

Preparação de ambientes informatizados nas escolas públicas

para a mudança
Coleção **Informática** na Educação

Coleção **Informática** **para a mudança**
na Educação

Presidente da República Federativa do Brasil

FERNANDO HENRIQUE CARDOSO

Ministro da Educação

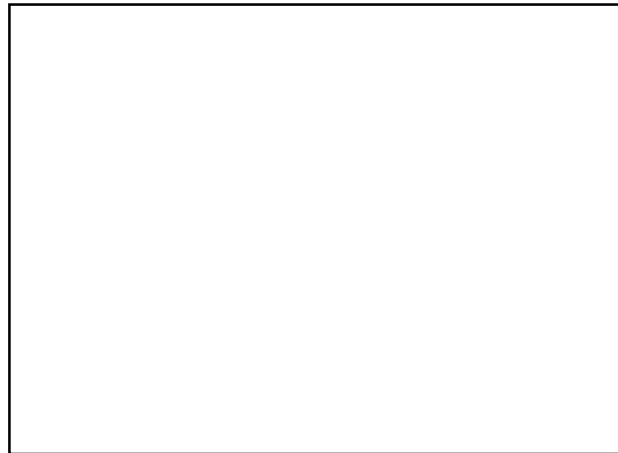
PAULO RENATO SOUZA

Secretário-Executivo

LUCIANO OLIVA PATRÍCIO

Secretário de Educação a Distância

PEDRO PAULO POPPOVIC



ORGANIZAÇÃO, PRODUÇÃO, ARTE



estapalavra@uol.com.br

Preparação de ambientes informatizados nas escolas públicas

EDUARDO MARTINS MORGADO

Professor Doutor e Chefe do Departamento
de Computação - DCo-Unesp-Bauru
Consultor técnico do Proinfo
Membro do Comitê Assessor
de Apoio ao Proinfo da SEED/MEC

MARCOS ANTONIO CAVENAGHI

Professor Doutor do Departamento de
Computação - DCo-Unesp - Bauru
Coordenador do Laboratório de Redes do LDC/DCo

NICOLAU REINHARD

Professor Doutor da Faculdade de Economia,
Administração e Contabilidade da Universidade de São Paulo
Membro do Comitê Assessor de Apoio ao Proinfo do SEED/MEC
Coordenador do Programa de Informática e Supervisor de
Projetos da FIA/FEA-USP (Fundação Instituto de
Administração/Faculdade de Economia, Administração e
Contabilidade da Universidade de São Paulo)

Informática para a mudança na Educação

A tarefa de melhorar nosso sistema educacional, dinâmico e complexo, exige atuação em múltiplas dimensões e decisões fundamentadas, seguras e criativas. De um lado, há melhorias institucionais, que atingem instalações físicas e recursos materiais e humanos, tornando as escolas e organizações educacionais mais adequadas para o desempenho dos papéis que lhes cabem. De outro, há melhorias nas condições de atendimento às novas gerações, traduzidas por adequação nos currículos e nos recursos para seu desenvolvimento, num nível tal que provoquem ganhos substanciais na aprendizagem dos estudantes. O MEC tem priorizado, ao formular políticas para a educação, aquelas que agregam às melhorias institucionais o incremento na qualidade da formação do aluno. Este é o caso do Programa Nacional de Informática na Educação – ProInfo.

O ProInfo é um grande esforço desenvolvido pelo MEC, por meio da Secretaria de Educação a Distância, em parceria com governos estaduais e municipais, destinado a introduzir as tecnologias de informática e telecomunicações – telemática – na escola pública. Este Programa representa um marco de acesso às modernas tecnologias: em sua primeira etapa, instalará 105 mil microcomputadores em escolas e Núcleos de Tecnologia Educacional – NTE, que são centros de excelência em capacitação de professores e técnicos, além de pontos de suporte técnico-pedagógico a escolas.

A formação de professores, particularmente em serviço e continuada, tem sido uma das maiores preocupações da Secretaria de Educação a Distância, em três de seus principais programas, o ProInfo, a TV Escola e o PROFORMAÇÃO.

Os produtos desta coleção destinam-se a ajudar os educadores a se apropriarem das novas tecnologias, tornando-os, assim, preparados para ajudarem aos estudantes a participar de transformações sociais que levem os seres humanos a uma vida de desenvolvimento auto-sustentável, fundada no uso ético dos avanços tecnológicos da humanidade.

Pedro Paulo Poppovic
Secretário de Educação a Distância

Sumário

9	Introdução
11	Propostas
13	Definições gerais e terminologia
13	O microcomputador
14	O hardware
16	O software
18	Conceitos gerais de redes de computadores
27	Preparação para receber os equipamentos
27	Sala informatizada
29	Rede elétrica
32	Cabeamento da rede local
37	A entrega dos equipamentos
	O papel dos NTEs
39	Assistência técnica
41	
	Informações e recomendações gerais
43	43 Dicas para a utilização dos equipamentos
	43 O que é um vírus de computador
	Alternativas para conexão com a Internet
51	51 A conexão
	52 Os provedores de serviço Internet – ISP– Internet Service Provider
	53 Alternativas para conexão da escola ao ISP

Introdução

O objetivo desta cartilha é apresentar recomendações de caráter geral para a criação de um ambiente de trabalho favorável ao uso do microcomputador na Educação, orientar docentes e usuários dos laboratórios sobre a instalação e sobre os cuidados que se deve ter com os equipamentos e acessórios. Lembramos, porém, que as condições de instalação e utilização podem variar de um local para outro, uma vez que dependem do projeto pedagógico de cada escola. Portanto, todas as sugestões e recomendações deste trabalho devem ser consideradas como referência básica.

Mesmo assim, é fundamental que os requisitos definidos para a instalação elétrica, disposição dos equipamentos, ambiente das salas, segurança etc. sejam rigorosamente observados. Caso contrário, os equipamentos podem ser precocemente danificados ou não apresentar o desempenho desejado.

O Proinfo (Programa Nacional de Informática na Educação) espera que esta cartilha venha contribuir para facilitar a introdução dos equipamentos de microinformática ao seu principal público, que são os professores envolvidos no processo.

Propostas

É preciso ver a tecnologia como uma ferramenta efetiva e necessária, capaz de aumentar tanto a habilidade de comunicação como a capacidade de produção de nossos estudantes e corpo docente. A oportunidade de desenvolver competência tecnológica permitirá aos estudantes e ao corpo docente maximizar seu acesso à informação, além de ampliar a habilidade de resolver problemas e desenvolver a comunicação efetiva na era da informação.

O uso do computador em uma escola pública será incorporado em toda instituição e utilizado em todas as disciplinas curriculares, dentro do que foi definido pelo projeto pedagógico de cada escola. A escola será integrada por rede, utilizando um software de comunicação. Com os computadores em um laboratório de informática, os alunos terão fácil acesso a essa tecnologia. Para dar suporte aos alunos, o corpo docente será capacitado a acompanhar os trabalhos dos estudantes e esclarecer possíveis dúvidas. Enfim, toda comunicação e disseminação da informação na forma escrita será efetuada eletronicamente por meio do uso do computador.

Os estudantes utilizarão a tecnologia como uma ferramenta que será parte integrante de seu desenvolvimento acadêmico e pessoal, no momento atual e no futuro. Hoje em dia é incontestável a afirmação de que a microinformática proporciona agilidade e qualidade ao ambiente escolar, que o microcomputador vem enriquecer o ensino e somar-se aos meios mais sofisticados – como a televisão e o vídeo –, e aos meios mais simples – como o quadro-negro, o livro e o mimeógrafo.

O Proinfo nasceu para levar essa tecnologia para as escolas públicas brasileiras, com a finalidade de ajudar na elaboração de materiais de apoio ao trabalho do professor e ser um valioso recurso para o ensino das diversas disciplinas do currículo, seja em sala de aula, em um trabalho coletivo, seja na dinâmica do trabalho desenvolvido em laboratórios.

Entretanto, para que a microinformática seja bem aproveitada pela comunidade escolar e cumpra adequadamente suas funções, o Proinfo verificou que é necessário não só promover instalações de boa qualidade, condições de manutenção e segurança dos equipamentos, como também estimular a capacitação dos professores e outros usuários, além de definir adequadamente as metas a serem atingidas.

A necessidade de preparar o estudante para um ambiente de trabalho rico em tecnologia já é uma realidade. Assim como os empregados de uma grande empresa usam computadores para fazer seu trabalho, o estudante usará computadores para o seu aprendizado. As ferramentas serão incorporadas ao processo de aprendizado como meios efetivos para os estudantes alcançarem suas metas.

A pesquisa, a análise de dados, a comunicação, a colaboração e a partilha de informações são exemplos de atividades normalmente desenvolvidas em empresas. O estudante pode desempenhar suas atividades de aprendizado com o uso dessas mesmas metodologias e, portanto, adquirir as habilidades funcionais e analíticas necessárias para uma sociedade de alta tecnologia.

Com a tecnologia, o estudante poderá produzir seu trabalho mais rapidamente e ter a oportunidade de assimilar mais conhecimento em um mesmo espaço de tempo. A qualidade de sua produção aumentará e atingirá um nível aceitável. Por exemplo, cada vez mais as apresentações são feitas via computador e integram elementos de multimídia. O estudante deve desenvolver as habilidades para ser bem-sucedido neste novo mundo. Conforme novas ferramentas forem disponibilizadas e aumentarem as alternativas, o desempenho do estudante poderá melhorar proporcionalmente.



As ilustrações foram feitas pelo estudante de 2º grau Alexandre Lenharo Morgado, com o uso de recursos disponíveis no computador

Definições gerais e terminologia

Nesta seção apresentaremos as principais definições relacionadas com os equipamentos recebidos pelas escolas no programa Proinfo. É necessário dizer que todas as figuras apresentadas neste documento são ilustrativas e servem apenas para diferenciar um equipamento de outro.

O MICROCOMPUTADOR

Os computadores possuem quatro áreas principais: os dispositivos de entrada de dados, a unidade central de processamento (CPU), os meios auxiliares de armazenagem e os dispositivos de saída de dados. Os dispositivos de entrada incluem os teclados, os *scanners* e as unidades de disco (HD e CD-ROM).

O processador contém os circuitos eletrônicos que ordenam e processam dados. Os meios auxiliares de armazenagem abrangem as unidades de discos flexíveis, os discos rígidos, os CD-ROMs e os cartuchos magnéticos. Os dispositivos de saída incluem os monitores e as impressoras.

Cada disco é dividido em uma série de trilhas magnéticas concêntricas, em que os dados podem ser gravados. Cada trilha magnética é subdividida em setores. O espaço disponível é alocado com base em setores inteiros. Normalmente, um setor tem 512 bytes de comprimento. O setor é a menor unidade de armazenagem que pode ser alocada para um arquivo.

Na prática, porém, normalmente os dispositivos de armazenagem em disco usam de dois a oito setores para formar um *cluster*, que é usado como unidade mínima de armazenagem. Portanto, um arquivo pequeno, com apenas 400 bytes, pode ocupar até oito setores de espaço de armazenagem (4.906 bytes). O espaço restante entre o marcador, que indica o final do arquivo, e os bytes não utilizados no final do *cluster* é chamado normalmente de *slack space* (espaço ocioso).

Quando o usuário armazena um arquivo grande, o Windows utiliza o menor número possível de *clusters* para armazenar todos os dados do arquivo. Muitas vezes esses *clusters* não são contíguos, o que faz com que o arquivo passe a ocupar *clusters* espalhados por todo o disco. Por essa razão, o Windows utiliza uma tabela de alocação de arquivos (FAT, *file allocation table*) para manter o controle dos *clusters* que estão sendo utilizados pelos arquivos.

O primeiro setor da trilha 0 é um setor especial, chamado setor de *boot*. Esse setor contém, entre outras coisas, informações sobre as dimensões físicas do disco e dimensões lógicas da estrutura do Windows. Os discos rígidos também armazenam informações adicionais no setor de *boot*, em uma área conhecida como tabela de particionamento. Essa tabela descreve as dimensões do disco, o número de partições e o tamanho de cada uma delas.

A tabela de particionamento e o setor de *boot* de um disco rígido são conhecidos como registro-mestre de *boot*. Imediatamente após o setor de *boot* vem a tabela de alocação de arquivos, que é seguida pelo diretório-raiz. O diretório-raiz é uma tabela que descreve todos os arquivos e subdiretórios existentes no disco.

Hardware é o conjunto de componentes físicos do microcomputador, formado pelos periféricos de entrada de dados – teclado, mouse e *scanner*; pelas unidades (drivers) de disquete ou CD-ROM; pela CPU (Central Processing Unit – Unidade Central de Processamento), onde os dados são processados; pelas memórias RAM e ROM¹; (onde os dados são armazenados durante seu processamento); pelas unidades de

¹ ROM (Read Only Memory – Memória Apenas de Leitura) é um tipo de memória que foi pré-gravada e cujo conteúdo não pode ser apagado. RAM (Random Access Memory – Memória de Acesso Aleatório) é outro tipo de memória cuja informação pode ser gravada e apagada de seu interior.

discos HD (Hard Disk); e pelos periféricos de saída de dados – monitor de vídeo e impressoras.

Software Básico é o que se chama usualmente de “programa de computador”. É um conjunto de instruções necessárias para que o microcomputador possa realizar suas tarefas básicas, como ligar, disponibilizar o acesso aos seus dados, gravar e recuperar informações, entre outras.

Software Aplicativo é um conjunto de instruções com a finalidade de executar uma ação específica, como permitir o processamento de textos, de planilhas automatizadas de cálculo, de executar um arquivo de som ou de imagem etc.

Mas para que as tarefas sejam efetivamente realizadas, o microcomputador depende ainda de um elemento fundamental: o usuário. É ele quem toma as decisões necessárias ao bom funcionamento do hardware e do software. Por ser imprescindível e completamente integrado ao microcomputador, o usuário é também conhecido por *peopleware*.



Figura 1: Microcomputador característico

O HARDWARE

As características básicas que devem ser observadas nos equipamentos fornecidos pelo Proinfo e que serão utilizados e manuseados dentro das escolas são:

- Sua capacidade de armazenar dados, que é medida em bytes (lê-se baites); portanto um hardware que tenha capacidade de armazenamento de 500.000 bytes (500 MB – *Megabytes*) é inferior a outro com capacidade de 1.000.000 bytes (1 GB – *Gigabytes*);
- Sua capacidade de processamento de dados, que se resume em capacidade de manipular os dados e gerar novas informações.

Essa capacidade é medida em MHz (Megahertz); portanto um micro de 166 MHz será mais lento no processamento de informações do que um micro de 266 MHz;

- Sua capacidade de memória de processamento (memória RAM), que é utilizada nas operações de processamento de dados.

Em princípio, quanto maior a capacidade de memória de um micro, melhor será sua performance ao processar dados. Essa memória é medida em *megabytes* (ex.: 16 MB, 32 MB etc.).

O usuário deve observar o equilíbrio entre o microprocessador, o disco rígido e a memória. Não adianta escolher um computador com um microprocessador potente sem levar em conta a capacidade de armazenamento do disco rígido e a capacidade de memória RAM. Esses três fatores estão intimamente relacionados e determinam o desempenho do computador.

As configurações médias dos micros fornecidos pelo Proinfo são:

- **CPU** – Microprocessador Intel Pentium ou AMD K6 de 266 MHz interno ao gabinete. Normalmente a CPU é confundida com todos os componentes de hardware internos ao gabinete do computador como na figura ao lado. Na realidade, é na CPU que todos os cálculos necessários à execução de uma tarefa são realizados. Portanto, ela pode ser comparada ao cérebro de um computador.



Figura 2: CPU característica

- **Memória RAM** – 32 MB de capacidade. A memória RAM de um computador é responsável pelo armazenamento de todas as informações intermediárias necessárias à CPU para realização de uma tarefa. Geralmente, todas as informações de como a CPU deve proceder para executar uma tarefa (tais informações são conhecidas por programa de computador) são armazenadas na memória RAM.
- **Unidade de disco flexível** – 3,5” 1,44 MB de capacidade. Uma unidade de disco flexível serve para que o usuário possa armazenar e transportar seus arquivos de um computador para outro, mesmo que não estejam conectados entre si. A unidade de disco flexível usa o que chamamos de disquete para gravar as informações. Este disquete pode então ser transportado pelo usuário e lido por outra unidade de disco flexível em um outro computador. Assim, o usuário tem muita mobilidade para transportar seus arquivos entre computadores distintos.
- **Unidade de disco rígido** – 2.1 GB de capacidade. Cada computador possui, além da unidade de disco flexível, uma unidade de disco rígido. Essa unidade é responsável pelo armazenamento de todos os softwares aplicativos e básicos disponíveis no computador. Além disso, a unidade armazena também arquivos pessoais de todos os usuários daquele computador onde a unidade está instalada.
- **Placa de rede** – Placa padrão NE2000, utilizada para conectar o microcomputador ao cabeamento da rede local, que permite a comunicação entre micros.



Figura 3: Placa de rede

- **Unidade de CD-ROM** – leitora de CD-ROM 5,25” de quádrupla velocidade (4x). Hoje em dia, a unidade de CD-ROM é muito utilizada tanto para armazenamento de software aplicativo ou básico como para armazenamento de enciclopédias e livros. A utilização dessa unidade permitirá ao usuário instalar softwares distribuídos em CD-ROM ou mesmo ouvir música com qualidade digital, já que a unidade permite também o uso de CD’s de música convencionais.



Figura 4: Unidade de CD-ROM

- **Teclado** – Mínimo de 101 teclas, atendendo ao padrão ABNT II (idioma português). O teclado é utilizado para que o usuário acesse o computador. É por meio dele que são digitados textos e também programas de computador. Pode-se dizer que ele é a interface por onde o usuário se comunica com o computador.

- **Monitor** – Padrão SVGA-Color de 15” com resolução de imagem até 1024x768 pixels e ponto (*dot pitch*) 0,28 mm. O monitor de vídeo permite ao usuário visualizar um texto ou figura sem ter de imprimi-lo em uma impressora. Em jargão de informática também se usa o termo “tela”.



Figura 5: Scanner de mesa

- **Scanner** – Com resolução de 600 x 600 dpi, é o equipamento utilizado para a captura (ou digitalização) de imagens ou textos.

- **Fax modem** – interno, com 28.800 bps (bits por segundo) de capacidade, para envio de fax e/ou comunicação entre micros.



Figura 6: Unidade de fax modem



Figura 7: Impressora jato de tinta

- **Impressora jato de tinta** – com resolução de 600 x 300 dpi (pontos por polegada);

- **Impressora laser** – Com resolução de 600 x 300 dpi (pontos por polegada).



Figura 8: Impressora laser

O SOFTWARE

Um microcomputador precisa de software para funcionar. A relação entre o software e o hardware pode ser comparada, guardadas as devidas proporções, à relação existente entre um disco de música e o toca-discos. O software seria o conteúdo do disco, que usa a máquina (hardware) para produzir sons. Podemos categorizar os softwares em Básicos e Aplicativos – os Básicos são aqueles responsáveis pela operação e funcionamento dos micros; os Aplicativos são aqueles utilizados (de fato) por usuários, como os processadores de texto e planilhas.

Os softwares, quando instalados nos microcomputadores, ocupam espaço de armazenamento no disco rígido. Por isso, temos de tomar cuidado quando instalamos muitos softwares em um mesmo equipamento, pois isso pode comprometer o funcionamento dos outros softwares ou da própria máquina, por falta de espaço para operacionalizar suas instruções.

Os usuários devem planejar a instalação dos softwares. Apenas os softwares de uso constante pela maioria dos usuários devem ser instalados em todos os equipamentos. O processador de texto, por exemplo, é comumente utilizado por todos. Já os softwares de uso restrito a algumas pessoas devem ser instalados em apenas um dos microcomputadores.

Os softwares encaminhados juntamente com os equipamentos do Proinfo para as atividades pedagógicas são:

- **Windows 95/98** – O Windows é um ambiente de trabalho gráfico de fácil manuseio. Uma das grandes vantagens do universo gerado pelo software Windows é que todos os softwares aplicativos desenvolvidos para funcionar nesse ambiente possuem os mesmos comandos básicos de navegação e operacionalização. O Windows tem esse nome por disponibilizar as informações para os usuários finais através de “janelas” de visualização, permitindo compartilhar informações entre os diversos aplicativos. Os usuários podem transportar informações de um aplicativo para outro, alternando a ação entre as janelas.

O Proinfo está disponibilizando nos microcomputadores entregues às escolas dois tipos de sistema Windows: o Windows NT e o Windows 95/98. O Windows NT é um sistema operacional de rede local dotado de recursos de gerenciamento e proteção. Ele é usado apenas nos microcomputadores chamados Servidores de Rede. Esses servidores são usados para funções de gerenciamento do ambiente informatizado da escola e também para possibilitar o acesso à Internet. Já o Windows 95/98 é o sistema operacional dos microcomputadores, chamados Estações de Trabalho. As Estações de Trabalho são os microcomputadores usados pelos alunos e professores para realizar trabalhos, como editar textos e desenvolver apresentações multimídia.

- **Microsoft Office** – O Microsoft Office é um conjunto de softwares aplicativos integrados: o processador de texto Word, a planilha eletrônica de cálculos Excel, o banco de dados Access e o software de apresentação PowerPoint compõem este conjunto.

1. **Word:** o Word terá grande utilidade para professores de todas as áreas, uma vez que possibilita a editoração eletrônica, ou seja, a preparação e montagem, no computador, de folhetos, catálogos, apostilas, revistas, manuais, jornais e livros completos. Apresenta recursos para organizar e diagramar páginas, integrando textos, ilustrações e imagens que foram gerados em outros programas. Poderá fazer os jornais da escola ou da classe, por exemplo, que são úteis para socializar informações, incentivar o trabalho em grupo; e o próprio uso do microcomputador pode ser elaborado com a ajuda desse software.

2. **Excel:** o Excel é um software de planilhas eletrônicas – um recurso para cálculos, fórmulas e gráficos. Com ele, o professor poderá desenvolver diversas atividades com os alunos. Em uma planilha, um professor pode lançar as notas de todas as provas e atividades desenvolvidas por seus alunos e facilmente calcular a média final de cada aluno.

3. **PowerPoint:** o PowerPoint é um software de apresentação e poderá ser usado pelos professores para a montagem de exposições gráficas de diversos assuntos, que utilizam o micro como forma de apresentação das informações.

4. **Access:** o Access é um gerenciador de banco de dados e poderá ser usado para a criação de bancos de dados. Por exemplo, para organizar o acervo da biblioteca da escola.

Por formarem um pacote integrado, esses aplicativos podem ser usados simultaneamente e suas informações podem ser transportadas de um aplicativo para outro. O usuário poderá, por exemplo, criar um gráfico referente às informações de uma planilha Excel e posteriormente transportá-lo para o processador de textos Word, a fim de ilustrar um texto que estiver sendo digitado. Esse pacote contém ainda um software de correio eletrônico (e-mail), destinado ao envio e ao recebimento de mensagens entre usuários da rede Proinfo de Informática na Educação.

- **Antivírus** – Primeiramente, vamos entender o que é um vírus de computador. Um vírus é, na verdade, um software aplicativo desenvolvido para bagunçar sua máquina ou mesmo para apagar tudo o que ela possui. A forma mais comum de propagação dos vírus de computador é pela cópia de informações de um micro para outro, por meio de disquetes ou e-mail. A instalação e a utilização de software antivírus é essencial para prevenir a entrada ou remover do computador os vírus já existentes. Novos programas de vírus são constantemente criados, por isso o usuário deve manter versões atualizadas do antivírus.
- **Software de comunicação** (ambiente de rede) – Os softwares de comunicação são responsáveis pela comunicação de um microcomputador para outro, por meio do uso de uma linha telefônica conectada a um modem ou pela comunicação de vários micros em um laboratório, que possibilitam, assim, a integração e troca de experiências e informações entre todos os usuários. Com esse software é possível acessar a Internet e, por exemplo, trocar experiências entre escolas, informações administrativas entre Delegacias de Ensino ou consultar uma biblioteca em qualquer parte do Brasil ou em outro país.
- **Outras categorias** – Existem diversas categorias de softwares aplicativos no mercado que podem ser utilizados com finalidades pedagógicas. Mas os que mais nos interessam são os classificados como softwares educacionais ou softwares de autoria. Os primeiros são produzidos com a intenção de facilitar o aprendizado das diversas disciplinas que utilizam o micro como meio de disseminação. Os softwares de autoria são utilizados para a montagem dos treinamentos automatizados que irão gerar os softwares educacionais. Para cada disciplina, há um bom número de softwares educacionais disponíveis no mercado, elaborados de forma a incentivar a participação do aluno no processo de construção de seu conhecimento.

CONCEITOS GERAIS DE REDES DE COMPUTADORES

Nesta seção serão apresentados os principais conceitos em redes de computadores. Como o assunto é extenso, serão apresentados apenas os conceitos mais relacionados com o nosso ambiente escolar:

O que é uma rede de computadores (LAN, MAN e WAN)

Uma rede de computadores é formada por um conjunto de estações de trabalho capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação, como mostra a figura 9.

O sistema de comunicação é constituído por enlaces físicos (meios de transmissão) e de um conjunto de regras com a finalidade de organizar a comunicação (protocolos).

Redes locais (*Local Area Network* – LAN) surgiram dos ambientes de institutos de pesquisa e universidades. Mudanças no enfoque dos sistemas de computação que ocorreram durante a década de 70 levaram em direção à distribuição do poder computacional. O desenvolvimento de microcomputadores permitiu a instalação de considerável poder computacional em várias unidades de uma organização, ao invés da anterior concentração em uma determinada área.

Redes locais surgiram, assim, para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software), que preservaram a independência das várias estações de processamento e permitiram a integração em ambientes de trabalho cooperativo.

Pode-se caracterizar uma rede local como uma rede que permite a interconexão de equipamentos de comunicação de dados em uma pequena região. Mas tal definição é bastante vaga principalmente no que diz respeito às distâncias envolvidas. Em geral, nos dias de hoje costuma-se considerar pequena região as distâncias entre 100 metros e 25 quilômetros, muito embora as limitações associadas às técnicas utilizadas em redes locais não imponham limites a essas distâncias.

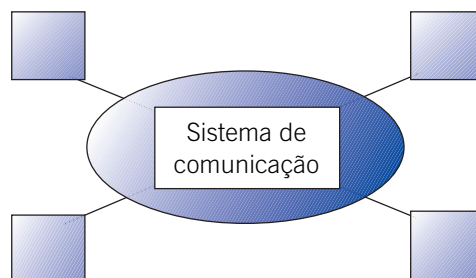


Figura 9: Esquema de uma rede de computadores

Outras características típicas encontradas e comumente associadas a redes locais são: altas taxas de transmissão (de 0,1 a 100 Mbps – megabits por segundo) e baixas taxas de erro (de 10^{-8} a 10^{-11}). É importante notar que os termos *pequena região*, *altas taxas de transmissão* ou *baixas taxas de erro* são suscetíveis à evolução tecnológica. Os valores que associamos a esses termos estão ligados à tecnologia atual e certamente não serão mais os mesmos dentro de poucos anos. Outra característica dessas redes é que são, em geral, de propriedade privada.

Quando a distância de ligação entre os vários módulos processadores começa a atingir distâncias metropolitanas, não chamamos mais esses sistemas de redes locais, mas de redes metropolitanas (*Metropolitan Area Network* – MAN). Uma rede metropolitana apresenta características semelhantes às das redes locais, sendo que as MANs, em geral, cobrem distâncias maiores do que as LANs.

Redes geograficamente distribuídas (*Wide Area Network* – WAN) surgiram da necessidade de se compartilhar recursos especializados com uma comunidade maior de usuários geograficamente dispersos. Por terem um custo de comunicação bastante elevado, tais redes são em geral públicas, isto é, o sistema de comunicação é construído, mantido e gerenciado por grandes operadoras (públicas ou privadas).

Topologias de redes de computadores

No item anterior, a estrutura geral de uma rede de computadores foi apresentada como formada por um conjunto de estações de trabalho e por um sistema de comunicação. O sistema de comuni-

cação vai se constituir de um arranjo topológico que interliga os vários módulos processadores através de enlaces físicos (meios de transmissão) e de um conjunto de regras com a finalidade de organizar a comunicação (protocolos).

Uma das questões vitais na montagem de qualquer rede de computador é a escolha do arranjo topológico (desenho) a ser utilizado. Essa escolha dependerá naturalmente do tipo de rede (LAN, MAN ou WAN) a ser implementada. Portanto, a topologia de uma rede de computadores refere-se à forma como os enlaces físicos e os módulos de processamento estão organizados e determinaram os caminhos físicos existentes e utilizáveis entre quaisquer pares de módulos conectados a essa rede.

Ao organizar os enlaces físicos em um sistema de comunicação confrontamo-nos com diversas formas de utilização das linhas de transmissão. Primeiramente, as ligações podem ser de dois tipos: ponto a ponto ou multiponto (figura 10). Ligações ponto a ponto caracterizam-se pela presença de apenas dois pontos de comunicação, um em cada extremidade da ligação em questão. Nas ligações multiponto, observa-se a presença de três ou mais dispositivos de comunicação com possibilidade de utilização do mesmo enlace.

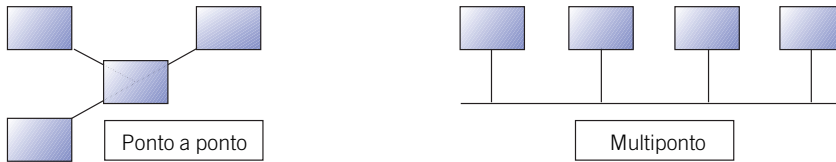


Figura 10: Tipos de ligação

A forma de utilização do meio físico que conecta estações dá origem à seguinte classificação sobre comunicação no enlace:

- Simplex:** o enlace é utilizado apenas em um dos dois possíveis sentidos de transmissão;
- Half-duplex:** o enlace é utilizado nos dois possíveis sentidos de transmissão, porém apenas um por vez;
- Full-duplex:** o enlace é utilizado nos dois possíveis sentidos de transmissão simultaneamente.

A implementação de comunicação Full-duplex pode ser feita com a utilização de dois pares de fios, que possibilitam a comunicação em dois sentidos simultaneamente.

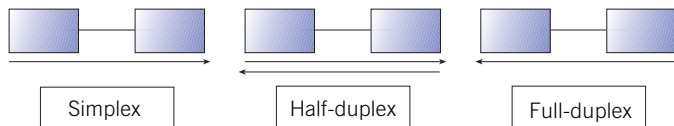


Figura 11: Comunicação simplex, half-duplex e full-duplex

Redes geograficamente distribuídas

Uma primeira tentativa bastante intuitiva para conexão de computadores em rede seria em uma topologia totalmente ligada. Nessa topologia, todas as estações estão interligadas duas a duas por meio

de um caminho físico dedicado. A troca de mensagens entre cada par de estações dá-se diretamente através de um desses enlaces.

Os enlaces utilizados poderiam ser ponto a ponto com comunicação *full-duplex*, de forma a permitir a comunicação plena entre quaisquer pares de estações. Embora essa topologia apresente maior grau de paralelismo de comunicação, torna-se quase sempre impraticável, principalmente em redes com grande número de estações e fisicamente dispersas.

Em uma rede com N estações, por exemplo, seriam necessárias $N(N-1)/2$ ligações ponto a ponto para que se pudesse conectar todos os pares de estações através de linhas dedicadas. Dessa forma, o custo do sistema em termos de instalação de cabos e de hardware específico para comunicação cresceria muito com o número de estações, tornando tal topologia economicamente inviável. A inviabilidade é principalmente observada quando os custos dos meios de comunicação é alto, como no caso das redes geograficamente distribuídas.

Outro caso extremo, desta vez no sentido inverso ao da topologia totalmente ligada, é a topologia em anel. Nessa topologia procura-se diminuir ao máximo o número de ligações no sistema, além de simplificar ao máximo o tipo de ligação utilizada. Dessa forma, utilizam-se para ligar a estação ao anel ligações ponto a ponto, e o anel para levar as mensagens de uma estação a outra, utilizando uma orientação ou sentido único de transmissão.

Uma mensagem deverá, portanto, circular pelo anel até chegar ao computador de destino, sendo passada de estação a estação, obedecendo ao sentido de tráfego definido pelo anel. Apesar de representar uma economia considerável no número de ligações, em sistemas geograficamente distribuídos tal topologia apresenta fatores limitantes que inviabilizam a sua utilização. O primeiro deles diz respeito ao aumento de pontos intermediários entre os pontos finais da comunicação.

Em redes geograficamente distribuídas, isso significa um aumento drástico no número de estações pelas quais uma mensagem tem de passar até chegar ao seu destino final; ou seja, há um aumento intolerável no tempo para a mensagem sair de sua origem e chegar ao destino, particularmente no caso de redes geograficamente distribuídas com meios de transmissão de baixa velocidade.

Outro fator limitante refere-se à inexistência de caminhos alternativos para o tráfego das mensagens. Em redes geograficamente distribuídas devem ser providenciados caminhos alternativos, principalmente se as linhas utilizadas forem de baixa velocidade e pouca confiabilidade – o que é o caso da maioria das redes existentes.

Ao considerar as limitações de velocidade e confiabilidade, somos levados à introdução de caminhos alternativos para um aumento de confiabilidade e de desempenho por meio do paralelismo de comunicações – sem, no entanto, cairmos na topologia completamente ligada, que possui as restrições antes apresentadas. Assim, cria-se uma topologia intermediária que é utilizada pela maioria das redes geograficamente distribuídas: a topologia parcialmente ligada ou topologia em grafo.

Nessa topologia, nem todas as ligações entre pares de estações estão presentes, mas caminhos alternativos existem e podem ser utilizados em casos de falhas ou congestionamento em determinadas ligações. Nos casos em que estações sem conexão física direta precisem comunicar-se, elas deverão de alguma forma, encaminhar as suas mensagens para outra estação que possa fazer a entrega da mensagem para a estação destino. Esse processo pode repetir-se várias vezes, de forma que a mensagem pode passar por vários sistemas intermediários até chegar ao seu destino final.

A escolha do caminho do módulo de origem ao módulo destino por onde a mensagem deve transitar é comumente chamada de roteamento. A escolha da rota (caminho) pode ser feita a priori, antes do envio da mensagem, ou ser realizada passo a passo. No primeiro caso, diz-se que é estabelecida uma

conexão entre os módulos de origem e destino e, neste estabelecimento, é definida a rota por onde deverão transitar as mensagens enquanto perdurar a conexão. No segundo caso, pode haver ou não o estabelecimento de conexão, mas, independentemente disso, cada nó intermediário do caminho é responsável pela escolha do próximo nó do caminho no instante em que recebe a mensagem a despachar, e não a priori como no caso anterior.

Todas as estações de trabalho devem ser capazes de reconhecer se uma mensagem ou pacote de mensagens recebido deve ser passado para um outro módulo ou se tem como destino a própria estação. Qualquer rede com topologia diferente da totalmente ligada tem a necessidade de definir mecanismos de endereçamento que permitam às estações de trabalho decidir que atitude devem tomar ao receber uma mensagem.

Esse endereçamento irá consistir em uma forma de identificar univocamente cada uma das estações conectadas à rede. No caso de ser estabelecida uma conexão entre dois módulos da rede antes da troca de qualquer mensagem, o endereço dos módulos de origem e destino só são necessários quando a conexão é estabelecida. A partir daí, basta que as mensagens transmitidas carreguem a identificação da conexão para que o encaminhamento seja feito a contento. Por outro lado, caso não haja estabelecimento de conexão, cada mensagem deve carregar o endereço do módulo destino e origem.

Redes locais e metropolitanas

As características das redes locais e metropolitanas levam a considerações de custo e tecnologia muito diferentes das redes de longa distância. Uma forma de aumentar a confiabilidade de uma rede local ou metropolitana é utilizar meios de comunicação com baixa taxa de erros e com maior velocidade de transmissão. Topologias muitas vezes inviáveis em ambientes geograficamente dispersos podem ser utilizadas. Em redes locais e metropolitanas geralmente são utilizadas topologias em estrela, anel e barra.

- **Topologia em estrela** – A figura 12 mostra um exemplo de topologia em estrela. Nesse tipo de topologia, cada módulo é interligado a um nó central através do qual todas as mensagens devem passar. Este nó age como centro de controle da rede e interliga os demais módulos. Nada impede que haja comunicações simultâneas desde que os módulos envolvidos sejam diferentes.

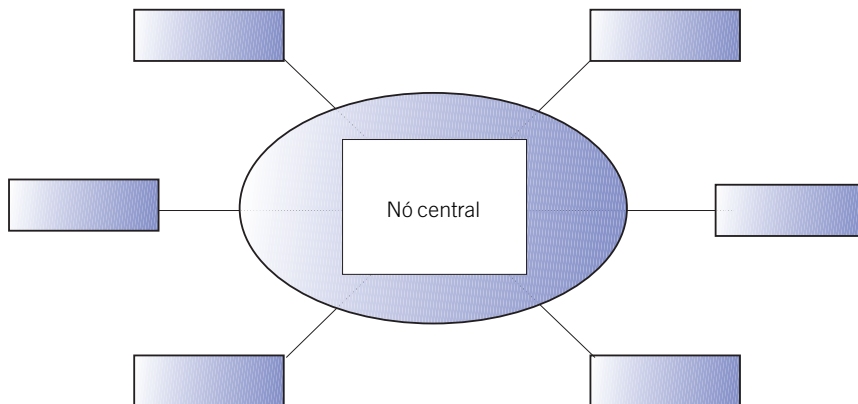


Figura 12: Topologia em estrela

Várias redes em estrela operam em configurações em que o nó central tem tanto a função de gerência de comunicação como facilidades de processamento de dados. Em outras redes, o nó central tem como única função o gerenciamento das comunicações. As situações mais comuns, no entanto, são aquelas em que o nó central está restrito às funções de gerente das comunicações e operações de diagnóstico.

Redes em estrela podem atuar por difusão (*broadcasting*). Nesse caso, todas as informações são enviadas ao nó central, que é o responsável por distribuí-las a todos os nós da rede. Os nós aos quais as informações estavam destinadas copiam-nas e os outros simplesmente as ignoram. Em redes que não operam por difusão, um nó pode apenas se comunicar com outro nó (módulo) de cada vez, sempre sob controle do nó central. Redes em estrela não têm a necessidade de roteamento, uma vez que concentram todas as mensagens no nó central.

Confiabilidade é um problema nas redes em estrela. Falhas no nó central podem causar a parada total da rede. Redundâncias podem ser acrescentadas, porém o custo de tornar o nó central confiável pode reduzir o benefício obtido com a simplicidade das interfaces exigidas pelas estações secundárias. Outro problema em redes em estrela é relativo à modularidade. A configuração só pode ser expandida até o limite imposto pelo nó central.

O desempenho obtido em uma rede em estrela depende da quantidade de tempo necessário para o nó central processar e encaminhar uma mensagem e da carga de tráfego na conexão, isto é, o desempenho é limitado pela capacidade de processamento do nó central. Um crescimento modular que vise ao aumento do desempenho torna-se, a partir de certo ponto, impossível e tem como única solução a troca do nó central.

- **Topologia em anel** – Uma rede em anel consiste em estações conectadas através de um caminho fechado, como mostra a figura 13.

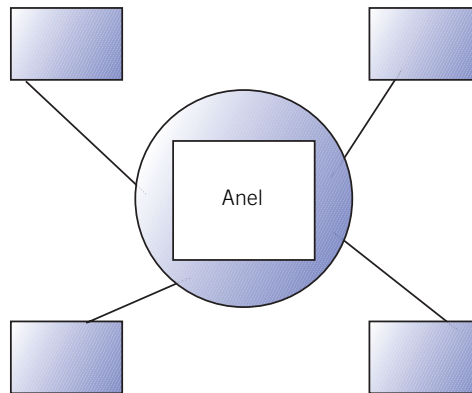


Figura 13: Topologia em anel

Redes em anel são capazes de enviar e receber dados em ambas as direções. As configurações mais usuais são unidirecionais de forma a simplificar o projeto da rede e a tornar menos sofisticados os protocolos de comunicação que asseguram a entrega das mensagens ao destino e em seqüência, pois, como são unidirecionais, evitam o problema de roteamento.

Quando uma mensagem é enviada por um nó, ela entra no anel e circula até ser retirada pelo nó destino, ou então até voltar ao nó de origem. Além de maior simplicidade, as redes em que a mensagem é retirada pelo nó de origem permitem mensagens de difusão, isto é, uma mensagem é enviada

simultaneamente para múltiplas estações. Essas redes possibilitam a determinadas estações receber mensagens enviadas por qualquer outra estação da rede, independentemente de qual seja o nó destino.

- **Topologia em barra** – Na topologia em barra todas as estações se ligam ao mesmo meio de transmissão, como mostra a figura 14. Ao contrário das outras topologias, que são configurações ponto a ponto, a configuração em barra possui uma configuração multiponto.

Nas redes em barra, cada nó conectado à barra pode “ouvir” todas as informações transmitidas, similar às transmissões de radiodifusão. Essa característica vai facilitar as aplicações com mensagens do tipo difusão.

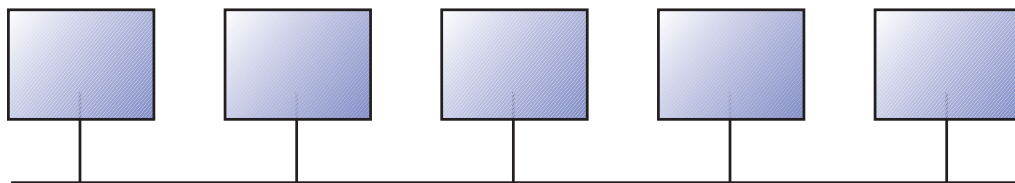


Figura 14: Topologia em barra

Existe uma variedade de mecanismos para o controle de acesso à barra, que podem ser centralizados ou descentralizados. Em um controle centralizado, o direito de acesso é determinado por uma estação especial da rede. Em um sistema de controle descentralizado, a responsabilidade de acesso é distribuída por todos os nós.

O controle centralizado oferece os mesmos problemas de confiabilidade de uma rede em estrela, com atenuante de que, nesse caso, a redundância de um nó da rede pode ser outro nó comum. Mecanismos de controle descentralizados semelhantes aos empregados na topologia em anel podem também ser empregados nesse tipo de topologia, o que acarreta os mesmos problemas encontrados naquela topologia.

Principais equipamentos utilizados em uma rede

Em uma rede de computadores são utilizados equipamentos específicos para permitir implementar o esquema de conexões entre computadores. Entre esses equipamentos, os utilizados pelas escolas são:

- **Concentrador para rede local (*hub*)** – O concentrador para rede local ou simplesmente *hub* é um equipamento usado para conectar vários computadores em rede local. Como o próprio nome diz, um *hub* concentra todos os cabos (ligações) que vêm dos computadores que compõem a rede.
- **Placa de rede** – Para poder ser conectado à rede local, o computador necessita de um dispositivo chamado placa de rede. Esse dispositivo é instalado internamente no gabinete da CPU. Para que a conexão funcione, é necessário ligar a placa de cada computador em uma das entradas do *hub*.



- **Cabeamento estruturado**— O cabeamento da rede é uma estrutura de fios e conectores que interligam as placas de rede dos computadores ao *hub*. O cabeamento de uma rede pode passar despercebido ao usuário menos atento, mas é parte fundamental na implementação de uma rede de computadores.



Arquiteturas *peer-to-peer* e cliente-servidor e o Sistema Operacional de Rede

A interface entre os programas aplicativos e o sistema operacional baseia-se em interações do tipo pedido/resposta, a aplicação solicita um serviço (abertura de um arquivo, impressão de um texto, alocação de memória etc.) através de uma chamada ao sistema operacional.

O sistema operacional executa o serviço solicitado e responde, informando o status da operação (se foi executada com sucesso ou não), transferindo os dados resultantes da execução para a aplicação que solicitou o serviço.

Nessa forma de interação cliente-servidor, a entidade que solicita um serviço é chamada “cliente” e a que presta o serviço é o “servidor”. A interação cliente-servidor constitui-se no modo básico de interação dos Sistemas Operacionais de Rede.

As estações que prestam serviços a outras estações devem possuir o módulo servidor. As estações que permitem que suas aplicações utilizem recursos compartilhados com outras estações devem possuir o módulo cliente.

Nas estações que possuem o módulo cliente, ao receber um pedido de acesso a um recurso localizado em outra estação da rede, o Sistema Operacional de Rede (SOR) monta uma mensagem que contém o pedido e a envia ao módulo servidor da estação onde será executado o serviço.

Na estação remota ou servidora, o SOR recebe a mensagem com o resultado da execução (nos casos em que o pedido envolve a devolução de dados, pode ser necessária mais de uma mensagem) e a envia de volta para o SOR na estação requerente. Quando o SOR da estação que requisitou o serviço recebe a mensagem que transporta a resposta, ele faz sua entrega à aplicação local.

Note que as funções necessárias ao SOR nos módulos clientes são diferentes das funções nos módulos servidores. No módulo cliente, o SOR restringe-se praticamente a fornecer serviços de comunicação de pedidos para o servidor e a entregar as respostas às aplicações.

No módulo servidor, além das funções de comunicação, vários outros serviços são executados. Um desses serviços é o controle do acesso aos recursos compartilhados por vários usuários através da rede, para evitar, por exemplo, que um usuário não autorizado apague arquivos que não lhe pertencem.

Em resumo, pode-se classificar os módulos de um SOR instalados nas estações em dois tipos: SORC (módulo cliente do sistema operacional) e SORS (módulo servidor do sistema operacional).

Na arquitetura *peer-to-peer*, em todas as estações, o sistema operacional de rede possui os dois módulos: SORC e SORS. Essa é a diferença fundamental entre a arquitetura cliente-servidor e *peer-to-peer*. Esse tipo de rede poderia ser montada a partir de micros que utilizam apenas o Windows 95/98, sem um servidor dedicado específico.

Na arquitetura cliente-servidor, caso típico de rede baseada em um servidor de rede Windows NT, as estações da rede dividem-se em estações clientes, que só possuem as funções do módulo cliente acopladas ao seu sistema operacional local, e em estações servidoras. As estações servidoras necessariamente

possuem as funções do módulo servidor e podem, opcionalmente, possuir também as funções do módulo cliente (possibilitando, por exemplo, que um servidor seja cliente de outro, caso típico da relação entre servidores de impressão de arquivos). A arquitetura cliente-servidor possui duas variações definidas pela forma como são utilizados os servidores.

Na arquitetura cliente-servidor com servidor dedicado, as estações servidoras incluem necessariamente um módulo SORS e, opcionalmente, um módulo SORC, que, se existir, só pode ser usado pelo módulo SORS para permitir que este seja cliente de outro servidor.

Nessa arquitetura, geralmente as estações servidoras não permitem usuários locais e são integralmente dedicadas ao atendimento de pedidos enviados pelas estações clientes através da rede.

Na arquitetura cliente-servidor com servidor não dedicado, as estações servidoras possuem um sistema operacional local que é estendido por um módulo SORS e um módulo SORC. O módulo SORC pode ser usado tanto pelo SORS quanto pelas aplicações dos usuários locais da estação servidora.

Assim, os recursos locais das estações servidoras são compartilhados tanto pelos usuários atendidos pelo sistema operacional local quanto pelos usuários remotos, que fazem pedido ao SOR através da rede. Como a estação servidora possui um módulo SORC, seu SORS pode ser cliente de outra estação servidora, como em alguns servidores dedicados.

Em resumo, servidores podem ser clientes de outros servidores da rede. Por exemplo, um servidor de impressão pode ser cliente de um servidor de arquivos ao fornecer serviços aos seus próprios clientes. Serviço de correio eletrônico é um outro exemplo de servidor que muitas vezes é realizado utilizando os serviços de armazenamento de arquivo de um outro servidor.

Para finalizar esse assunto, vamos nos ater mais detalhadamente a um servidor muito utilizado: o servidor de impressão. O servidor de impressão tem como finalidade oferecer serviços de impressão a seus clientes, possuindo um ou mais tipos de impressora acoplados, cada um adequado à qualidade ou rapidez de uma aplicação particular.

Existem várias formas para implementar um servidor de impressão. A forma mais simples é baseada na pré-alocação da impressora. Nesse caso, o cliente envia um pedido ao servidor, manifestando o desejo de uso de uma impressora específica.

Caso essa impressora esteja disponível, ela é alocada ao cliente até que este a libere ou então se esgote o tempo máximo de utilização, conforme negociação na alocação. Caso a impressora não esteja disponível, o cliente é avisado e colocado, se for de seu desejo, em uma fila de espera.

Uma outra forma de implementar um servidor de impressão é utilizar a técnica de *spooling*. Nesse caso, o cliente, ao invés de pedir a alocação de uma impressora, envia diretamente ao servidor o documento a ser impresso. Esse documento é colocado em uma fila de espera e é impresso quando a impressora estiver disponível.

A fila de impressão pode ser implementada em forma de arquivos localizados nos discos existentes no servidor de impressão ou então por meio de arquivos de um servidor de arquivos localizado ou não na mesma estação do servidor de impressão.

Nesse último caso, o cliente envia seu documento ao servidor de arquivos e um pedido ao servidor de impressão para a impressão do arquivo determinado. O servidor de impressão, que atua como cliente do servidor de arquivos, solicita que ele lhe envie o arquivo para impressão quando tiver uma impressora disponível para tal.

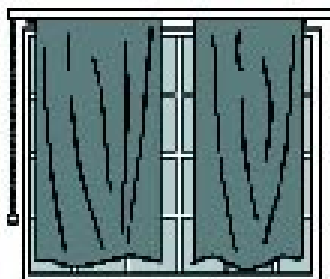
Preparação para receber os equipamentos

A seguir, apresentaremos recomendações para a preparação do ambiente para recebimento dos equipamentos, as instalações elétricas por cabeamento da rede local, mobiliário e segurança.

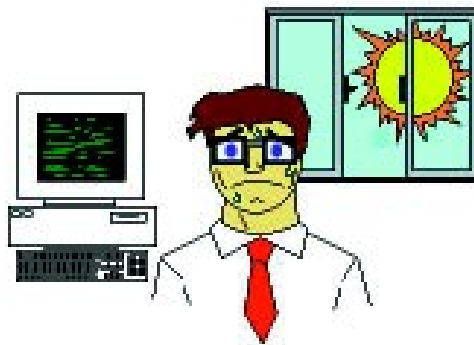
SALA INFORMATIZADA

Vamos considerar a existência de apenas um ambiente informatizado ou laboratório. A preparação da sala informatizada deverá seguir os seguintes pontos:

- Área livre de, no mínimo, 36 m² (dimensões entre 5 x 7 m e 4 x 9 m), pé-direito mínimo de 2,6 m, boa iluminação, mas sem exposição à luz direta do sol, ventilação adequada e sem falhas estruturais ou ambientais, tais como infiltrações, rachaduras, mofo, calor excessivo ou poeira.
- Os equipamentos não podem ficar expostos à luz solar direta. Providenciar cortinas (grossas) e/ou persianas quando for o caso.



- Caso o clima local e as condições de ventilação da sala propiciem temperatura ambiente inferior a 30°C em qualquer época do ano, o uso de ar condicionado poderá ser dispensado.
- Caso contrário deverá ser instalado um ar condicionado capaz de manter as características ambientais adequadas.



- O dimensionamento da capacidade do ar condicionado deve ser realizado por pessoa ou empresa especializada, de forma a garantir uma temperatura ambiente entre 22°C e 25°C, com a sala em uso normal (repleta de alunos).
- A sala não deverá ser instalada em áreas expostas a agentes corrosivos, tais como areia, maresia, ácidos etc.
- No caso de prédios de mais de um andar, evitar que a sala seja instalada sob as tubulações hidráulicas do andar superior, já que qualquer problema de vazamento poderá danificar os equipamentos.



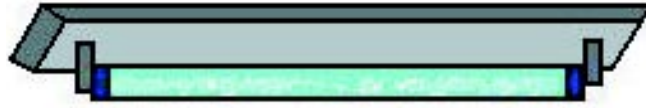
- Janelas resistentes, que possam ser trancadas por dentro, reforçadas externamente por grades de aço fixadas à parede.



- Quadro de laminado melanínico branco (quadro branco) fixado em uma das paredes, em posição de acesso livre e sem incidência de reflexos. Lembrar que o pó de giz danifica os equipamentos e deve ser totalmente evitado. Em hipótese alguma deverá ser utilizado quadro-negro.



- A iluminação artificial deverá usar lâmpadas fluorescentes. Garantir que existam interruptores que permitam o desligamento parcial das lâmpadas, de forma que seja possível reduzir a luminosidade próxima ao quadro branco para evitar reflexos.



- Deverá haver uma única entrada para a sala, fechada por porta em madeira resistente com fechadura tipo “yale” com travamento interno rápido. Além das condições gerais da segurança do prédio, considerar uma segunda porta (grade de aço e cadeado) no mesmo batente.



- O piso pode ser em madeira, pedra, cimento liso, vinil, cerâmica ou equivalente, sem desníveis ou ressaltos. Em nenhuma hipótese poderão ser usados carpetes, tapetes ou similares, pois acumulam pó e são de difícil limpeza.
- As paredes devem ser pintadas em cor clara, com tinta resistente à água. É preciso haver fornecimento de energia elétrica de 110V ou 220V com capacidade suficiente para alimentar todos os equipamentos (cerca de 10KVA). Em caso de dúvida, deverá ser consultado o responsável pela manutenção elétrica do prédio para averiguar a real capacidade da rede elétrica local.
- Um canto da sala, de fácil acesso e distante da porta, será escolhido para a instalação do *hub* para os cabos da rede local e os quadros de distribuição elétrica e lógica.
- O acesso ao Provedor Internet, que pode ser o NTE, será feito por linha telefônica comum. Para tanto, deverá ser providenciada uma linha telefônica a ser instalada próxima ao micro onde estará a placa fax-modem.

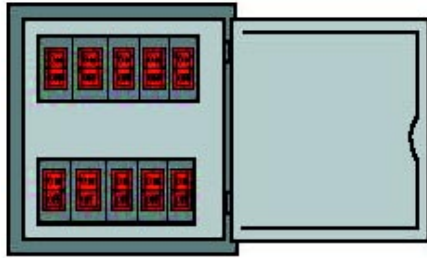
REDE ELÉTRICA

A instalação elétrica é fator crítico para o bom funcionamento dos equipamentos e para a segurança dos usuários. Ela deve ser orientada e/ou realizada por profissional ou empresa especializada. Seguem algumas recomendações essenciais:

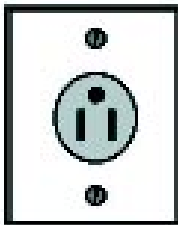


- Circuito independente 110V e/ou 220V.
- Tubulações ou canaletas exclusivas com diâmetro mínimo de 1/2 polegada.

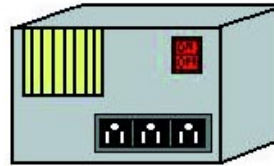
- O circuito elétrico de alimentação dos equipamentos de informática deve ser exclusivo, isto é, não pode ser compartilhado com outros equipamentos, principalmente aqueles de alta potência, como motores e aparelhos de ar condicionado.
- Os circuitos elétricos de distribuição podem ser internos ou externos às paredes. A montagem externa é normalmente mais adequada para a redução de custos e, nesse caso, os fios deverão ser protegidos por canaletas coladas à parede.
- Todos os circuitos elétricos e suas tomadas devem ser claramente identificados como “Circuito Exclusivo para Computadores”, para evitar que alguém ligue qualquer outro equipamento na mesma rede.
- A sala deverá dispor de um quadro de distribuição de energia elétrica dotado de um aterramento real (não usar o “Neutro” da rede), feito por malha e barras de cobre enterradas no chão, com resistência final menor que 10Ω , medida por equipamento específico;



- Na falta de equipamento específico, um teste prático para verificar a qualidade do aterramento é ligar uma lâmpada de 100W entre os pinos “Fase” e “Terra”. Se a lâmpada acender totalmente, o aterramento está em boas condições. Se ela não acender ou acender parcialmente, o aterramento está com problemas.
- Esse quadro de distribuição exclusivo para os computadores deverá conter disjuntores de proteção. Lembrar que o consumo estimado de um microcomputador e impressora é de cerca de 0,6 Kva.
- Cada disjuntor alimentará quatro tomadas de computador, próximas entre si.
- Os disjuntores e as tomadas deverão ter etiquetas identificadoras para cada circuito elétrico.
- Ao longo das paredes das salas deverão ser instaladas tomadas tripolares (três pinos) monofásicas, em caixas modulares externas, a 50 cm de altura do chão, próximas aos locais onde serão instalados os equipamentos (computadores, impressoras, *hubs* etc.).



- Os equipamentos não devem ser ligados diretamente às tomadas da rede elétrica. Devem ser ligados nos estabilizadores de voltagem (com filtro de linha interno) com potência mínima de 0,6 Kva.



- A fiação para os computadores deverá ser realizada com condutores “antichama” compatíveis com a voltagem local e a corrente calculada nos disjuntores.
- No caso de montagem externa, deverão ser instaladas canaletas plásticas ventiladas de tampo removível, ao longo das paredes da sala e imediatamente abaixo das tomadas tripolares.
- Os fios devem ser de boa qualidade, com bitola mínima de 2,5 mm². Um fio de boa qualidade traz gravadas em sua extensão as especificações: nome do fabricante, bitola, isolamento, temperatura e certificação Inmetro.
- A rede elétrica deve ser protegida por pára-raios de linha, a fim de evitar que descargas atmosféricas danifiquem os equipamentos.



- Por segurança e estética, todos os cabos e fios devem ficar ocultos ou presos. Nenhum usuário deve ter acesso a eles, para evitar problemas de contato e curto-circuito.

Não atender às exigências mínimas em relação à parte elétrica pode significar sérios prejuízos para o microcomputador, comprometer seu bom funcionamento ou até causar-lhe avaria total. Isso desestimula o usuário iniciante, que terá somado às suas dúvidas normais de aprendiz outras tantas decorrentes do mau funcionamento de uma máquina que ainda não domina. Portanto, todo cuidado é necessário no que se refere à instalação elétrica.

Aterramento da rede elétrica

Nos locais onde não existe um sistema de aterramento instalado, deverá ser construído um sistema que possibilite o aterramento de todos os equipamentos de informática. O sistema de aterramento em hipótese alguma deverá ser substituído pelo neutro da rede elétrica.

Sugerimos que a questão seja tratada com o auxílio de assessoria especializada – eletricista ou empresa de instalações elétrica. Mesmo assim, apresentamos sugestões para construção de um sistema de aterramento simples:

1. Na canaleta destinada à fiação elétrica, passe juntamente com os cabos elétricos um fio de cobre com aproximadamente 0,5 cm (meio centímetro) de diâmetro. Este cabo deverá ter o comprimento suficiente para passar pela canaleta e ainda sobrar para os procedimentos que se seguem;
2. No exterior do ambiente informatizado, faça um buraco de aproximadamente 2 m de profundidade e 20 cm de diâmetro no solo;
3. Uma extremidade do cabo de cobre descrito no item 1 deverá ser lançado dentro do buraco até atingir o fundo. Recomenda-se que na extremidade faça-se uma dobra em forma de anel para que o cabo fique seguro no interior do buraco e também posicionado no meio do buraco e não nas suas extremidades;
4. Em seguida, o buraco deverá ser preenchido. O preenchimento do buraco deverá ser feito com uma mistura da própria terra retirada e carvão mineral, na proporção de uma parte de terra para uma parte de carvão mineral;
5. O buraco deverá ser preenchido com essa mistura até a boca. Deverá também haver a compactação da mistura de terra e carvão, de forma a fixar o cabo de cobre ao solo;
6. Durante o preenchimento do buraco, poderá haver o acréscimo de um pouco de água para ajudar na compactação;
7. Em terrenos muito arenosos, sugerimos que não se use a terra retirada do buraco para preenchê-lo, mas sim terra com menor teor de areia;
8. O fio de cobre, que agora é o terra, deverá ser ligado ao terceiro pino de todas as tomadas da rede elétrica que se desejem aterrar.

O neutro da rede elétrica não deve ser utilizado porque não é um terra (embora popularmente seja conhecido com o nome de terra). O neutro é usado apenas como referência para a fase. Se, por exemplo, uma rede possui uma voltagem de 110V, isto significa que a diferença entre a voltagem do neutro e a voltagem da fase é de 110V, não significando que a voltagem do neutro seja zero. Conseqüentemente, pode haver eletricidade no chamado neutro da rede, e é por isso que ele não deve ser usado em hipótese alguma como terra da rede elétrica.

Outra prática muito comum, mas com resultados catastróficos, é a utilização de fios amarrados em pregos, canos de ferro, canos de PVC ou torneiras para servir como aterramento. Esses sistemas não são terras e, se usados, podem colocar em risco todos os equipamentos elétricos a eles ligados.

CABEAMENTO DA REDE LOCAL

O cabeamento da rede local ou rede lógica será fundamental para o funcionamento dos equipamentos em rede. Ele deve ser orientado e/ou realizado por profissional ou empresa especializada. Seguem algumas recomendações essenciais:

- Deverá ser usado fio par trançado de oito vias Categoria 5.
- A fiação lógica deve correr dentro de canaletas plásticas ventiladas de tampo removível, ao longo das paredes da sala, com seção reta mínima de 9 cm², instaladas 20 cm acima da fiação elétrica. Em hipótese alguma os cabos da rede local deverão com-

partilhar a mesma canaleta da fiação elétrica.

- A extremidade que será ligada ao *hub* deverá possuir conector macho padrão RJ-45.
- Entre cada dois computadores e imediatamente acima da canaleta devem ser colocadas caixas plásticas externas para conexão lógica. Cada uma delas com duas tomadas fêmeas padrão RJ-45. A extremidade da fiação lógica oposta à ligada ao *hub* deverá ser ligada a essas tomadas.
- Concentrador lógico (*hub*) que será fornecido com os equipamentos da rede local deverá ser localizado em local de fácil acesso, porém distante de local de trânsito de pessoas.
- Antes da interligação dos equipamentos, todo o cabeamento da rede deverá ser testado com equipamentos específicos. A empresa responsável pelo cabeamento deverá realizar esse teste.
- Todos os cabos devem ser identificados por etiquetas nas duas extremidades: a extremidade que se liga ao *hub* e a extremidade que se liga ao micro (tomada conector fêmea padrão RJ-45).
- Todas as tomadas com conectores fêmea padrão RJ-45 deverão possuir etiquetas, de forma que uma determinada tomada e a extremidade que será ligada ao *hub* possam ser identificadas apenas por meio dessa etiqueta.

A interligação dos equipamentos na rede local não é uma tarefa complexa, podendo ser realizada por qualquer pessoa, que siga os seguintes passos:

1. Ligar todos os cabos UTP ao *hub*. Esta tarefa é simples, bastando apenas conectar cada extremidade etiquetada dos cabos em cada uma das entradas do *hub*. A ordem de ligação desses cabos não é importante, sugere-se apenas que seja mantida uma ordem crescente (ou decrescente) para facilitar a localização de um cabo específico;
2. Ligar todos os microcomputadores em suas respectivas tomadas da rede. Esta tarefa consiste em conectar um dos cabos de rede fornecidos com os microcomputadores em uma tomada padrão RJ-45 e na traseira de um microcomputador. Note-se que os microcomputadores terão apenas uma entrada em sua traseira que seja capaz de receber o cabo.

Mobiliário

As características do mobiliário dependem diretamente da configuração (*layout*) da sala. A seguir são apresentadas recomendações de ordem geral que podem orientar a aquisição desse mobiliário.

Mesas

- Com tampo em madeira revestida de laminado texturizado (fórmica) fosco, cor clara, inteiro, com profundidade mínima de 75 cm, mínimo de 2 cm de espessura, cantos arredondados e borda revestida.
- Altura do tampo ao chão de aproximadamente 70 cm.
- Pés em estrutura metálica de aço perfilado, com parafusos niveladores nos pontos de apoio no chão, unidos entre si por chapa de aço dobrada ou madeira similar ao tampo, de no mínimo 35 cm de largura.
- Todas as partes metálicas devem ter tratamento antiferrugem, ponteiros arredondados nas extremidades e pintura eletrostática de cor preta ou grafite.

Cadeiras

- Estrutura de sustentação tubular em aço, sem braços, com no mínimo quatro pés.
- Os pontos de apoio no chão deverão ter ponteiros em aço ou plástico resistente ao atrito, que não risquem o chão.
- Assento e encosto estofados em espuma injetada, coberta por tecido ou vinil, em cor escura.
- Altura do assento ao chão de 43 cm, com encosto fixo e côncavo, em altura adequada para suporte lombar ao tronco do usuário.
- Todas as partes metálicas devem ter tratamento antiferrugem, ponteiros arredondadas nas extremidades e pintura eletrostática de cor preta ou grafite.

Mesas para impressoras

- Tampo em madeira revestida de laminado texturizado (fórmica) fosco, cor clara, inteiriço, medindo aproximadamente 60 cm x 50 cm com, no mínimo, 2 cm de espessura, cantos arredondados e borda revestida de PVC flexível, a uma altura de aproximadamente 75 cm.
- Pés em estrutura metálica de aço perfilado, com parafusos niveladores nos pontos de apoio no chão, unidos entre si por chapa de aço dobrada ou madeira similar ao tampo, de no mínimo 35 cm de largura.

A sala informatizada deverá ter ainda:

- Um armário, em madeira laminada de cor clara, com aproximadamente 100 cm x 160 cm x 40 cm com portas dotadas de fechadura, dividido internamente em prateleiras.
- Um quadro de laminado melanínico branco (quadro branco), com 1,5 x 1,25 m, para ser fixado à parede, com calha-suporte para marcadores e acompanhado de apagador adequado ao quadro.

Segurança

A segurança dos equipamentos da sala informatizada é fundamental para prevenir depredações e furtos. Para isso são feitas algumas recomendações:

- As janelas que dão acesso externo, tanto para o interior da escola quanto para a rua, deverão estar protegidas por grades de ferro devidamente instaladas.
- As portas que dão acesso ao interior da sala informatizada, deverão possuir batentes reforçados e grades de ferro com cadeado devidamente instaladas.
- Quando a sala for externa à escola ou então a escola estiver em local de alta periculosidade, instalar alarmes monitorados em todas as portas e janelas.
- A segurança da sala informatizada não deverá ficar somente a cargo do zelador da escola nem deve ele ficar com a chave do cadeado das portas que dão acesso à sala, evitando assim que possa ser obrigado a abrir a sala para um roubo.
- Quando não estiver sendo utilizada, a sala informatizada deverá permanecer trancada e, onde for o caso, com o sistema de alarme ligado.

Os equipamentos serão entregues acompanhados de um dispositivo antifurto formado por uma trava com chave que, fixada na parte posterior da CPU, vai prender todos os cabos; e um cabo de aço que vai

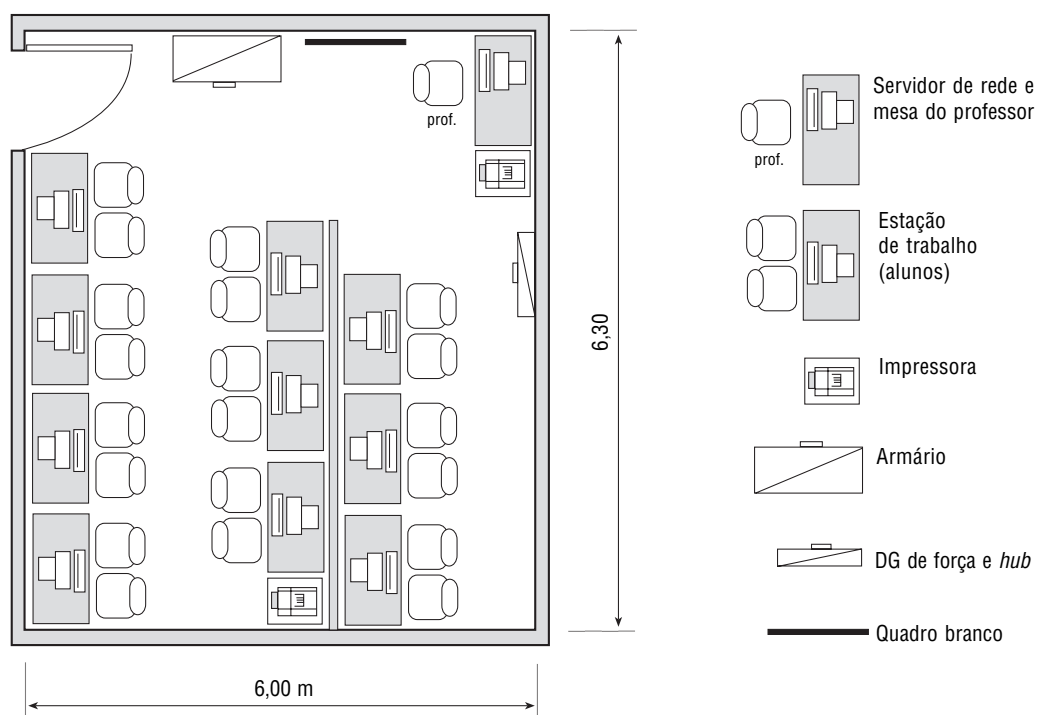
prender a trava à mesa. Esses dispositivos devem ficar sempre instalados e com suas chaves fechadas. Eles não impedem o furto qualificado, mas evitam o furto de oportunidade ou brincadeiras de mau gosto.

Disposição dos equipamentos na sala

A disposição dos equipamentos irá depender do projeto pedagógico da escola. No entanto, dentro da preocupação de descrever uma situação de laboratório típico, apresentamos algumas recomendações de ordem geral:

- Os equipamentos precisam ser instalados com uma distância mínima de 1 m entre eles.
- Essa distância impede interferências e facilita a sua utilização e manutenção.
- Uma distância maior precisará ser adotada, caso o uso predominante dos equipamentos seja por dois alunos simultaneamente.
- Lembrar que os cabos elétricos e lógicos (cabos de impressoras, de monitor etc.) ficam na parte posterior do equipamento. É preciso considerar isso e deixar o espaço adequado quando houver trânsito de pessoas. Lembrar também que o *hub* deverá estar localizado em local de fácil acesso e longe do trânsito de pessoas. A título de exemplo, sugere-se o seguinte *layout*.

Proposta de sala informatizada



A entrega dos equipamentos

As escolas participantes do Proinfo foram selecionadas pelas Comissões Estaduais de Informática na Educação, com base em critérios próprios que definiram, inclusive, a quantidade de equipamentos (ou conjuntos) designados para cada escola.

No entanto, para receber os equipamentos, essas escolas precisam também atender aos requisitos básicos do Proinfo, que são: ter um projeto pedagógico aprovado, professores treinados ou em treinamento, e instalações físicas adequadas. A adequação das instalações físicas é fundamental para assegurar as condições de garantia de funcionamento dos equipamentos, que é de cinco anos.

O processo de entrega é, portanto, precedido da verificação das condições de instalação física e técnica. Somente a aprovação dessa vistoria é que permitirá ao Proinfo liberar a instalação dos equipamentos.

A instalação dos equipamentos em cada escola será realizada por um técnico autorizado da empresa vencedora da licitação, na presença do diretor da escola e/ou do responsável designado pela Comissão Estadual de Informática na Educação. A guarda provisória dos equipamentos será de responsabilidade do representante que assinou o respectivo Termo de Aceitação, com a co-responsabilidade da Comissão Estadual de Informática na Educação, até a transferência definitiva dos conjuntos, mediante Termo de Doação com Encargos, a ser assinado pela autoridade competente.

O papel dos NTEs

Os Núcleos de Tecnologia Educacional (NTEs) são importantes estruturas descentralizadas de apoio ao processo de informatização das escolas. Ali são preparados os professores da rede pública e os técnicos de suporte à informática educativa.

Os núcleos são instalados de acordo com o plano de informatização definido pelos estados nos seus Projetos de Informática Educativa. Em média, até 50 escolas estarão vinculadas a cada NTE, dependendo das condições específicas de cada Estado, tais como número de alunos, dispersão geográfica, telecomunicações e facilidade de acesso.

Cada núcleo disporá de uma equipe composta por educadores e especialistas em telemática e de um conjunto adequado de equipamentos de informática. Os NTEs deverão estar ligados a pontos de acesso à Internet e ter papel de destaque no processo de formação da Rede Nacional de Informática na Educação, onde atuarão como concentradores de comunicação para interligar as escolas a eles vinculados.

Em adição ao seu papel de estrutura de capacitação, os núcleos deverão assumir o papel de estrutura permanente de suporte ao uso da informática, para apoiar, em termos técnicos e pedagógicos, os professores e os técnicos de suporte das escolas sob a sua subordinação. Além disso, eles farão parte do sistema de Acompanhamento e Avaliação do Programa.

Os Núcleos de Tecnologia Educacional (NTEs) serão responsáveis pelas seguintes ações:

- Sensibilização e motivação das escolas para incorporação da tecnologia de informação e comunicação.
- Apoio ao processo de planejamento tecnológico das escolas para aderir ao Projeto Estadual de Informática na Educação.
- Capacitação e reciclagem dos professores e das equipes administrativas das escolas.
- Realização de cursos especializados para as equipes de suporte técnico.
- Apoio (*help-desk*) para resolução de problemas técnicos decorrentes do uso do computador nas escolas.
- Assessoria pedagógica para o uso da tecnologia no processo de ensino-aprendizagem, acompanhamento e avaliação local do processo de informatização das escolas.

Os Núcleos de Tecnologia Educacional disporão de:

- Laboratórios semelhantes aos que serão instalados nas escolas, de forma a reproduzir o ambiente tecnológico que estará disponível para os professores.
- Servidores de recursos da Internet, para que os Núcleos sejam os Provedores de Serviços para as escolas de sua área de atendimento.
- Equipamentos para desenvolvimento, testes e avaliação de programas educativos.

Assistência técnica

Os equipamentos do Proinfo estão cobertos por uma garantia de funcionamento de cinco anos. A assistência técnica autorizada da empresa vencedora da licitação é a única responsável pela manutenção dos equipamentos do Proinfo.

Cabe às escolas e aos NTEs a responsabilidade de manter os equipamentos nas condições especificadas pelo fornecedor, para que sejam mantidos os direitos à garantia de funcionamento.

Os NTEs darão apoio às escolas sob sua jurisdição e, para isso, contarão com técnicos especializados em redes de computadores e manutenção de hardware e software, que auxiliarão as escolas na diagnose de falhas. Todos os Chamados Técnicos devem ser encaminhados por intermédio da estrutura dos NTEs, que definirá os procedimentos a serem seguidos pelas escolas.

Apresentamos, a seguir, algumas definições sobre a assistência técnica que foram estabelecidas no Edital da Concorrência 01/98, que adquiriu os equipamentos do Proinfo:

- **Chamado técnico** é a solicitação de um atendimento técnico. Os chamados técnicos devem ser precedidos de tentativas de solução dos problemas por intermédio do NTE e do serviço de *help-desk* da Procomp.
- **Atendimento técnico** é a presença no local de instalação dos conjuntos de técnico habilitado. Todo atendimento terá um relatório de atendimento, que deverá ser vistado pelo representante da escola, comprovando, ou não, a solução dos problemas.
- **Consulta técnica** é qualquer contato com o fornecedor, feito através de telefone ou Internet para consulta, esclarecimento ou orientação.
- **Prazo de reparo** é o período, em dias úteis, transcorrido entre o chamado técnico e o efetivo restabelecimento do funcionamento dos equipamentos. Esse período não pode ultrapassar os seguintes prazos:

REGIÃO DA ESCOLA	PRAZO DE REPARO MÁXIMO
Nordeste	5 dias úteis
Norte/Centro-Oeste	9 dias úteis
Sudeste	4 dias úteis
São Paulo	3 dias úteis
Sul	3 dias úteis

- É facultado à empresa vencedora da licitação (licitante vencedor) elaborar plano de manutenção que inclua treinamento especializado para técnicos dos Núcleos de Tecnologia Educacional (NTEs) e escolas, com o objetivo de maximizar a eficiência das Consultas Técnicas e minimizar a necessidade de chamados técnicos.

Antes de recorrer à assistência técnica, faça algumas verificações simples, evitando chamados desnecessários. Apresentamos abaixo uma pequena lista de tópicos a serem verificados:

PROBLEMAS MAIS COMUNS	VERIFICAR
O teclado está travado	<ul style="list-style-type: none">• Se está corretamente conectado à CPU• Se a chave de trava do teclado (na CPU) está desativada
O monitor está sem imagem (tela escura)	<ul style="list-style-type: none">• Se o monitor está ligado à energia elétrica• Se o cabo lógico do monitor está conectado à CPU• Os botões de brilho e contraste
O mouse não funciona ou o cursor não obedece ao mouse	<ul style="list-style-type: none">• Se o cabo do mouse está conectado à CPU• Se não há sujeira no interior do mouse
A impressora não funciona	<ul style="list-style-type: none">• Se a impressora está ligada à tomada de energia• Se o cabo lógico está corretamente conectado à impressora e à CPU• Se está sem papel ou sem <i>toner</i> ou cartucho• Se o driver da impressora está devidamente instalado no equipamento

Informações e recomendações gerais

DICAS PARA A UTILIZAÇÃO DOS EQUIPAMENTOS

Equipamentos de informática não são simples nem baratos, por isso é altamente recomendável que se tomem alguns cuidados adicionais para a sua correta utilização:

- Antes de ligar qualquer equipamento, verificar sempre se a voltagem da rede elétrica é a mesma requerida pelo equipamento.
- Não transporte ou mova equipamentos ligados ou funcionando – sempre desligue antes.
- Evite comer, beber e fumar enquanto opera o equipamento.
- As capas de plástico servem para evitar o acúmulo de poeira e devem ser usadas quando o equipamento estiver desligado. Com o equipamento ligado não devem ser usadas, pois impedem a ventilação interna.
- É recomendável que o equipamento não seja ligado e desligado várias vezes ao dia – ligue no início do período e só o desligue ao final.
- Caso o equipamento vá ficar longo tempo desligado, é aconselhável desligá-lo da tomada.
- Evite tocar a tela do monitor de vídeo.
- Evite colocar objetos sobre o microcomputador.

O QUE É UM VÍRUS DE COMPUTADOR

Um vírus é um programa que, sob determinadas circunstâncias, causa anomalias no funcionamento do computador. Essas anomalias podem variar desde um simples atraso no processamento (tornando o computador um pouco lento) até a perda total das informações gravadas. Embora quase todos os vírus provoquem algum tipo de efeito indesejável, nem sempre causam danos.

Além dos vírus temos os *Worms* (vermes) e *Trojan Horses* (Cavalos de Tróia). Um verme é um programa maligno, geralmente projetado para executar alguma atividade ilegal, que se dissemina com a produção de múltiplas cópias de si próprio. Enquanto os vírus sempre exigem um hospedeiro, como um disco ou programa, os vermes são programas auto-suficientes.

Os Cavalos de Tróia (*trojans*) são programas disfarçados sob a aparência de software legítimo. O programa pode ter aparência e funcionamento idênticos aos do programa autêntico, mas outras atividades podem estar ocorrendo em segundo plano sem que o usuário perceba. Existem *trojans* de todo tipo, desde aqueles que travam a máquina, até aqueles que apagam todo o disco. Ao contrário dos vírus, que se auto-instalam, os *trojans* são instalados pelo próprio usuário, que pensa estar instalando um programa inofensivo.

Outros tipos de *trojans* que têm dado muita dor de cabeça são os conhecidos como *ansi-bombs*. Eles não passam de um arquivo simples e inocente, porém, quando o mesmo é visualizado por um

comando *type* (do DOS), ao invés de mostrar o seu conteúdo, ativa o comando `deltree /y c:*.*`, o que significa apagar todos os arquivos e todos os diretórios do seu disco sem pedir confirmação.

Esse tipo de *trojan*, porém, só pode entrar em ação se o arquivo Ansi.Sys estiver presente na cláusula Device do seu Config.Sys. Se você precisar usar um *driver ansi*, prefira o Ansi.Com, que é chamado do Autoexec.Bat, pois este não possui uma série de recursos indispensáveis para que as *ansi-bombs* funcionem.

Uma das maiores confusões sobre o tema vírus de computador é quanto à contaminação e ataque. Muitas pessoas acham que as duas ações são a mesma coisa, porém há diferenças que podem não ser tão sutis assim.

Contaminação – Uma contaminação pode ocorrer a cada dia ou a cada hora ou momento. A maioria dos vírus infectam um sistema, e em seguida permanecem escondidos, ficando à espreita de mais “alguém” para contaminar.

Ataque – Um ataque só ocorre em uma determinada combinação de fatos muito específicos: pode ser apenas uma data, uma certa quantidade de execuções ou uma combinação de eventos desse tipo; nesse momento o vírus causa todo o estrago que seu autor programou para fazer.

Dessa forma, seu computador pode ser contaminado por um vírus hoje e só perceber as conseqüências meses depois, quando o vírus, por exemplo, formatar o seu disco rígido. Eis um exemplo hipotético: seu computador pode ter sido contaminado por um vírus que só ataca nos dias 13 que caírem em uma sexta-feira (só para lembrar: existem dois vírus com tal data de ataque – Jerusalém e NXeram) e você nunca liga o micro nessas datas. Então, talvez nunca saberá da existência nem conhecerá as conseqüências do ataque de tais vírus.

Assim, seu computador pode ser contaminado 365 dias do ano e só em uma determinada situação atacado pelo vírus. Isso não quer dizer que você não deva se preocupar com a situação – lembre-se que muitos novos vírus aparecem constantemente. Portanto, é bom estar preparado todos os dias do ano, com um eficiente antivírus, que seja permanentemente atualizado, para poder achar e eliminar os velhos e os novos tipos dessas criaturas, criadas para matar.

Tipos de vírus

Alguns vírus são tão ousados e agressivos que destroem completamente todas as informações no sistema. Por outro lado, outros vírus são totalmente inócuos – reproduzem-se, contaminam sistemas e não têm nenhuma outra função. Os vírus inócuos não causam danos, não apresentam mensagens na tela e não interferem no funcionamento normal do sistema. Esses vírus só querem morar no seu disco.

Entre o inerte e o agressivo, existem milhares de outros tipos de vírus concebidos por pessoas perversas, mas criativas e até originais em alguns casos. Para efeito de classificação, resolvemos dividir os vírus em quatro categorias, que relacionamos a seguir:

- **Boato** – Os *Hoax Virus* (ou como revela a tradução desse nome: Vírus Boato) não são vírus na verdade, nem Cavalos de Tróia nem nada – apenas o mais puro boato. A intenção é clara. Transmitir e causar pânico entre os usuários novatos, ou que não conhecem detalhes verídicos sobre métodos de funcionamento e ataque dos verdadeiros vírus de computador. Adicionalmente, por incentivarem os receptores dos e-mails a retransmitir os e-mails falsos para todos os amigos e conhecidos, causam um grande tráfego, e conseqüente congestionamento na rede. Os sinais típicos desses e-mails (sempre os *Hoax*

Vírus são transmitidos por e-mail) são, basicamente, os seguintes:

1. sempre chegam por e-mail;
2. sempre têm dizeres como “Jamais abra (ou leia) um e-mail com o texto ...”;
3. sempre informam que o vírus causa “grandes estragos – em geral, dizem horrores sobre as conseqüências físicas do seu ataque”;
4. o texto sempre solicita que você retransmita o e-mail para todos os amigos e conhecidos.

Só para fechar uma questão importante: vírus são programas de computador e como tal só podem agir no software, nunca poderão causar estragos ao hardware (o micro, o disco rígido, os drivers, o mouse – isto é o mais ridículo !! – o vídeo, o teclado etc.). Não há a mais remota possibilidade prática de que problemas – a não ser a perda de dados e/ou programas ou lentidão no sistema – possam aparecer como conseqüência da ação de um verdadeiro vírus de computador.

- **Inócuo** – Esses vírus se instalam nos discos e disquetes, mas não causam nenhuma perturbação ao sistema, apenas contaminam disquetes e outros tipos de mídia digitais que venham a ter contato com eles. A contaminação se dá de maneira que não há corrupção de programas ou dados; o vírus inócuo evita qualquer interferência com os processos normais executados no PC.
- **Humorístico** – Esses vírus geralmente apresentam uma mensagem ou imagem gráfica humorística na tela do PC. Alguns perturbam o usuário com eventos agravantes, mas nenhum efeito destrutivo sobre programas e dados. O vírus humorístico é concebido como se fosse uma anedota e não pretende causar danos ao sistema. No pior caso, esse vírus causa uma interrupção ou travamento do sistema operacional e sua remoção é geralmente simples e rápida.
- **Boot** (Vírus de Setor de *Boot*) – Vírus de *Boot* são o tipo de vírus mais comum entre todos os vírus existentes no mundo. Tudo que é preciso para se infectar com este tipo é simplesmente esquecer um disquete contaminado dentro do driver A. Esse disquete não precisa ser do tipo que dá *boot*, na verdade quando você vir a mensagem que o disco está sem sistema já é tarde demais, seu micro já está contaminado. Para contrabalançar, os vírus de *boot* são os mais fáceis de pegar, e eliminar.
- **Programa** – Vírus de Programa existem aos milhares e normalmente infectam os arquivos com extensão .EXE e .COM. Alguns contaminam arquivos com outras extensões, tais como .OVL e .DLL, que, na verdade, são executáveis, mas de um tipo um pouco diferente. Os mais bem escritos dentre os vírus de programa se “replicam” e contaminam outros arquivos, de maneira silenciosa, sem jamais interferir com a execução dos programas que estão contaminados. Assim, os usuários não vêem nenhum sinal exterior do que está acontecendo em seu micro. Alguns dos vírus de programa vão se reproduzindo até que uma determinada data, ou conjunto de fatores, seja alcançada. Aí começa o que importa: eles destroem algo em seu micro. Muito embora os vírus de programa não sejam tão difíceis de pegar, os danos que causam são, muitas vezes, de impossível recuperação, já que partes inteiras dos programas acabam corrompidos pelos vírus. Assim, em geral a única alternativa é reinstalar os aplicativos contaminados desde os discos originais, e reconfigurá-los.

- **Multipartite** (ou Polimórficos) – Os vírus desse tipo são, na verdade, uma mistura dos tipos de vírus *boot* e de vírus de programas. Eles infectam ambos – arquivos de programas e setores de *boot* –, o que os torna muito mais eficazes na tarefa de se espalhar e contaminar outros arquivos e/ou discos e também mais difíceis de serem detectados e removidos. Devido à enorme disputa entre os que escrevem os vírus e os que desenvolvem antivírus, a tendência é de que os vírus tentem ficar cada vez mais camuflados a ponto de poderem passar despercebidos para os produtos antivírus. Foi assim que surgiram os vírus chamados de polimórficos, cuja principal característica é estar sempre em mutação. Essa permanente mutação tem como objetivo alterar o código do próprio vírus, o que dificulta bastante a ação dos antivírus que, em geral, caçam os vírus por meio de uma assinatura digital que sabem ser parte integrante de um determinado vírus. Nesses casos, como o código do vírus se altera a cada infecção, dificilmente os programas antivírus atualizados reconhecerão as novas formas dos velhos vírus.
- **Stealth** (Invisíveis) – Mais uma variação sobre o mesmo tema. Desta vez os vírus que trazem a característica de *stealth* têm a capacidade de, entre outras coisas, temporariamente se auto-remover da memória, para escapar da ação dos programas antivírus. Note bem: os vírus do tipo polimórfico ou do tipo *stealth* são, na verdade, espécimes que se enquadram em um dos já descritos, e esses adjetivos, utilizados para descrever capacidades adicionadas aos mesmos para que sejam os mais discretos possíveis – o que impede, ao máximo, a sua detecção pelos programas antivírus.
- **Macro** – O advento dos vírus de macro – ocorrido pela primeira vez em 1995, com o ataque do vírus Concept, que se esconde em macros do programa de processamento de textos Microsoft Word – trouxe novas preocupações aos usuários do computador tipo PC. Tal advento forçou-os (e aos administradores) a fazer rápidas mudanças nos métodos até então utilizados para detecção de vírus. O conceito por trás dos vírus de macro é, na verdade, bastante simples. Muitas aplicações permitem a inclusão de programas simples, chamados de macros, dentro de arquivos de dados. Assim como essas aplicações evoluíram, tais linguagens de macros se tornaram incrivelmente poderosas e permitiram que os programadores que trabalham com tais macros possam fazer quase de tudo – por exemplo, chamar internamente um outro aplicativo diferente; apagar ou alterar outros arquivos; copiar ou criar outros arquivos. Com 70 a 100 tipos de comandos embutidos na linguagem de macros dos pacotes mais vendidos no mercado, tais comandos permitem executar ações diversas, e poderosas, sem necessitar de nenhuma interferência do usuário. Atualmente alguns pacotes (de programas) do mercado estão suscetíveis ao ataque desse tipo de vírus, entre eles o Word e o Excel. Entretanto, praticamente 95% dos casos que têm sido reportados referem-se a ataques nos arquivos do Word.

Para entender com um pouco mais de profundidade como funcionam tais tipos de vírus, vamos examinar alguns detalhes do primeiro vírus descoberto, que se utilizava deste conceito de contaminação: o vírus *WinWord* Concept, também conhecido por Concept: ao carregar um arquivo do Word, seja pelo comando Arquivo e Abrir, seja pelo duplo clique sobre um arquivo .doc, o Word inicia um processo

de abertura e carregamento que começa pelo exame do tipo de documento que está carregando. Se o arquivo for do tipo documento, o Word abre-o pronto para iniciar o processo de edição. Se, entretanto, o documento for do tipo modelo (*template*), o Word carrega todas as macros existentes nesse modelo. Se tal modelo contiver uma macro denominada *AutoOpen*, o conteúdo dessa macro é automaticamente executado. O vírus Concept aproveita-se dessa habilidade do software e acrescenta algumas macros a arquivos já existentes. Essas macros, uma vez instaladas, podem acrescentar novas funcionalidades à operação da barra de menus e permitem que o vírus infecte outros documentos existentes na máquina. A macro *AutoOpen* certamente não é a única opção disponibilizada para os programadores para a execução automática de certas rotinas dentro do ambiente Word. Outros tipos de macros, dentro do Word, trazem vantagens aos programadores para a execução de suas necessidades ou vontades. Embora o vírus Concept não contenha uma rotina do tipo *trigger* (disparo/gatilho), o vírus contém dentro de si as palavras *That's enough to prove my point* (“Isso é o bastante para provar meu ponto de vista”). O seu autor quer dizer com isso que se quisesse poderia fazer outras coisas (na verdade, qualquer coisa). O vírus Concept e seus pares tornam-se cada vez mais vírus com alto grau de disseminação devido ao seu meio de contaminação. Enquanto os usuários só raramente trocam programas ou dão *boot* em seus micros por meio de disquetes, a imensa maioria troca entre si seus arquivos de texto – seja para que os outros possam ler e/ou imprimir em suas próprias máquinas, seja para que outros possam colaborar na preparação de seus documentos. Com a ajuda das redes locais e da Internet, tais trocas se fazem, hoje, com muito maior facilidade e velocidade. O futuro dos vírus do tipo macro portanto é certo: cada vez mais eles participarão dos ataques às nossas máquinas. E com a expansão geométrica do poder das novas aplicações, com certeza, em breve, suplantarão os demais na destruição dos nossos dados.

Mandamentos antivírus

O ambiente sem vírus é similar ao ambiente estéril que as equipes médicas estabelecem antes de realizar uma cirurgia. Uma vez estabelecido, é preciso garantir que tudo que seja trazido para dentro do ambiente estéril também seja esterilizado. Conheça os “10 Mandamentos Antivírus”, extraídos da revista *INFO* que garantem ótima proteção para o seu micro pessoal ou para sua rede.

1. Nunca dispense a proteção do antivírus – Com a rápida proliferação do vírus e a facilidade na criação dos vírus de macro, não dá mais para arriscar e achar que incêndio só ocorre na casa do vizinho. Conte com a proteção de um antivírus e esforce-se para mantê-lo sempre atualizado.
2. Verifique todos os disquetes – Não esqueça que os destrutivos vírus de *boot* disseminam-se via disquetes contaminados. Assegure-se de que seus disquetes estão sadios e não introduza disquetes não rastreados nos seus drivers.
3. Mantenha cópias de segurança – Fruto de trabalho criativo, os dados armazenados no seu disco rígido representam horas e horas de árdua dedicação, que podem ser danificados em segundos pela ação de um vírus. Não se esqueça de fazer *backups* desse patrimônio.
4. Não utilize programas de origem desconhecida – Programas distribuídos de mão em mão passam por muitos equipamentos antes de chegar a você. Portanto, eles são naturalmente suspeitos.

5. Utilize somente programas originais – Estes têm procedência conhecida. Mesmo assim, deve-se manter os disquetes protegidos contra gravação.
6. Não inicialize o sistema a partir de disquetes desconhecidos – Nunca esqueça que um grande número de vírus invade seu sistema por meio de um *boot* ou uma tentativa de *boot* com disquete infectado. Guarde seu disco de *boot* sadio e devidamente protegido contra gravações para situações de emergência.
7. Não dispense a proteção antivírus na rede – Do ponto de vista da contaminação, a Internet ainda é considerada um meio muito pouco seguro. Por isso, não navegue sem proteção de vírus.
8. Verifique arquivos baixados de sites suspeitos – Junto com a Internet e demais serviços *on line*, este conjunto deverá representar 70% das contaminações de vírus. Assim, verifique todos os arquivos baixados antes de utilizá-los.
9. Rastreamento periódico – Se o seu antivírus não contém a função de verificação automática, como o ScreenScan do VírusScan para Windows 95, crie o hábito de rastrear seu sistema várias vezes ao dia. Afinal, como diz o ditado, o seguro morreu de velho.
10. Na dúvida, pare tudo – Em caso de suspeita de infecção, suspenda a operação e entre em contato com o suporte técnico.

Por que os vírus são e sempre serão um problema

A maioria das pessoas acredita que a ameaça, representada pelos vírus de computador, é uma coisa sem importância. “O simples ‘escaneamento’ de alguns arquivos uma vez por mês é suficiente para não ter de se preocupar novamente até o próximo mês”. É, seria muito bom se fosse verdade. Porém, a cada dia que passa, novos vírus aparecem e muitas variantes – em geral mais daninhas que seu original – surgem diariamente, e cada vez em maior quantidade.

A cada geração de vírus, novas técnicas de “criptação”, ou invisibilidade, são desenvolvidas e um pacote de um bom antivírus pode, do dia para a noite, virar algo completamente imprestável. Todos temos de estar permanentemente alertas para cobrir pelo menos três áreas:

1. Evitar a entrada de vírus em nossas máquinas.
2. Checar a existência de vírus em hibernação em nossos discos.
3. Atentar para indícios que exteriorizem os tipos de sinais de infecção e/ou ataque dos vírus mais conhecidos.

Cobertas essas três áreas, temos de garantir pelo menos três ações:

1. Atualizar os arquivos de dados dos nossos antivírus, pelo menos uma vez a cada dois meses.
2. Possuir pelo menos um antivírus de reconhecida eficácia.
3. Não ler um disquete ou se conectar a um *driver* de rede local sem antes “escaneá-lo”, usando os recursos máximos que seu melhor programa antivírus permita.

Vários sinais são típicos de ataque, ou de simples presença, de um vírus, sendo os principais os seguintes:

- Várias palavras de seu texto mudaram subitamente de lugar.

- Um arquivo cresceu de tamanho de um dia para outro.
- Seu computador começou a ficar muito lento e você instalou apenas um joguinho hoje.
- Você não consegue mais dar *boot* pelo seu disco rígido.
- Metade dos seus arquivos anda sumindo misteriosamente.
- Você acaba de receber “Parabéns a você” de um indivíduo autodenominado Joshi.

Talvez possa existir uma causa mais natural para esses problemas e muitos outros problemas estranhos, tais como problemas de configuração, erros de leitura/escrita em disco etc. Talvez, porém, seja melhor confiar em um profissional tarimbado ou então comprar um bom pacote antivírus. Mas de qualquer modo, aja logo, senão...

Os vírus de computador são tão citados em filmes, jornais e revistas especializadas que, de tanto ouvir falar sobre eles, começamos a não dar mais a devida atenção ao problema. Não faça isso!

Os vírus são coisas reais – como já mencionamos, na verdade são pequenos programas de computador – que podem trazer um dano irreversível aos seus dados e às vezes à sua carreira. Devido às explosões no uso de redes locais e, mais recentemente, da Internet, a disseminação de tais tipos ocorre de maneira extremamente rápida, e alcança muitos micros em curto espaço de tempo.

Se você tiver sorte, quem sabe apenas perderá alguns minutos – ou poucas horas – para eliminar completamente um vírus. Caso, entretanto, você pegue um vírus “ruim”, então seus dados podem ficar irremediavelmente perdidos no limbo. Só para ficar em um único exemplo: se você pegar o vírus *One Half* (Metade, em inglês), o vírus vai gradualmente – e muito sutilmente – “encriptando” o conteúdo de seu disco rígido dia a dia e sempre “decriptando” em *real-time* quando você quiser ler um arquivo já “encriptado”. Até que, um certo dia, a contaminação atinja metade de seu disco rígido; aí então o *One Half* pára de “desencriptar” seus arquivos (você já não pode ler nada que há nesses arquivos) e, em seguida, ele torna seu disco rígido não “bootável”!

Características dos principais vírus

Na tabela abaixo, apresentamos as características dos principais vírus conhecidos. Esta tabela não pretende esgotar o assunto, já que, como dissemos, vários vírus novos aparecem todo mês. Portanto, não se espante se um vírus que não esteja listado na tabela atacar seu microcomputador.

TIPOS DE VÍRUS MAIS FREQUENTES			
TIPO DE VÍRUS	MÉTODO DE INFECÇÃO	VÍRUS MAIS CONHECIDOS	COMO EVITAR TAL VÍRUS
Vírus de <i>Boot</i>	A partir de um <i>boot</i> feito com um disquete contaminado, que tenha sido deixado no drive A:	AntiCMOS AntiEXE Form.A Leandro & Kelly NYB (New York Boot) Ripper Satria.A Stealth_C Stoned Michelangelo	Use um antivírus com um detector de ação de vírus. Não deixe disquetes no drive A:. Altere o SETUP para o micro dar <i>boot</i> na seqüência C:, A:.

TIPOS DE VÍRUS MAIS FREQUENTES			
TIPO DE VÍRUS	MÉTODO DE INFECÇÃO	VÍRUS MAIS CONHECIDOS	COMO EVITAR TAL VÍRUS
Vírus de Programa	Ao rodar um programa do disco rígido ou de disquete, que esteja contaminado	Alevirus.1613 Athens (Atenas) FroDo.4096 Junkie Jerusalem Joshi	Rode o antivírus sempre que receber um novo programa. Use um antivírus com um detector de ação de vírus. Nunca rode um programa compactado sem antes checar a presença de vírus dentro do arquivo compactado.
Vírus de Macro	Ao executar uma macro num processo de texto (do tipo Word, o mais comum dos aplicativos atacados) ou mesmo apenas abrir um documento que possua uma macro do tipo "Auto Open".	MDMA.C Bad Boy Concept Hare.7610 Helper Pathogen Wazzu	Rode o antivírus sempre que receber um novo documento (principalmente se for do tipo Word). Use um antivírus com um detector, residente na memória, de ação de vírus. Sempre cheque TODOS OS ARQUIVOS de qualquer disquete recebido (ou e-mail ou Download pela Internet).
Vírus Multipartite	A partir de <i>boot</i> feito com um disquete contaminado no drive A:, ou ao rodar um programa que esteja contaminado.	One Half Junkie Natas Parity Boot VCL	Faça como apontado nas opções <i>Vírus de Boot</i> e <i>Vírus de Programa</i> , já que este tipo de vírus ataca dessas duas maneiras.

Alternativas para conexão com a Internet

A utilização pedagógica da Internet pelos NTEs (Núcleos de Tecnologia Educacional) e as escolas participantes do Proinfo é considerada de vital importância para esse projeto de introdução da telemática na Educação, conforme claramente definido em diversos documentos, principalmente no das “Diretrizes do Proinfo”. Como decorrência disso, a interligação dos NTEs e escolas à Internet torna-se imprescindível. O Proinfo, por meio de projeto específico, estuda e planeja alternativas técnicas para a construção de uma Rede Nacional de Informática na Educação (RNIE), projeto de grande envergadura, que deverá ser operacionalizado ao longo do ano de 1999.

Considerando que muitos NTEs e escolas podem estar pensando em se antecipar à implantação da RNIE, de forma a garantir o seu acesso à Internet, procuramos identificar alternativas técnicas para a conexão entre as escolas e a Internet que possam servir de orientação para as Comissões Estaduais de Informática na Educação, as equipes dos NTEs e as escolas.

A conexão entre a escola e a Internet pode ser efetuada de diversas formas, utilizando uma ampla gama de tecnologias que variam desde a telefonia fixa (a mais comum e mais adotada atualmente), passando pela telefonia móvel até a tecnologia de satélites.

Importante: queremos destacar que estas alternativas não são definitivas, uma vez que as tecnologias associadas à Internet estão em constante evolução e modificação.

A CONEXÃO

Computadores isolados ou ligados por uma rede local de computadores (LAN) podem interligar-se à Internet por meio de conexões discadas ou dedicadas, o que possibilita o acesso completo e/ou permanente aos seus recursos e serviços.

A conexão discada permite acesso à Internet através da rede pública de telefonia (IP discado) em qualquer velocidade até 56 Kbps. Em geral, o serviço de conexão discada é usado por usuários remotos que queiram conectar seus micros através de discagem por uma linha telefônica comum. É indicado para aplicações de baixo tráfego e de acesso esporádico.

A conexão dedicada permite a interligação de redes locais à Internet, por meio de uma linha privada dedicada, em velocidades de até 2 Mbps. O serviço de conexão dedicado atende a mais de um usuário e exige que o serviço de linha dedicada seja contratado de uma concessionária telefônica.

As conexões dedicadas são indicadas para usuários de todos os portes que têm a intenção de prover acesso interno aos seus empregados/clientes por meio da rede corporativa; ou que desejam montar serviços de informação (*information providers*) e criar uma presença institucional na Internet; ou, ainda, que queiram transformar-se em provedores de serviços de conexão (*Internet Service Providers* – ISP), fornecendo conexão à Internet para terceiros, através de sua própria rede.

OS PROVEDORES DE SERVIÇO INTERNET-ISP – INTERNET SERVICE PROVIDER

Um ISP é uma organização que provê acesso à Internet para usuários externos, doravante referidos como “clientes” neste documento. Seus serviços são voltados para os usos pessoal e comercial da Internet. O ISP possui infra-estrutura de comunicação, recursos de software, recursos de hardware e comunicação de dados e pode oferecer aos clientes diferentes classes de serviços.

A maioria dos clientes conecta-se ao ISP através de um modem – que pode ter diferentes velocidades de acesso (ex. 14 Kbps, 28 Kbps, 33 Kbps ou 56 Kbps) – e da infra-estrutura de comunicação entre o cliente e o ISP oferecida pelas companhias telefônicas, por meio das tradicionais linhas telefônicas.

A comunicação do ISP com a Internet é feita por meio de links, que também podem ter velocidades diversas. Esses links são alugados das concessionárias telefônicas e são implementados por meio de diferentes tecnologias (par trançado, fibra óptica, link de rádio, satélite etc.).

A figura 15 mostra um esquema típico de interconexão de clientes e um ISP e entre o ISP e a Internet. Portanto, para que haja o acesso à Internet, sempre é necessário uma conexão entre o cliente (usuário) com o ISP e entre o ISP com a Internet. Enquanto a conexão do cliente ao ISP pode variar entre permanente (acesso dedicado) e eventual (acesso discado), a conexão do ISP à Internet precisa, obrigatoriamente, ser permanente.

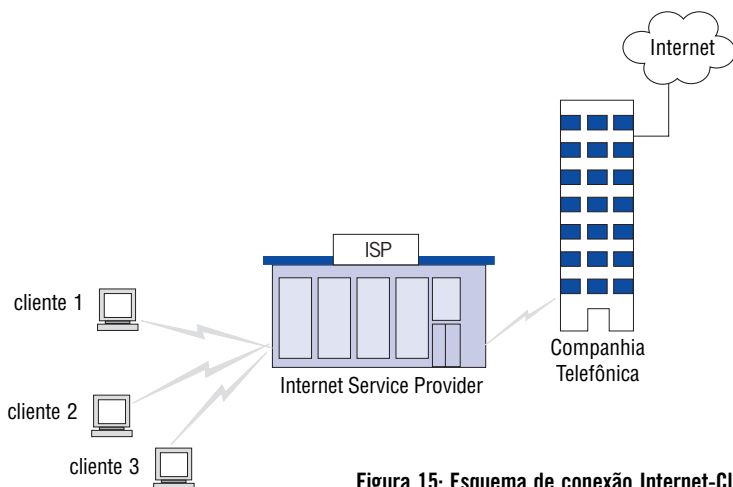


Figura 15: Esquema de conexão Internet-Cliente x ISP – Internet

Para garantir a estabilidade e a qualidade do acesso dos seus clientes à Internet, o ISP necessita de uma infra-estrutura de hardware, software e de uma estrutura permanente de recursos humanos para manter os diversos serviços que proporciona aos clientes – que podem ir além do simples acesso ao suporte aos serviços de lista, desenvolvimento e hospedagem de páginas *web*, serviços de acessos a banco de dados, rotinas de segurança e, principalmente, suporte à utilização.

Salientamos que não há possibilidade de conexão à Internet sem que o cliente faça uso dos serviços de um ISP, que fornece a infra-estrutura computacional e de serviços para o acesso. Esse destaque está sendo feito porque normalmente dá-se mais atenção aos diferentes meios que um cliente pode usar para acessar seu ISP, esquecendo-se de que a capacidade e a qualidade de serviços do ISP é o que realmente importa.

Nas seções seguintes são apresentadas várias possibilidades para conectar um cliente ao seu ISP e as alternativas para conectar um ISP à Internet.

ALTERNATIVAS PARA CONEXÃO DA ESCOLA AO ISP

Todos os levantamentos de valores, citados apenas a título de exemplo, foram coletados em dezembro de 1998 no Estado de São Paulo, onde a equipe de autores está baseada.

Via linha discada a um ISP comercial

No caso de conexão Internet via ISP, as escolas precisam ser assinantes de um ISP (“ter uma conta”) e dispor de uma linha telefônica comum de boa qualidade.

Quadro 1 – Exemplos de custos de provedores de acesso – ISP (dados dezembro de 1998)

PROVEDOR	OBSERVAÇÕES	CUSTO	
UOL - Universo Online http://www.uol.com.br/	Nas cidades onde o Universo Online ainda não provê acesso à Internet, o assinante pode navegar livremente mediante pagamento de taxa fixa mensal de R\$ 22,00	4 horas	R\$ 9,95
		10 horas	R\$ 22,00
		30 horas	R\$ 40,00
		120 horas	R\$ 59,00
ZAZ http://www.zaz.com.br	Possui tarifas diferenciadas por cidade. Na coluna ao lado estão os preços para a cidade de São Paulo	10 horas	R\$ 25,00
		20 horas	R\$ 35,00
		30 horas	R\$ 50,00
		50 horas	R\$ 75,00
		100 horas	R\$ 90,00
SOL - SBT on line http://www.sol.com.br		Oferece a opção de acesso limitado por R\$ 35,00 mensais com direito a navegação pela Internet e uso de correio eletrônico ou apenas uso do correio eletrônico por R\$ 5,00 mensais.	
ORIGINET http://www.originet.com.br	Uso no período das 2 às 6 horas (120 horas de acesso grátis) Atende as cidades de São Paulo, São José dos Campos e Campinas. Na coluna ao lado estão os preços para a cidade de São Paulo	10 horas	R\$ 20,00
		15 horas	R\$ 25,00
		25 horas	R\$ 40,00
		40 horas	R\$ 50,00
		60 horas	R\$ 56,00
CORREIONET http://www.correionet.com.br	Atende as cidades de Campinas, Americana, Itu, Itapira e Valinhos. Preços praticados nessas cidades, vide coluna ao lado	10 horas	R\$ 22,00
		18 horas	R\$ 30,00
		27 horas	R\$ 45,00
		sem limite de horas	R\$ 70,00
BLV - Bauru on line http://www.blv.com.br	Atende a cidade de Bauru (SP)	10 horas	R\$ 9,90
		20 horas	R\$ 14,90
		50 horas	R\$ 19,90
		sem limite de horas	R\$ 34,90

Quadro 2 - Tarifas das ligações locais aplicadas pela Telesp (fonte: <http://www.telesp.com.br>)

TARIFAS DAS LIGAÇÕES LOCAIS APLICADAS PELA TELESP (ATUAL TELEFÔNICA)
Pulso (excedente à franquia de 90 pulsos) = R\$ 0,08
Dias úteis (das 6:00 às 24:00 horas) e sábados (das 6:00 às 14:00 horas):
1 pulso: quando a chamada for completada
1 pulso: entre 0 e 4 minutos (aleatório)
1 pulso: a cada 4 minutos excedentes
Segunda a sábado: da 00:00 às 6:00 horas; Sábado: das 14:00 às 24 horas; Domingos e feriados nacionais: o dia todo.
1 pulso por chamada, independentemente do tempo de conversação.

Simulação de custos para utilização da Internet de 100 horas por mês

Situação 1 (assinatura residencial) – Uma chamada local em horário comercial com duração de 5 horas corresponde a 76 pulsos. Supondo-se que ao longo do mês sejam realizados 20 acessos de cinco horas, seriam consumidos 380 pulsos mensais. Veja Quadro 3.

Quadro 3 – Custos envolvidos na Situação 1

ITEM	CUSTO
Pulsos locais: 380 - 90 (franquia) = 290 * 0,08	R\$ 23,20
Mensalidade do provedor (preço médio)	R\$ 61,00
valor total mensal	R\$ 104,93

Situação 2 (assinatura comercial) – Uma chamada local em horário comercial com duração de duas horas corresponde a 31 pulsos. Supondo-se que ao longo do mês sejam realizados 50 acessos de 2 horas, seriam consumidos 1.550 pulsos mensais.

Quadro 4 – Custos envolvidos na Situação 2

ITEM	CUSTO
Assinatura de conta não residencial	R\$ 20,73
Pulsos locais 1.550 - 90 (franquia)= 1.460 *0,08	R\$ 116,80
Subtotal	R\$ 119,53
Mensalidade do provedor (preço médio)	R\$ 61,00
Valor total mensal	R\$ 180,53

Compartilhando uma conexão via linha discada entre vários usuários

A conexão via linha discada é normalmente utilizada por usuários individuais (um único micro). No caso das escolas, parece óbvio que se queira compartilhar uma única conexão física (uma ligação) entre os vários micros de uma rede local de computadores. Para que esse compartilhamento possa ocorrer, é necessário a instalação e configuração de programas especiais para o compartilhamento de conexão (estes programas são conhecidos como servidores *proxies* e os mais conhecidos no mercado são o Wingate, Ishare e o Microsoft Proxy Server). Os custos envolvidos nesse tipo de conexão são mostrados nos Quadro 5.

Quadro 5 – Custos envolvidos em uma conexão ISP via linha discada para 10 usuários

ITEM	CUSTO
Instalação e configuração do Wingate	R\$ 200,00
Configuração dos micros da rede	R\$ 250,00
Software Wingate 2.1 Lite (10 usuários)	R\$ 279,00
Valor total inicial	R\$ 729,00
Valor total mensal	Depende do tempo de utilização

Via linha discada de voz

Uma outra opção de acesso à Internet via ISP é por meio de uma linha dedicada de voz. Diferente do acesso discado, em que o cliente “liga” para o ISP e concorre com outros usuários-clientes ao serviço de acesso, o acesso por meio de linha dedicada permite uma conexão privativa de 24 horas/dia entre o cliente e o ISP. As principais vantagens desse tipo de conexão são: a disponibilidade do serviço (serviço sempre disponível), fácil acesso (não é preciso concorrer com os outros usuários para estabelecer uma conexão) e custo mensal fixo independentemente do nível de utilização.

Essa opção utiliza um modem comum (que funcione em linha privativa) e uma linha dedicada de voz. O Quadro 6 apresenta um exemplo de custos envolvidos na instalação e operação de uma linha dedicada de voz entre o cliente e o ISP. Os recursos de hardware e software são semelhantes aos utilizados no Quadro 5.

Quadro 6 – Custos envolvidos em uma conexão ISP via linha privativa de voz

ITEM	CUSTO
Custos iniciais	
Instalação e Configuração do Wingate	R\$ 200,00
Configuração dos micros da rede (por micro)	R\$ 25,00
Software Wingate 2.1 Lite (10 usuários)	R\$ 279,00
Valor total inicial	R\$ 647,00

ITEM	CUSTO
Custos mensais	
Mensalidade LP Voz Telesp	R\$ 89,00
Mensalidade ISP para acesso 24 h	R\$ 280,00
Total total mensal	R\$ 369,00

Todas as concessionárias de telecomunicações oferecem o serviço de linha dedicada de voz, normalmente uma linha telefônica analógica privativa, destinada ao transporte de voz para uso geral. Embora não seja uma solução ideal para a transmissão de dados, o custo mais baixo dessa opção, torna-a atraente para soluções de transporte de dados que não tenham necessidade de altas velocidades de transmissão (taxas máximas de 55,6 Kbps). Salientamos que, para grupos pequenos de usuários Internet (máximo de 15), essa solução pode ser considerada bastante adequada.

Existe ainda, a possibilidade de utilizar-se um tipo de modem especial, atualmente fabricado apenas pela *Boca Modem*, que utiliza duas linhas (dois pares de fios) e que pode atingir velocidades de transmissão de 110 Kbps. A principal dificuldade é a exigência de que o ISP tenha um modem idêntico correspondente.

Via linha dedicada de dados

Esta conexão, devido ao seu desempenho, é indicada para um número grande de microcomputadores em rede. Geralmente, contrata-se o serviço de uma concessionária de telecomunicações para fazer a ligação dedicada entre o cliente e o ISP. Essa opção utiliza modems especiais e um serviço de dados das concessionárias de telecomunicação.

Quadro 7 – Custos em uma conexão ISP via linha dedicada de dados a 64 Kbps

ITEM	CUSTO
Custos iniciais	
Roteador com uma porta síncrona (preço médio)	R\$ 3.600,00
Instalação/Configuração do roteador	R\$ 850,00
Configuração do ambiente operacional do ISP	R\$ 650,00
Configurações dos equipamentos do cliente (por estação)	R\$ 25,00
Instalação de uma LP (linha privativa) de dados 64 Kbps	R\$ 1.253,69
Valor total inicial	R\$ 6.378,69
Custos mensais	
Mensalidade da LP de dados 64 Kbps	R\$ 494,90
Mensalidade pelo acesso 64 K consumido do ISP	R\$ 700,00
Total mensal	R\$ 1.194,90

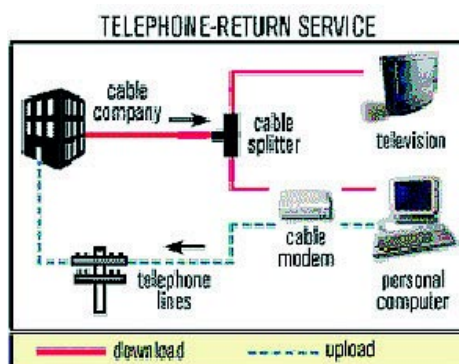
A conexão via linha dedicada de dados garante taxas maiores de comunicação e disponibilidade do serviço, entretanto requer maiores investimentos na infra-estrutura e maiores custos de manutenção. Basicamente, para operacionalizar esse tipo de conexão são necessários roteadores com pelo menos uma porta síncrona. Portanto, faz-se necessária a contratação de uma linha privativa de dados e de uma porta síncrona junto ao ISP.

No caso de uma linha dedicada de dados, existe a possibilidade de contratação de várias taxas: 64 Kbps, 128 Kbps, 256 Kbps, 512 Kbps, T1 (1Mbps) e E1 (2Mbps). Logicamente, a disponibilidade de velocidades acima de 64 Kbps depende da localidade onde se encontra o cliente. Normalmente, a taxa contratada pelos ISP é, em média, de 512 Kbps para atendimento de todos os seus clientes e, portanto, clientes interessados em contratar links com taxas superiores a 64 Kbps poderiam causar problemas de tráfego para o ISP.

Companhia de TV a cabo como ISP - acesso via cabo ou UHF/telefone

Em uma conexão por meio de companhia de TV a cabo, a recepção (*downlink*) é feita através de um *cable modem* conectado ao cabo coaxial da TV a cabo. O *cable modem* tem função similar ao do modem convencional de linha telefônica, mas através dos cabos coaxiais.

Os dados da Internet para o assinante (*downlink*) chegam por um dos canais de televisão – os sinais da Internet são transmitidos diretamente ao assinante a altas velocidades (27 Mbps). Os dados do assinante para a Internet (*uplink*) são feitos por intermédio de linhas discadas ou de linhas dedicadas.



Companhia de TV a cabo como ISP

Quadro 8 – Exemplos de provedores de acesso via cable modem ou UHF

PROVEDOR	OBSERVAÇÕES	CUSTO
Link Express http://www.linkexpress.com.br	Atende a cidade de Brasília por intermédio da operadora de TV por assinatura TV Filme	Taxa de inscrição: R\$ 66,00 Mensalidade: R\$ 35,00 - sem limite de horas
Interlink http://www.interlink.com.br	Atende a cidade de Vitória por intermédio da operadora de TV por assinatura Vitória Vídeo Cabo (VVC)	Taxa de inscrição: R\$ 10,00 Mensalidade: R\$ 46,95 - sem limite de horas

No quadro 9 são mostrados os custos médios envolvidos no acesso à Internet via companhia de TV a cabo.

Quadro 9 – Custos envolvidos com conexão via companhia de TV a cabo

ITEM	CUSTO
Custo inicial	
Aquisição do Cable Modem	R\$ 548,00
Taxa de adesão	R\$ 38,00
valor total inicial	R\$ 686,00
Custo mensal	
mensalidade (acesso sem limite de horas)	R\$ 41,00
Valor total mensal	R\$ 41,00

Empresas de TV a cabo que utilizam a transmissão via radiofrequência (UHF) também se preparam para fornecer serviço de acesso à Internet. Nesse caso, o *uplink* se daria através de linhas telefônicas e o *downlink* via sinal de UHF, pela mesma antena já utilizada pelo usuário.

Destacamos dois pontos:

- a) esta modalidade de acesso está sendo oferecida apenas aos atuais clientes dos serviços de TV a cabo, não é oferecida de forma isolada;
- b) neste caso, a própria empresa de TV a cabo é que exerce o papel de ISP.

Mudança é a palavra de ordem na sociedade atual. A educação não pode ficar alheia. A inclusão da Informática na Educação deverá mudar a maneira como aprendemos e poderá ajudar a formar cidadãos críticos, criativos e preparados para a sociedade do conhecimento. Nosso desejo é que a Informática possa contribuir para a construção de um projeto de uma sociedade melhor para todos.

Preparação de ambientes informatizados nas escolas públicas

Esta obra orienta os professores-multiplicadores dos Núcleos de Tecnologia Educacional e os professores das escolas participantes do Proinfo sobre os principais aspectos técnicos e estruturais para a preparação e montagem dos ambientes de trabalho informatizados.

Apresenta os conceitos básicos sobre a preparação das salas, eletricidade, montagem de redes locais e os procedimentos de entrega dos equipamentos do Proinfo.