papel como controle

detectivo, pois poderá levantar problemas que, se detectados, posteriormente, teriam uma chance de correção.

5- Revisão de pós-implantação

Esta atividade é executada algum tempo após a implantação do Sistema e traz, em si, grande parte dos problemas que o sistema já apresentou até este momento. Da análise conjunta por técnicos e usuários dos problemas surgidos resultará a identificação de causas de ameaças e as ações de correção nos Sistemas.

6- Documentação

Como controle detectivo, a Documentação de Sistemas age nos seguintes aspectos:

- Permite a revisão do projeto pela Administração, usuários, pessoal técnico e auditores, em cada uma de suas fases.
- Como decorrência, permite a localização de erros na concepção do sistema.

Controles Corretivos

1- Documentação

Aqui, a documentação de Sistemas representa o único controle corretivo possível, pois somente ela pode evidenciar a existência de erros no desenvolvimento do Projeto e, é por meio dela que as correções poderão ser feitas, e o Sistema poderá ser mantido.

IX - O PLANO DE EMERGÊNCIA E RECUPERAÇÃO (PER)

O ponto básico para a correção dos efeitos de um desastre em Processamento de Dados é a existência de um PER adequado e eficaz e que seja capaz de fazer frente a interrupções dos mais diversos tipos. Sem dúvida, o PER deve ser elaborado tendo em vista a sua eminente necessidade, algo que realmente será posto em prática, e não simplesmente como um “desencargo de consciência”. Para isso, deve ser fomentada na empresa a mentalidade de segurança em PD como base elementar para o sucesso do PER.

Características Desejáveis de um “PER”

Formalização: Não há dúvida que podemos encontrar em nossas empresas uma série de medidas de emergência, geralmente divulgadas por circulares, procedimentos isolados e mesmo instruções verbais, provenientes de diferentes setores e, que principalmente, a oficialização destes procedimentos, por meio de um Manual de PER, composto e divulgado por “todos” os setores envolvidos, além do CPD.

Modularidade: Se verificarmos que existem várias fontes de geração de desastre (interrupção), sabemos que nosso plano será mais eficiente se cobrir os diversos tipos de desastre possibilitando uma ação corretiva por níveis de prioridade e levando em consideração que nem todos os elementos de uma instalação detêm o mesmo grau de risco.

Por outro lado, as aplicações em produção normal no CPD não têm todas a mesma prioridade. Isto é, algumas poderão ser reiniciadas após certo tempo.

O PER Deve Ser Exercitado

Como condição básica para nos certificarmos de sua eficiência, devemos testar o PER, em todos os aspectos possíveis de serem simulados. Isto deve ser encarado como um dos pontos essenciais à consecução de um Plano que realmente funcione. Embora, não possa ser rigidamente determinado, aconselha-se que este teste deva ser, mesmo que parcialmente, executado pelo menos uma vez ao ano. Como decorrência dos resultados obtidos, relatórios de análise serão feitos, com vistas aos ajustes e modificações.

Quadro 6 – Passos para a elaboração de um plano de emergência e recuperação

PASSOS PARA A ELABORAÇÃO DE UM PLANO DE EMERGÊNCIA E RECUPERAÇÃO

**ESTABELECIMENTO DO
COMITÉ DE RECUPERAÇÃO**

1

**FIXAÇÃO DAS PRIORIDADES DE
RECUPERAÇÃO PARA AS
APLICAÇÕES**

2

**LEVANTAMENTO E SELEÇÃO DE
LOCAIS ALTERNATIVOS PARA
UTILIZAÇÃO DE COMPUTADOR**

3

**LEVANTAMENTO E SELEÇÃO DE
LOCAL EXTERNO PARA
GUARDA DE BACK UP DE
DOCUMENTAÇÃO E DADOS**

4

**FIXAÇÃO DOS PROCEDIMENTOS
DE EMERGÊNCIA E
RECUPERAÇÃO**

5

**DETERMINAÇÃO DAS
INFORMAÇÕES NECESSÁRIAS
PARA RECUPERAÇÃO DE
EQUIPAMENTOS, SERVIÇOS,
FORMULÁRIOS MÓVEIS E
ACESSÓRIOS**

6

**CRIAÇÃO, DISTRIBUIÇÃO E
MANUTENÇÃO DO “MANUAL DE
EMERGÊNCIA E
RECUPERAÇÃO”**

7

TESTE DO PER

8

Passos Para a Elaboração de um Plano de Emergência e Recuperação

Os passos acima agrupam os principais conjuntos de atividades imprescindíveis à obtenção de um PER adequado.

O Conteúdo do Plano de Emergência e Recuperação

O detalhamento apresentado, a seguir, não pretende exaurir o assunto, mas apresentar o conjunto mínimo de aspectos a serem coberto pelo PER. Cada organização deve analisar profundamente suas peculiaridades tais como:

- Tipo de *Hardware* empregado - *Standard* ou *O&M*.
- Modelo de operação - *Batch*, T.P., Centralizado.
- Características das Aplicações.
- Instalações e porte do investimento.
- Organização.

E montar o Plano tendo em vista o conjunto de riscos de desastre e respectivas medidas de recuperação.

Assim, o Manual do PER deverá conter no mínimo as seguintes seções:

- Introdução
- Atualização e Distribuição do Manual
- Formação do Comitê e Responsabilidades
- Locais de *Backup*
- Locais de Segurança Externos
- Listas de Telefones de Emergência
- Prioridades de Processamento para Recuperação
- Relação de Equipamento de Processamento de Dados
- Suprimentos e Fornecedores

- Representantes de Serviço
- Biblioteca e Fitas e/ou Discos
- Móveis, utensílios e *Layout* físico

Conteúdo de Cada Seção do PER

1- Introdução:

Descreve os objetivos e ação do Manual. Deverá conter alusão ao fato de que o Manual é propriedade da Companhia e que se o indivíduo que o detém desligar-se da mesma, esta cópia deverá ser encaminhada ao superior imediato.

Esclarece ainda que as ações contidas no plano não devem impedir outras ações não previstas, mas que sejam imperiosas no momento de recuperação.

Estabelece que, no caso de desastre, cada membro do comitê será contatado, para ser informado quando e onde comparecer.

2- Atualização e Distribuição

Estabelece o responsável pela atualização e fixa o prazo mínimo para revisão, (ex.: a cada seis meses).

Relaciona o nome de todas as pessoas, cargo e local, que recebem cada cópia do manual. Obrigatoriamente, os seguintes setores devem ter cópias:

- Sala de Operações
- Departamento de Análise e Programação
- Local de Segurança Externo
- Diretor da área de SPD
- Presidente ou Diretor Geral

3- Formação do Comitê e Responsabilidades:

Contém os títulos (cargos) dos membros do comitê. Devem estar incluídas todas as áreas usuárias envolvidas. Exemplo da lista.

É neste capítulo que, para cada membro do comitê, serão estabelecidas suas responsabilidades e ações durante o desastre.

Exemplo de Fixação de Responsabilidade no Manual do PER

Supervisor de Contabilidade - Reporta-se ao Gerente de Contabilidade. Sua principal responsabilidade é informar e manter os registros relacionados a vendas, recebimentos e despesas por Centros de Custos.

Ações durante o Desastre:

- a) Verifica e apura os danos à área de Contabilidade, fisicamente e com referência ao Processamento de Dados.
- b) Relata ao Comitê de Desastre as condições encontradas.
- c) Coordena os funcionários da Contabilidade nos trabalhos de obtenção dos documentos necessários ao restabelecimento dos arquivos à condição normal.
- d) Mantém lista atualizada de nomes, telefones, endereços dos funcionários da Contabilidade
- e) Revê o “*schedule*” de cada sistema interrompido para determinar o status do último processamento. Determina o quanto será necessário processar para atingir o ponto em que ocorreu o desastre.

4- Backup para Equipamento:

Nesta seção, devem constar os locais previamente estabelecidos para execução de processamento em caso de desastre. Os dados devem ser detalhados na seguinte forma:

- Local e endereço
- Nome e telefone da pessoa responsável

- Descrição da configuração que pode ser utilizada
- Cópia de contrato ou entendimento entre as partes com relação ao uso do equipamento.

No caso de se ter mais de um local, o manual deve estabelecer a ordem de preferência para contato.

5- Locais de Segurança Externos

A finalidade deste tópico é indicar qual ou quais os locais que a empresa destinou para a guarda de documentos, fitas , etc.. Tendo em vista que estes locais estarão sempre situados a certa distância da área do CPD, deve existir procedimento indicando como estes documentos ou fitas podem ser acessados em caso de necessidade e como será processada sua atualização.

6- Lista de Telefones de Emergência

Nesta seção, devemos incluir o nome, título e telefone da residência ou para contato de cada uma das pessoas que devam ser chamadas em caso de desastre. Esta lista deve indicar a seqüência a ser obedecida para os contatos, indicando as alternativas de chamada quando a inicial não for conseguida. Cada membro do Comitê é responsável pela manutenção da lista telefônica de seus subordinados.

No caso da empresa ter ligações com outras organizações que seriam afetadas pela interrupção do CPD, os nomes, títulos e telefones destas pessoas devem figurar na lista.

7- Prioridades de Processamento para Recuperação:

Esta seção é a que estabelece as prioridades de processamento para as atividades de recuperação. Como regra geral, incluímos, aqui, pelo menos, todos os serviços em produção normal.

A fixação das prioridades deve ser formalmente feita com base nas decisões dos respectivos usuários e validada pelo Comitê.

8- Relação de Equipamentos de Processamento de Dados:

Devem estar listados, aqui, todos os equipamentos existentes na Instalação, detalhando o nome, modelo, número de série, fabricante, bem como qualquer outra informação que auxilie na procura de substituto, em caso de destruição.

9- Suprimentos e Fornecedores:

Em qualquer instalação, encontramos variada gama de itens fornecidos por distintas empresas, desde chaves elétricas a formulários, fitas , etc..

Esta seção deverá conter os detalhes de cada um dos itens necessários à continuidade das operações bem como o nome, telefone e endereço dos fornecedores, onde cada item possa ser obtido.

10- Representantes de Serviços

Incluímos, aqui, a relação dos respectivos nomes e telefones de cada um dos Fornecedores de *Hardware* que seriam contatados na eventualidade de um desastre. Recomenda-se que estas informações sejam obtidas formalmente junto a cada Fornecedor.

11- Biblioteca de Fitas e ou Discos:

Deve estar incluída nesta seção uma cópia do sistema que regulamenta a execução do *backup*, contendo as seguintes informações:

- Localização
- Responsáveis pela manutenção e execução do sistema
- Procedimentos para obtenção e utilização do *backup*

12- Móveis, Utensílios e *Layout* Físico:

Serão listados nesta seção todos os móveis e utensílios necessários, não somente os móveis e utensílios, mas toda e qualquer tubulação e/ou fiação referente à fonte de energia e linhas de comunicação acopladas ao sistema.

X - CONCLUSÃO

Durante os últimos anos, a aplicação dos meios eletrônicos de processamento de dados tem sido feita de maneira extensiva em todos os tipos de organização e obedecendo a uma pressão de fora para dentro. O computador nos nossos dias representou um impacto que ainda não foi absorvido adequadamente pelas organizações tanto por gerentes, analistas de sistemas e programadores, como por aqueles que justificam sua instalação, ou seja, os usuários. Este impacto não tem sido de todo absorvido não só pela grande desinformação existente a respeito das possibilidades do computador como meio de auxílio à administração dos recursos da empresa, como pela falta de um enfoque mais técnico, quanto à administração do próprio Centro de Processamento de Dados - CPD.

Este trabalho tem como objetivo primordial levantar alguns aspectos de sua importância na administração de um CPD e que aqui serão tratados sob o título "Segurança em Processamento de Dados". Não se pretende, o óbvio, desviar a atenção de outros componentes importantes do ambiente de Processamento e Dados, como o da Programação e o da Análise de Sistemas e nem desconsiderar que os equipamentos de processamento de dados são as peças fundamentais na operação de processar dados.

É também importante ressaltar que a otimização do funcionamento das máquinas de processamento (*hardware*), bem como a evolução dos sistemas operacionais dos programas de controle e monitorização dos utilitários, dos gerenciadores de banco de dados, monitores de teleprocessamento, (*software*) vêm ocorrendo de maneira bastante rápida mas, principalmente, no sentido de simplificar a utilização do equipamento e aumentar a sua produtividade dentro da seguinte relação:

Quadro 7 – Fatores de transformação no processamento de dados

Os elementos acima mencionados obviamente são conjugados em cada tipo ou categoria de computador de maneira diferente e formam a grande variedade de configurações de computador existentes nas empresas.

No entanto, a otimização constante conseguida pelos fabricantes de equipamentos e empresas produtoras de *software* não são, por si só, suficientes para manter o nível de confiabilidade e uma operação de Processamento de Dados.

Este é um fato comprovado, pois, o Computador como instrumento básico necessário ao desenvolvimento e operação de Sistemas de Informação, está inserido em um ambiente, onde outros elementos o completam, o influenciam e, com ele, formam o que chamamos de Instalação de Processamento de Dados.

Assim, o perfeito funcionamento de uma Instalação de Processamento de Dados estará sempre condicionado ao perfeito funcionamento dos elementos que a compõem.

No transcorrer deste trabalho, tivemos a intenção de demonstrar a importância de cada um e os aspectos mais importantes, como fatores influentes na avaliação do nível de Segurança de uma Instalação de Processamento de Dados.

XI - BIBLIOGRAFIA

1. Allen, Brandt R., "Computer Security" , Data Management, Fev. 1972, pp. 24-30.
2. Allen, Brandt R., " EDP Security" , Data Management, Jan. 1972, pp. 18-24.
3. Allen, Brandt R., "Danger Ahead. Safeguard Your Computer". Harvard Business Review, (Nov-Dez. 1968).
4. Ardrey, Robert, "The Territorial", NY, 1966.
5. Armer, Paul "Social Implications of the Computer Utility", "Computers and Communications - Toward a Computer Utility", Prentice-Hall, Englewood Cliffs, N. J., Mar. 1967.
6. Adams, Donald L., "Performance Measurement in EDP", EDPACS, Maio 1974, pp. 1-11.
7. Agajimian, A. H., "A Bibliography on System Performance Evaluation" Computer, November, 1975. Aso in ACM-Sigmetrics Performance Evaluation Review 5,1, Jan. 1976.
8. Anderson, Harold A., Jr., and Sargent, Robert G., "A Statistical Evaluation of the Schedules of an Experimental Interactive Computing System" in Freidberger W., Statistical Computer Performance Evaluation, New York, 1972, pp. 73-98.
9. Andrews, Wallace C., and Sontag, Lester J." Carreer Development - A New Approach to Performance Appraisal", AFIPS Conference Proceedings, 1974, Vol. 43, pp. 867-871.
- 10.Arinc Reseach Corp., Annapolis, MD Guidebook for Systems Analysis/ Cost-Effectiveness, National Technical Information Service, AD-688 154, Mar.1969.
- 11.Army Materiel Command, Washington, D.C., Engineering Design Handbook : System Analysis / Cost-Effectiveness, National Technical Information Service, AD-884 151, Abril 1971.
- 12.Arthur Young & Company, "Computer Auditing", A Special edition of the Arthur Young Journal.
- 13.Autrey, Vaughn, "Bench the Benchmarks", Data Management, Dez. 1975, Vol.13 , pp. 22-24.
- 14.Avots, Ivar, "Making Project Management Work" Datamation, Jan. 1973, Vol. 19, pp. 42-45.
- 15.Adams, Donald L., "Audit Review of Program Code - I" , EDPACS, Reston, Virginia: Automation Training Center, Ago.1975.

- 16.Adams, Donald L., "Library System Packages - Revisited", EDPACS, Reston, Virginia: Automation Training Center, Fev.1974.
- 17.Adams, Donald L., " Performance Measurement in EDP" , EDPACS, Reston, Virginia: Automation Training Center, Maio 1974.
- 18.Adams, Donald L., "Recovery from a Data Center Fire" , EDPACS, Reston, Virginia: Automation Training Center, Abril 1974.
- 19.Adams, Donald L., "A Survey of Library System Packages", EDPACS, Reston, Virginia: Automation Training Center, Jul.1973.
- 20.Adams, Donald L., " A Survey of Test Data Generators" , EDPACS, Reston, Virginia: Automation Training Center, Abril 1973.
- 21.Adams, Donald L., and Mullaeky, J. F., "A Survey of Audit Software" Journal of Accountancy, Set. 1972. pp. 39-66...
- 22.American Institute of Certified Public Accountants. Audit Guide: Audits of Service-Center-Produced Records. New York: The American Institute of Certified Public Accountants, 1974.
- 23.American Institute of Certified Public Accountants. Statements on Auditing Standards. New York: American Institute of Certified Public Accountants, 1973, 1974 e 1976.
- 24.American National Standards, Inc. Flowchart Symbols and Their Usage in Information Processing. American National Institute, Inc. 1971.
- 25.Anderson, Lane K.; Herdershot, Raymond A.; and Shoonmaker, Robert C. " Self-Checking Digit Concepts, " Journal of System Management, Cleveland, Ohio, Set 1974, pp. 36-42.
- 26.Arens, Alvin, and Loebbecke, James K., Auditing: an Integrated Approach, Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1976.
- 27.Arkins, Herbert. Handbook of Sampling for Auditing and Accounting, 2nd Edition, New York, New York: McGraw-Hill Book Co. 1974.
- 28.Automation Training Center, Index. EDPACS. Reston, Virginia: Automation Training Center, Dez.1975.
- 29.Baird, Linsay., "An Analytical Approach to Identifying Computer Vulnerability". Security Management, Washington D.C.; American Society for Industrial Security, Maio 1974 pp. 6-11
- 30.Bank Administration Institute. Auditing Bank EDP System. Chicago, Illinois: Bank Administration Institute, 1968.
- 31.Boutell, Wayne S. Computer-Oriented Business Systems, Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1968.
- 32.Brown, Foster. "Auditing Control and System Design." Journal of Systems Management. Cleveland Ohio, Abril, 1975. pp. 24-31.
- 33."Banks May Face Trouble with DP Disasters", Data Management, Maio 1971.

34. Bates, William S., "Security of Computer-Based Information Systems", Datamation, Maio 1970.
35. Bigelow, Robert P., "Opportunity Makes a Thief", INFOSYSTEMS, Dez. 1973, pp. 29 & 42.
36. "Bomb Threats and Personnel Safety", Industrial Security, (Março 1971).
37. Braithwaite, Tim, "Visiting Lecturer on Computer Security", at The American University, (27 Março 1972)
38. Baker, Laurence H., "Consider the Alternatives Before You Upgrade", Computer Decisions, Maio 1972; pp. 33-35.
39. Bard, Y. "Performance Criteria and Measurement for a Time Sharing System" IBM Systems Journal, Vol 10 nº 3, 1971, pp. 193-214.
40. Barnetson, Paul, Critical Path Planning, Auerbach Publishers, 1970.
41. Bates, Robert E., "Auditing the Advanced Computer Systems", Management Accounting. Jun. 1970, pp. 34-37.
42. Battaglia, Vincent J., "Cutting Computer Costs", Financial-Executive, Vol. 40 nº 8. pp. 26-30.
43. Bell, Thomas E., "Choose Your Tools to Check Your Computer". Computer Decisions, Nov. 1972; pp. 12-25.
44. Bell, Thomas E., "Managing Computer Performance with Control Limits", ACM Performance Evaluation
45. Bell, Thomas E.; Boehm, B. W., and Watson, R.A., "Framework and Initial Phases for Computer Performance Improvement", Proceeding of the 1972 Fall Joint Computer Conference, Vol. 41 Part 2; pp. 1141-1154.
46. Bell, Thomas E.; Boehm, B. W., and Watson, R.A., "How to Get Started on Performance Improvement", Computer Decisions, Mar. 1973, Vol, 5; pp. 30-34.
47. Benjamin, Robert I., Control of the Information System Development Cycle, New York; Wiley-Interscience, 1971.
48. Berliner, Thomas H., "Early to Bid - Evaluating Computer Procurement Proposals", Computer Decisions, Nov. 1975, Vol. 7 ; pp. 34-36.
49. Bieses, John, "Management by Objectives or Appraisals by results". Data Management, Abril 1970, pp.24-25.
50. Bookman, Philip G., et al. "Use Measurement Engineering for Better System Performance". Computer Decisions, Abril 1972, Vol. 4; pp.28-32.
51. Boydston, John, "Evaluation the Performance of Large Systems". Data Processing Magazine, Winter 1971, vol. 13; pp.57.
52. Boyse, John W., and Warn, David R., "A Straightforward Model for Performance Prediction", Computing Surveys, Jun. 1975; pp. 73-93.

53. Brandon, Dick H., and Gray, Max, Project Control Standards Brandon/System, Press, Inc., 1970.
54. Brandon, Dick H., et al., Data Processing Management, Macmillan Information, 1975.
55. Brooks, Frederick P., "The Mythical Man-Month". Datamation, Dez.1974; pp. 45-52.
56. Brooks, Frederick P., "The Mythical Man-Month, Essays on Software Engineering, Addison-Wesley Publishing Co., 1975.
57. Brotherton, Dale, E., and Harder, Donald C., " Computer Performance Measurement", Data Management Jan. 1975, vol. 13, pp. 12-15.
58. Brown, Harry L., "Auditing Computer Systems", Management-Accounting, Set. 1972, Vol. 56; pp. 23-26.
59. Brown, William F., and Mason, Richard P., "Overhauling the Computer Center", Journal of Systems Management, Mar. 1973; pp. 28-32.
60. Browne, J. C., "An Analysis of Measurement Procedures for Computer Systems" ACM Performance Evaluation Review, Jan. 1975; pp. 29-32.
61. Bunt, R., and Tsichritzis, D., "An Annotated Bibliografy for Operating Systems", Computing Review 13, 8 Ago. 1972; pp. 377-388.
62. Buoy, Dona, and Hue, " Job Accounting Data - A Resource for the Computer Auditor", The Internal Auditor, Vol. 32, nº 1, Jan/Fev., 1975; pp. 63-67.
63. Burdick, R.W., "Operations Plannig Techniques: Planning for Profit", Data Management, Set, 1970; pp. 50-54.
64. Burpo, Christopher, W., "Is the Post Audit Necessary", Data Management, December 1973, vol. 11; pp. 14-17.
65. Canning, Richard G. (editor) "Managing the Programming Effort", EDP Analyser, Jun. 1968, Vol. 6 nº6.
66. Canning, Richard G. (editor) " Using the Reward System", EDP Analyser, Set. 1969, vol. 7, nº9.
67. Canning, Richard G. (editor) " Get More Computer Efficiency", EDP Analyser, Mar. 1971, vol. 9 nº3.
68. Canning, Richard G. (editor) "Saving From Performance Monitoring", EDP Analyser, Set.1972, vol. 10, nº 9.
69. Canning, Richard G. (editor) "That Maintenance 'Iceberg", EDP Analyser, Out 1972, vol. 10, nº 10.
70. Canning, Richard G. (editor) "The Internal Auditor and The Computer", EDP Analyser, Mar., 1975, vol. 13, nº 3.
71. Canning, Richard G. (editor) "Are we Doing the Right Things?", EDP Analyser, Maio, 1975, vol. 13, nº 5 .

- 72.Canning, Richard G. (editor) "Are we Doing the Things Right?", EDP Analyser, Jun., 1975, vol. 13, nº 6 .
- 73.Canning, Richard G. (editor) "Do we Have the Right Resources?", EDP Analyser, Jul., 1975, vol. 13, nº 7 .
- 74.Canning, Richard G. (editor) "Computer Security: Backup and Recovery Methods", EDP Analyser, Jan., 1972, pp. 1-15 .
- 75.Canning, Richard G. "The Importance of EDP Audit and Control", EDP Analyser, Jun, 1977.
- 76.Canning, Richard G. "Data Encryption - Is it for you?", EDP Analyser, Dez, 1989 .
- 77.Canning, Richard G. "Computer Fraud and Embezzlement", EDP Analyser, Set, 1973.
- 78.Canning, Richard G. "The Security of Manager's Information", EDP Analyser, Jul, 1979.
- 79.Canning, Richard G. "Data Security in the CDB", EDP Analyser, Maio, 1970.
- 80.Churchill, Neil C., and Kempster, John and Uretsky, Myron, "Computer-Based Information System for Management : A Survey" National Association of Accountants, 1969.
- 81.Carlsen, Robert D., and Lewis, James A., "The Systems Analysis Workbook", Prentice - Hall, Inc., Englewood Cliffs, N. J. 1979.
- 82.Cadmus, Bradford Operational Auditing Handbook, New York, New York: The Institute of Internal Auditors, Inc., 1964.
- 83.Canadian Institute of Chartered Accountants. Computer Audit Guidelines, Toronto, Ontário, Canadá: Canadian Institute of Chartered Accountants, 1975.
- 84.Canadian Institute of Chartered Accountants, Computer Control Guidelines, Toronto, Ontário, Canadá: Canadian Institute of Chartered Accountants, 1971.
- 85.Carey, J. L. , and Doherty, W. O., "The Concept of Independence Review and Restatement". Journal of Accountancy, Jan., 1966.
- 86.Carter, Ciel. Guide to Reference Sources in the Computer Science, New York, New York: McMillan Publishing Co., Inc., 1973.
- 87.Chan, Stephen. "SEC Rules on Indendence". CPA Journal, Out, 1972, pp. 843-844.
- 88.Cochran, William G. Sampling Techniques - Secound Edition, New York, New York; John Wyley & Sons, Inc., 1963.
- 89.Crowley, Thomas H. Understanding Computers. New York, NY: McGraw Hill Book Company, 1967.
- 90.Carlson, Paul, "A Bank Protects its Memory" Banking, Abril, 1971.

- 91.Chu, Albert L.C., "Computer Security - The Corporate Achilles Heel", Business Automation, 1 Fev. 1971, pp. 33-38.
- 92.Communications News, July, 1972.
- 93.Computer Growth Calls for Security in Banks", Data Management, Set. 1970.
- 94.ComputerWorld (12 Jul., 19 Jul., 2 Ago., 30 Ago., 6 Set., 15 Nov., 6 Dez. 1972).
- 95.Cosby, H. Douglas, "Secrety vs. Confidentiality", Data Management, Jan., 1974, pp. 20 e 21.
- 96.Carey, Zane E., "A Control System for EDP Projects", The Interpreter Set, 1970; pp. 19-25.
- 97.Carlson, Gary, "Practical Economics of Computer Monitoring", Management Informatics, Dez. 1972; pp. 251-256.
- 98.Carter, D. M.; Gibson, H. L.; and Rademacher, R.A., "A Study of Critical Factors in Management Information Systems for U.S. Air Force", National Technical Information Services, Mar. 1975, AD. A009 647/9ST.
- 99.Chervany, Norman L., and Dickson, Gary W., "Economic Evaliation of Management Information Systems : "An Analystic Framework", Decision Sciences, 1970, Vol.1 ; pp.296-308.
- 100.Chester, K. W., "Computer Resource Allocation", Datamation, Set1974, Vol. 20; pp.107-110.
- 101.Clapp, J.A., and Sullivan, J.E., "Automated Monitoring of Software Quality" AFIPS Conference Proceedings, 1974, vol. 43.
- 102.Collier, Roger J., "Simulation of Computer Systems, An Introduction"Management Accounting, Maio 1973, vol. 54; pp. 45-47.
- 103.Comptroller General of The United States, "Acquisition and Use of Software Products for Automatic Processing Systems in the Federal Government" United States General Accounting Office Repot to the Congress, Jun. 30, 1971.
- 104.Cooke, John E., "Feasibility Studies For the Selection of Compute Systems and Applications", Cost and Management, Set-Out., 1970; pp. 11-19.
- 105.Cooke, Lawrence H. Jr., "Programming Time Vs. Running Time", Datamation, Dez. 1974, Vol. 20; pp; 56-58.
- 106.Corsiglia, Jack, "Matching Competitors to the Job - First Step Towards Selection", Data Processing Magazine, Dez. 1970, pp; 23-27.
- 107.Cunningham, Jan, "Establishing Internal Controls for a COM Operation" Information and Records Management, Jul., 1973, vol. 7; pp. 30-32.
- 108.Cushing, Barry E. D., Ial, David H., "Cost-Performance Trade-offs in Real Time Systems Design, "Management Advisor", Nov/Dez , 1973, Vol. 10; pp. 29-38.

- 109.The Data Communications User , “RBT Choise Rests on Price-Performance and Data Throughput”, Maio, 1975; pp. 53-55.
- 110.Department of the Army, Data Processing, Installation, Management, Procedures AR 18-7 , Set., 1966.
- 111.“Managing The Data Center”, Data Management, Out 1974 ; pp.20-25.
- 112.Dawson, G. A., “Monotoring Information Processing Systems”,ISDOS Working Paper 69, Department of Industrial and Operations Engeneering, University of Michigan, Fev.1973.
- 113.Dearde, John, and Nolan, Richard, L., “How to Control the Computer Resource”, Harvard Business Review, Nov.-Dez, 1973.
- 114.Deckard, Noble S., “Capturing the Development Cost of an Integrated MIS” Journal of Systems Management, Jan. 1970; pp. 14-17.
- 115.Defense Documentation Center, Alexandria, Virginia, Bibliografy - Volume I: Cost Effectivenesss Analysis, National Technical Information Service, AD-675 900, Ago. 1968.
- 116.Denelsky, Garland Y. Mckee, Michael G., “Prediction of Computer Programmer Training and Job Performance Using The AABP Test”, Personel Psychology, Primavera 1974; pp. 129-138.
- 117.Desiderio, Louis J.; Saloky, Dennis; and Wasserman, Arnold; Measuring Computer Performance For Improvements and Savings, New York: Cooper & Lybrand, 1974.
- 118.Demeis, W. M., and Weizer, N., “Measurement and Analysis of A Demand Paging Time-Sharing System”, Proceedings of the 24th ACM National Conference; 1969, pp. 229-245..
- 119.Diebold Group, Inc., “Computer Performance Appraisal - A Top Priority For Top Management” ADP Newsletter, 9 Dez. 1974.
- 120.Doherty, W. G., “Scheduling TSS/360 For Responsiveness” AFIPS Proceeding, Outono 1970; pp. 97-111.
- 121.Doll, Dixon R., “How To Evaluate Service Offerings of Varied Carriers”, Data Communications User, Nov.1974; pp. 16-18.
- 122.Donati, Frank R., “The Evaluation and Appraisal of Programmers Performance” Data Management, Out. 1971; pp. 42-43.
- 123.Dyba, J. E., “Criteria ... For Utilizing Data Management Resources”, Data Management, Maio 1974; Vol. 12.
- 124.Drucker, Peter, The Age of Discontinuity, Harper and Row,. Best Explanation of “Knowledge Economy”, NY, 1989.
- 125.Davis, Gordon B. “Auditing and EDP”, New York, NY: American Institute of Certified Public Accountants, 1968.

- 126.Ditri, Arnold E.; Shaw, John C.; and Atkins, William, "Managing The EDP Funcion", New York, NY: McGraw-Hill Book Company, 1971.
- 127.Ditri, Arnold E. and Wood, Donald R., "The End of the Beginning" TEMPO, New York, NY: Touche Ross & Co., 1969.
- 128.Dorricott, Keith O., "Appraising Computer-Assisted Audit Techniques." CA Magazine, Toronto, Ontario, Canadá: The Canadian Institute of Chartered Accountants, Ago. 1975; pp. 24-29.
- 129."Eletronic Security in the Computer Room", Banking, Maio 1970.
130. Ellul, Jacques, The Technological Society, NY, Prentice-Hall, paper ed.,. An overall critique of impact of technique ans technology upon society by a French Theologian, 1964.
- 131."Survey Results: Management Performance in Reporting" EDP Performance Review, Out, 1975.
- 132."Evaluating Performance in Computer Auditing" EDPACS, Fev 1975; pp. 1-7.
- 133.Emery, James. C., "Can We Develop Cost-Effective Information Systems?", Management Informatics, 1972, Vol. 1; pp. 243-249.
- 134.Emery, James C., "Costs and Benefits of Information Systems", Proceedings of IFIP Congress, 1974; pp. 967-971.
- 135.Esposito, J. E., "Statistical Analysis To Determine Digital Computer Worload Characteristics", National Technical Information Service, Jun.1974; AD-786 061/2SL.
- 136.Estes, Neil, "Step-by-Step Costing of Information System", Journal of Systems Management, Ago. 1969; pp. 31-35; Out. 1969; pp. 20-28.
- 137.Estrin, G., and Kleinrock, L., "Measures, Models, and Measurements For Time Shared Computer Utilities", Proceedings of the 1967 ACM National Conference, pp. 85-96, 1967.
- 138.Estrin, G., Muntz, R. R. , and Uzgalis, R. C., "Modeling, Measurement, and computer Power", AFIPS Proceedings SJCC, 1972; pp. 752-738.
- 139.FAIM Technical Products, Inc., EDP Review, Vol I Management; Vol II Systems and Operations 1973; atualizado em 1974.
- 140.Fiedelman, Lawrence A., "How Good is Your EDP?, Industrial Distribution Magazine, Maio 1975, Vol. 65; pp. 108-109.
- 141.Finney, John E. , "Costing In a Data Processing Department", Management Accounting, Out., 1974; pp. 29-35.
- 142.Fraser, Ronald, "Cost Control System in EDP", Cost and Management, Nov.-Dez., 1971; pp. 7-14.
- 143.Freiberger, Walter (editor), "Statistical Computer Performance Evaluation", Academic Press, New York, 1972.

163. Grochow, J. M., "Utility Functions For Time Sharing Systems Performance Evaluation", Computer, Set-Out. 1972; pp. 16-19.
164. Gruenberger, Fred (editor), Effective Efficient Computing, Prentice-Hall, Inc., 1973.
165. Gellman, Harvey S., "Using the Computer to Steal", Computers and Automation, April 1971.
166. Gillen, Vincent, "What do you know about your employees?" The Office, Ago, 1973; pp. 58-62.
167. Ginsburg, Harold, "Electronic Security at Work". The Office, Ago, 1973, pp. 53-56.
168. Girsdanský, M. B. , "Cryptography, The Computer, and Data Privacy", Computers and Automation, April, 1972.
169. Goode, George E. , "Security for Teleprinters and Data Communications", Data Management, Jan., 1973; pp. 21-26.
170. Graham, Robert M., "Protection in an Information Processing Utility", CACM, Vol. 11 nº 5, Mar., 1968.
171. Harper, William L., Data Processing Documentation: Standards, Procedures and Applications, Prentice-Hall, Inc. Englewood Cliffs, N. J., Oct, 1975.
172. Hansen, J. Burke, On The Trail of Effective DP Audits, ComputerWorld, Set, 17, 1979.
173. Hammer, Carl Dr., Computer Security: Past, Present, Future, 1978.
174. Hagelbarger, David, And Frergerman, Saul, Instruction Manual for Cardiac, Bell Telephone Laboratories, 1968.
175. Horwitz, Geoffrey B., "Standards for Program and System Testing". "EDFACS, Reston, Virginia: Automation Training Center, Inc., Nov., 1975.
176. Hudes, Albert, "Behind The Scenes at Equity Funding", TEMPO, New York, NY: Touche Ross & Co., Vol. 19, nº 1, 1973; pp. 12-19.
177. Hamilton, Peter, Computer Security, Auerbach Publishers, Philadelphia, Pa., 1973.
178. Hammer, Carl, "Electronic Data Systems Security", Contributed Paper, ADP Secure Data Sharing Conference Washington D.C., 27 Set. 72.
179. Hawkins, David H., "How Safe is Your Software", Computer Decisions, Jun. 1972; pp. 18-20.
180. Hedin, Robert, "Space Age Security", Industrial Security, Jun. 1971.
181. Hew Secretary's Advisory committee on ADP Systems, Records, Computers and the Rights of Citizens, , GPO, Washington D.C, Jul. 1973.
182. Hirschfield, Richard A. , "Security in On-line Systems - A Primer for Management", Computers and Automation, Set 1971, pp. 15-18.

- 183.Hoffman, Lance J., "Computers and Privacy: A Survey", Computing Surveys, Vol. 1, n^o 2, Jun., 1969. Deals with Tecnology of 1969. Has an annotade Bibliography.
- 184."How Bad Guys Thwart Computers", The Office, Set 1970.
- 185."How Security Does Pay Off", The Office, Set 1971.
- 186.Howes, Paul R., "EDP Security - Is Your Guard Up? Price Waterhouse Review, Primavera, 1971.
- 187.Hallam, Stephen F., "An Empirical Investigation of the Objetives and Constraints of Eletronic Data-Processing Departments", Academy of Management Journal, Mar. 1975, Vol. 18; pp. 55-62.
- 188.Hand, A. B., and River, W. L., "Constructing A Data Processing Cost Accounting System", Bank Administration, Abril 1974; pp. 34-44.
- 189.Hardy, I. T., Jr., "System Implementation and Evaluation", Journal of System Management, Dez., 1973, Vol. 24; pp. 24-27.
- 190.Harper, Donald C., "Measuring the Performance of the Compact Computer", Data Management, Nov. 1971, vol. 9, p. 30.
- 191.Harris, Richard D., "EDP Systems Audits", Data Management, Set, 1971, Vol. 9, p. 64.
- 192.Hart, Larry E., and Ipovich, George J., "Choosing a System Stethoscpo", Computer Decisions, Nov. 1971, Vol. 3, p. 20.
- 193.Hausmn, F.; Kistler, W. and Shultz, H. , "Modeling for Computer Center Planning", IBM System Journal, Vol. 10, n^o 4, 1971, pp. 305-324.
- 194.Haynes, R. J., "The Evaluation of Management Information Systems", In Conference on Man-Computer Interaction, IEE, England, 1970.
- 195.Hershman, Arlene, "New Programs For Computers", Duns, Maio, 1972, Vol. 99, pp. 53-55.
- 196.Highland, Harold J. (editor), Computer Performance Evaluation, Proceeding of the Meeting of Computer Performance Evaluation User Group (CPEUG) , National Technical Information Service, Set, 1974.
- 197.Hill, P. B., "The Control of Large-Scale Software Projects", IAG Journal, Dez., 1970; pp. 394-405.
- 198.Hirsch, Rudolf E., "Data Processing Can Be Cost Automated", Computers and Automation, Dez., 1971; pp. 8-15.
- 199.Hoffman, J. M., "Devide Gain - A Measure of System Component Simultaneous Operation", Proceedings of ACM Annual Conference, 1973; pp. 320-326.
- 200.Hollingworth, F. D., "Evaluating Computer System Projects", Canadian Charactered Accountant, Maio 1971, pp. 331-333.

- 201.Holmes, Fenwiche W., "Auditing From The DP Manager's Viewpoint", The Internal Auditor, Nov./Dec., 1975; pp. 29-34.
- 202.Holt, George A., And Stern, Henry C., "Cost-Benefit Evaluation of Interactive Transaction Processing Systems", AFIPS Conference Proceedings, 1975, Vol. 44, pp. 687-694.
- 203.Hopkins, Robert H., "It Pays to Evaluate Your Systems Department", Canadian Chartered Accountant, Fev.1975, Vol. 106; pp. 22-25.
- 204.Horwitz, Geoffrey B., "Standars for Program and System Testing", EDPACS, Nov. 1975, Vol. 3; pp. 1-6.
- 205.Howard, Philip C. (editor), "What Management Shoud Know About Performance", EDP Performace Review, Jan., 1974, vol. 2.
- 206.Howard, Philip C. (editor), "Predicting the Effects of Hardware Changes", EDP Performace Review, Fev., 1974, vol. 2.
- 207.Howard, Philip C. (editor), "More on Synthetic Benchmarks", EDP Performace Review, Maio, 1974, vol. 2.
- 208.Howard, Philip C. (editor), "Performance Evaluation Highlights From The NCC", EDP Performace Review, Jun., 1974, vol. 2.
- 209.Howard, Philip C. (editor), "Update On Hardware Monitors", EDP Performace Review, Out, 1974, vol. 2.
- 210.Howard, Philip C. (editor), "Cost Justifying Performance Evaluation Projects", EDP Performace Review, Jul., 1975, vol. 3.
- 211.Howard, Philip C. , "Monitors and Merriment", Computer Decisions, Set., 1975, pp. 40-42, 47.
- 212.Howard, Philip C. (editor), "Survey Results: Management Performance Reporting", EDP Performace Review, Out, 1975, vol. 3.
- 213.Howard, Philip C. (editor), "Third Annual Survey of Performance Related Software Packages", EDP Performace Review, Dez, 1975, vol. 3.
- 214.Howard, Philip C. (editor), "DP operational Cost Management", EDP Performace Review, Jan., 1976, vol. 4.