

Aula nº1 e 2

Unidade temática 2: Introdução ao Estudo dos Sistemas Operativos .

Sumário: Noção de Sistema Operativo.

SISTEMA OPERATIVO é um software de sistema, sendo portanto, um gestor dos um software de sistema, sendo portanto, um **gestor dos recursos** que compõem o computador :

e um escalonador de tarefas.

Partilha e protege os recursos a serem usados pelas aplicações do utilizador, servindo de interface entre este e a máquina. Partilha e protege os recursos a serem usados pelas aplicações do utilizador, servindo de interface entre este e a máquina.

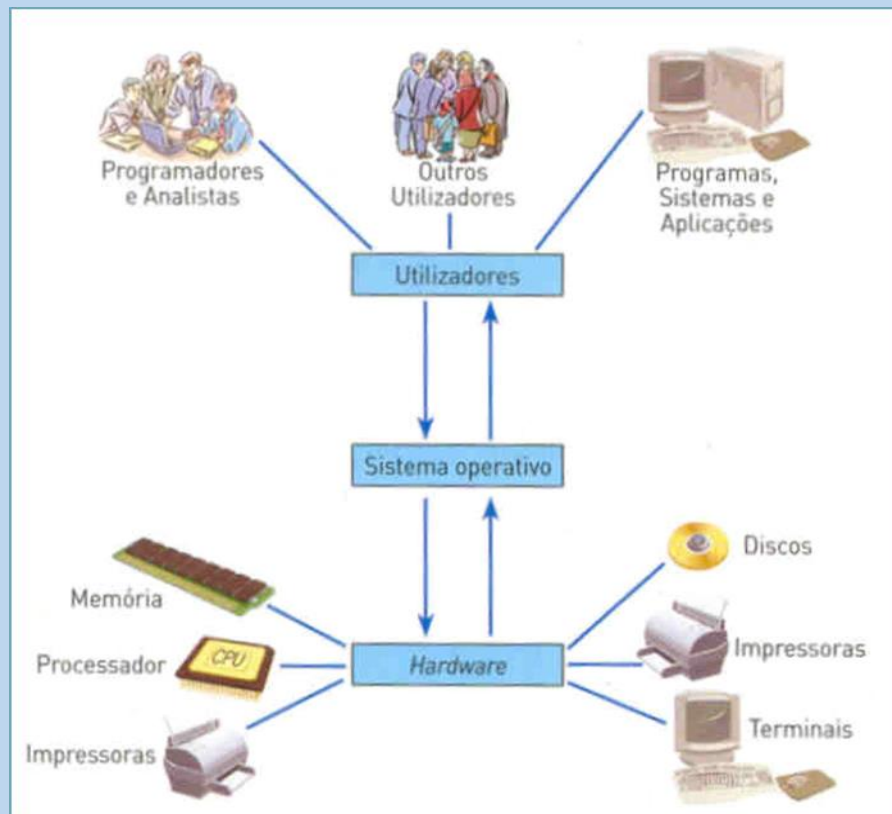
O sistema operativo deve:

fornecer a abstracção de hardware, isto é, apresentar ao utilizador uma máquina mais simples (máquina virtual);

funcionar em modo kernel ou modo supervisor, protegendo o hardware da acção directa do utilizador;

Estabelecer critérios de utilização dos recursos e a ordem de acesso dos mesmos;

Níveis que separam o hardware do utilizador



O sistema operativo deve:

- 1- fazer a gestão e protecção dos dispositivos;
- 2- fazer a gestão dos programas e distribuir memória para as aplicações;
- 3- Impedir a violação do espaço de memória reservado a um determinado programa (processo) e as tentativas de acesso simultâneo a um mesmo recurso;
- 4- Processar as mensagens internas para os dispositivos de I/O;
- 5- Fornecer um meio de comunicação entre o utilizador e o hardware

Unidade temática 2: Introdução ao Estudo dos Sistemas Operativos .

Sumário: Caracterização de um Sistema Operativo.

Evolução dos sistemas operativos

Os sistemas operativos têm evoluído devido à necessidade de gerir eficientemente estes equipamentos, através do controlo da execução dos programas dos diferentes utilizadores, efectuado, assim, a gestão dos recursos da máquina.

Ao servir de interface entre o utilizador e a máquina, faz com que esta, seja uma máquina virtual, cada vez mais simples e fácil de utilizar.

As funções principais de um sistema operativo

Partilha de recursos com protecção:

Físicos: processador, memória, discos, periféricos diversos.

Lógicos: programas de uso geral (editores, compiladores) e bibliotecas partilhadas por diversos programas.

Gestão da concorrência:

Controlar diversos fluxos de actividades que se executem “em paralelo”, sem que os mesmos interfiram não intencionalmente.

Gestão da informação persistente:

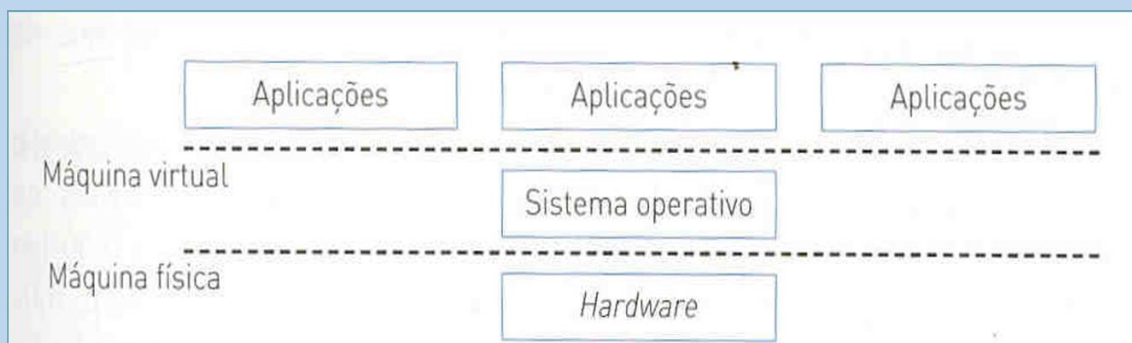
Armazenamento fiável e seguro da informação não volátil em suportes magnéticos, ópticos, etc.

Controlo dos gastos:

Contabilização e limitação da utilização dos recursos físicos.

Missão de um Sistema Operativo:

Criar uma máquina virtual sobre a máquina física que ofereça os recursos lógicos básicos necessários ao desenvolvimento das aplicações.



Unidade temática 2: Introdução ao Estudo dos Sistemas Operativos .

Sumário: Tipos de Sistemas Operativos.

Os principais :

Sistemas operativos para mainframes (Mainframe Operating System):

Para computadores de grande porte e orientado para o processamento simultâneo de inúmeras tarefas (muitas entradas e saídas). Ex: VM (virtual machine) para a família IBM 4341.

Sistemas operativos para servidores (Server Operating System):

Destinado a servidores de modo geral, que podem ser máquinas com grandes capacidades, workstations ou mesmo mainframes. Servem múltiplos utilizadores da rede e permitem a partilha de hardware ou de outros recursos (software, ou serviços).

Sistemas operativos para Multiprocessadores (Multiprocessor Operating System):

Para computadores (várias CPU) que formam um único sistema, dependendo da forma como estão ligados e do que é partilhado, denominam-se computadores paralelos, multicomputadores ou multiprocessadores. Podem ser variação de sistemas operativos para servidores com características especiais de conectividade. (neste grupo incluem-se os SO distribuídos).

Sistemas operativos para Computadores Pessoais (Personal Computer OperatingSystem):

Tem por objectivo servir de interface para um único utilizador. Largamente utilizados para tarefas comuns : processamento de texto, acesso a internet .

Sistemas operativos de Tempo Real (RTOS) (Real Time Operating System):

É uma aplicação multitarefa na qual várias tarefas críticas devem ser processadas em simultâneo. O sistema deve assegurar que as tarefas sejam tratadas em tempo útil. Exemplos de implementação : controle de tráfego, processos de fábrica.

Sistemas operativos Embebidos (Embedded Operating System):

Para sistemas cada vez mais pequenos, como telecomandos, os telemóveis, os palmtops ou PDA (Personal Digital Assistant). Executam um reduzido conjunto de tarefas, tendo restrições de tamanhos, memória e de alimentação. Ex. Windows CE, Android, IOS (Consumer Electronics).

Sistemas operativos para Smart Card (Smart Card Operating System):

São os SO mais pequenos, que são executados em cartões de créditos contendo pequenas CPU. Tem grandes restrições de processamento e pouca memória.

Alguns sistemas deste tipo executam apenas uma tarefa (pagamento electrónico), outros que permitem ainda a execução de outros tipos de tarefas (acesso a áreas reservadas).

Unidade temática 2: Introdução ao Estudo dos Sistemas Operativos .

Sumário: Estrutura dos sistemas operativos (Arquitetura dos Sistemas).

Na construção de um sistemas operativo observam-se, pelo menos dois tipos de requisitos:

Requisitos do utilizador – sistema fácil de utilizar e aprender, rápido e adequado às tarefas para as quais se destina.

Requisitos de software – manutenção, forma de funcionamento, restrições de utilização, eficiência,tolerância aos erros e flexibilidade.

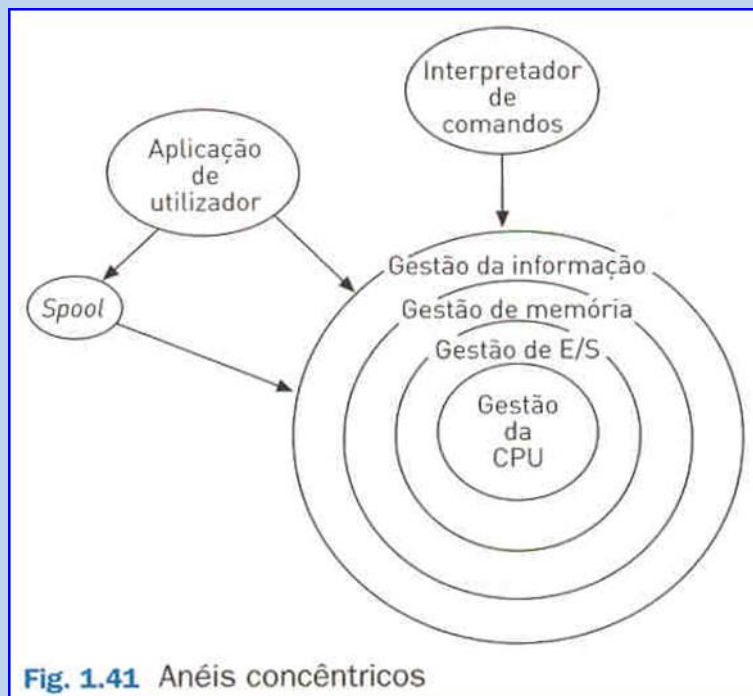
Quanto a forma podem ter a seguinte estrutura: Monolítica, Hierárquica, Máquina virtual, Cliente-servidor.

SO Monolítico: Primeiros S.O, constituídos por um único programa, composto por várias sub-rotinas.

Carecem de protecções e privilégios ao executar as rotinas. São feitos à medida, pelo que são eficientes e rápidos na execução e gestão, mas pouca flexibilidade para suportar diferentes ambientes de trabalhos ou aplicações.

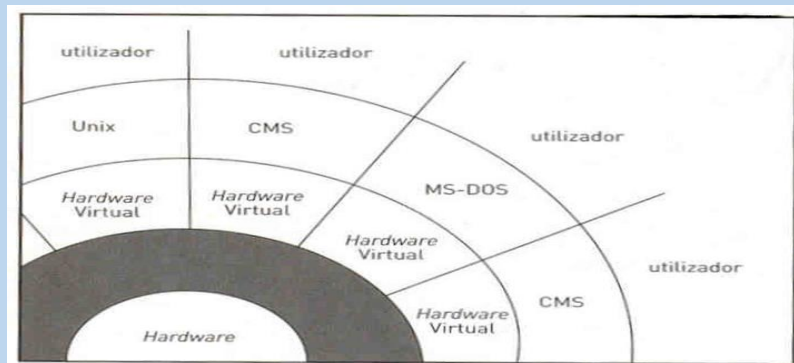
SO Hierárquico ou de níveis: Parte do sistema operativo contém outras subpartes, organizadas em forma de níveis. Ou seja, dividiu-se o SO em pequenos blocos muito bem definidos, com uma interface clara.

A maior parte dos SO actuais baseiam-se neste tipo de estrutura.



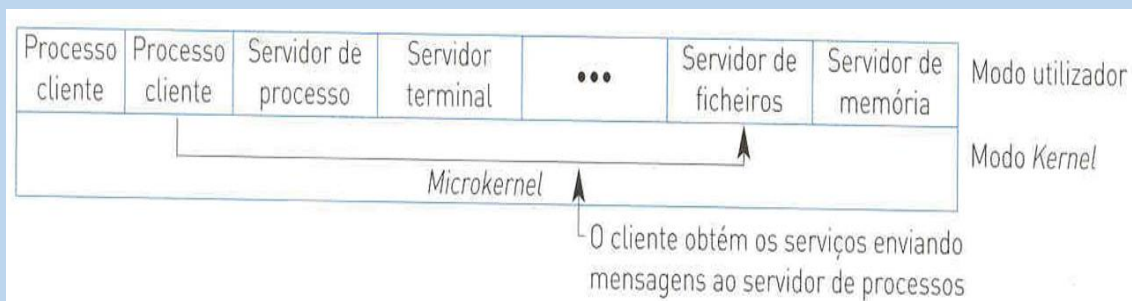
SO Máquina Virtual: Disponibiliza uma interface a cada processo, mostrando ao utilizador uma máquina idêntica ao hardware existente. O objectivo é o de integrar diferentes sistemas operativos, dá a sensação ao utilizador de várias máquinas diferentes.

O núcleo denomina-se Monitor Virtual, tem por objectivo a multiprogramação. Apresenta aos níveis superiores tantas máquinas quantas as solicitadas.



SO Cliente-Servidor: É um sistema operativo de propósitos gerais, servindo a todos os tipos de aplicações, cumprindo as mesmas funções dos sistemas operativos convencionais.

O núcleo tem como missão estabelecer a comunicação entre os clientes e os servidores. Os processos podem ser tanto servidores como clientes.



SO Cliente-Servidor: Oferece uma grande flexibilidade aos serviços fornecidos ao utilizador final, uma vez que o núcleo serve apenas as funções mais básicas de memória, entrada/saída, ficheiros e processos, deixando para os servidores os outros serviços.

Os servidores devem ter mecanismos de segurança e de protecção.



Aula nº11 e 12

Unidade temática 2: Introdução ao Estudo dos Sistemas Operativos.

Sumário: Funções de um Sistema Operativo.

Processador: CPU (Unidade de Processamento Central), Gere todo o sistema computacional.

Principal Função: controlar e executar instruções presentes na memória principal. Composto por :

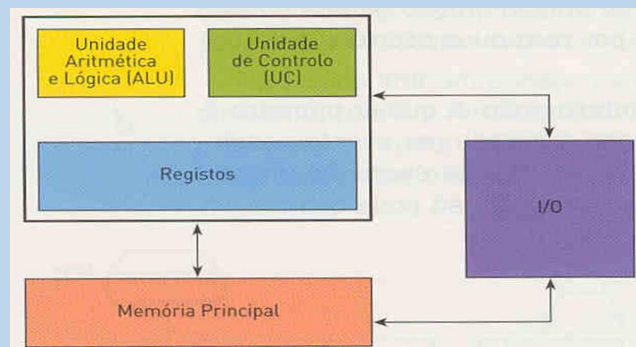
Unidade de Controlo: Gere as actividades de todos os componentes do Computador.

Unidade Aritmética e Lógica: Operações Aritméticas e lógicas.

Registos: Armazenam dados temporariamente. Memória interna do processador de alta velocidade.

Unidade de Processamento Central: Unifica todo o sistema, controlando as funções realizadas por cada unidade.

A CPU é responsável pela execução de todos os programas do sistema, que obrigatoriamente deverão ser armazenados na memória principal.



Um programa é composto por instruções, a CPU procura cada instrução na memória principal e interpreta-a para a sua execução.

Sistemas monoprogramáveis/Monotarefa: O processador, a memória e os periféricos exclusivamente dedicados à execução de um único programa. Enquanto um programa aguarda por um evento, o processador permanece sem realizar qualquer tipo de processamento. A memória é sub utilizada, caso não a preencha totalmente.

São simples de implementação, não existindo muita preocupação com problemas de protecção.

Organização da memória em sistemas Monoprogramáveis: Programa em utilização: Sistema Operativo na (RAM), Sistema Operativo na ROM: Programa em utilização, Device drivers (ROM): Programa em utilização, Sistema Operativo(RAM).

Sistema Operativo(RAM): Mais complexos e eficientes, permitem a partilha dos recursos

A partir do número de utilizadores que interagem com o sistema, podem classificar-se como monoutilizador ou multiutilizador.

Sistemas Multiprogramáveis/Multitarefa: Sistemas batch, Sistemas de tempo compartilhado, Sistemas de tempo real.

Sistemas multiprogramáveis/Multitarefa:

Mainframes e Minicomputadores – Multitarefa e Multiutilizadores Computadores Pessoais – Mutitarefa e Monoutilizador.

Caracterizam-se por permitir por que o utilizador, em simultâneo, edite um texto, imprima um ficheiro, copie um ficheiro pela rede e utilize uma folha de cálculo, etc. Ou seja é possível a execução de diversas tarefas concorrentemente ou mesmo simultaneamente.

Aula nº11 e 12

Unidade temática 2: Introdução ao Estudo dos Sistemas Operativos.

Sumário: Segurança nos Sistemas Operativos.

Possíveis ameaças à segurança da Informação.

- 1-Vírus;
- 2- Concorrência empresarial
- 3-Sabotagens internas
- 4- Internet

Objectivo da Segurança.

- 1-Detectar as vulnerabilidades dos sistemas
- 2-Proteger o tratamento de informação
- 3-Proteger as transacções de informação



Aspectos da Segurança.

Autenticação - Processo para validar a identidade de um utilizador.

Confidencialidade – Limita o acesso à informação apenas às entidades autorizadas (previamente autenticadas).

Integridade – Garante que a informação que vai ser armazenada é autêntica, ou seja, não é corrompida.

Controlo de acesso – Capacidade de impedir o acesso não autorizado a um determinado recurso.

Não repudição – São funções que impedem que uma determinada entidade negue a execução de determinada acção.(Comércio electrónica)

Disponibilidade – Procura garantir que, mesmo após um ataque a uma rede, os recursos chave ficam disponíveis para os utilizadores.

Tipos de Intrusos no sistema.

- 1-Intrusos ocasionais, com poucos conhecimentos técnicos
- 2-Intrusos internos, com conhecimentos técnicos
- 3-Indivíduos que pretendem obter ganhos com o ataque
- 4-Espionagem comercial ou militar.

Os vírus informáticos encontram-se noutra categoria da segurança, uma vez que é um código que, normalmente, se reproduz sozinho e provoca sempre algum dano.

Nem só as ameaças causadas por intrusos, são importantes. Existe outra a “PERDA DE DADOS”.

Erros de Software e Hardware:

Causados por:

- Discos avariados
- CPU avariados
- Erros de programas

Erros Humanos:

Causados por:

- Dados mal introduzidos
- Comandos mal dados

Fenómenos da Natureza:

Causados por:

- Incêndios
- Cheias
- Terramotos
- Guerras
- Motins

Tipos de Ameaças à Segurança

Acesso não Autorizado: Baseia-se na descoberta de logins e passwords de um dado utilizador que é posteriormente utilizado por outro para aceder aos recursos do primeiro.

Ataques por Imitação: Consiste em fazer com que um dados utilizador ou sistema se comporte como um outro. Spoofing attacks e Replay attacks.

Disrupção de Serviços: O objectivo é a interrupção ou a perturbação de um serviço devido a danos causados nos sistemas que o suportam. Podem ser danos físicos ou lógicos. (Denial of Service – DoS).

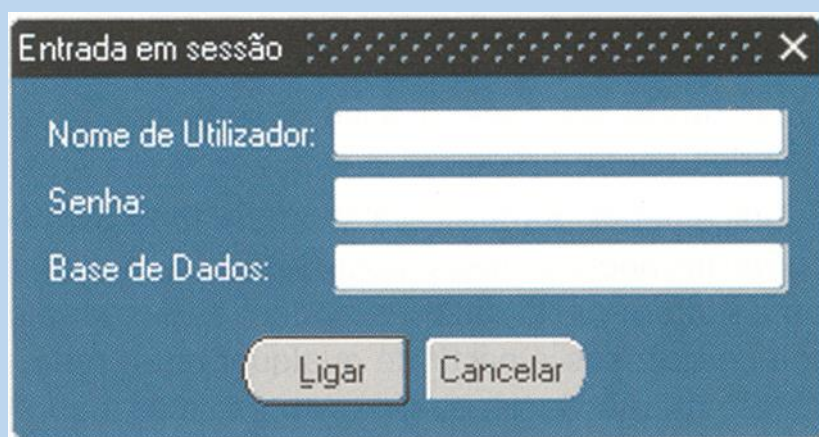
Mas, nem tudo está perdido...

Existem diversos tipos de FERRAMENTAS e MECANISMOS para proteger os sistemas ou detectar invasões Encriptação, Firewalls, Antivírus, Sistema de detecção de intrusão, Segurança Interna, Autenticação de Utilizadores, Assinatura Digital, Backup e Restore.

Autenticação de Utilizadores

Estabelecem a identidade de utilizador e/ou de sistemas, tendo em vista a determinação de acções e das capacidades permitidas. Permitindo desta forma que os utilizadores tenham tipos de acesso diferenciados aos recursos. Exemplo:

- Consultar certos ficheiros
- Imprimir para certas impressoras
- Não poder apagar ficheiros



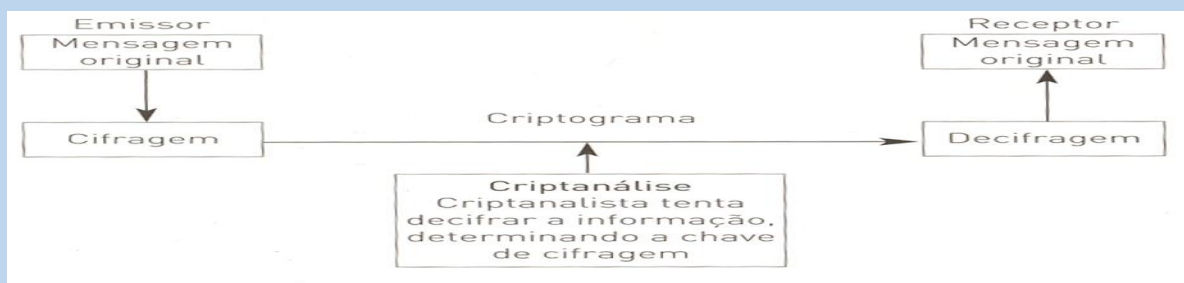
The image shows a classic Windows NT-style login dialog box. The title bar reads 'Entrada em sessão' with a close button (X) on the right. The dialog has a blue background. It contains three text input fields stacked vertically, each preceded by a label: 'Nome de Utilizador:', 'Senha:', and 'Base de Dados:'. At the bottom of the dialog, there are two buttons: 'Ligar' (Login) and 'Cancelar' (Cancel).

Formas de autenticação:

- Biométricos (Impressão digital, íris)
- Físicos (Smartcard)
- Passwords

Encriptação:

É um processo que modifica os dados através de uma chave secreta, conhecida somente por partes autorizadas. Ao processo de modificação da mensagem dá-mos o nome de cifragem transformando-a num criptograma. São normalmente funções matemáticas, sendo compostas por dois algoritmos o de cifragem e o de decifragem.



Firewalls:

É colocado na zona de fronteira e que tem como objectivo principal o controlo de acesso de utilizadores à rede, a partir de outras redes.

Por norma controlam os acessos a uma Intranet feitos a partir da Internet.

Só protege a rede dos ataques externos, não dos internos.



Assinatura Digital: Consiste num conjunto de dados encriptados associados a um documento. Garantem a integridade do documento ao qual estão associadas e a entidade de quem o envio. Não garantem a confidencialidade do documento ao qual estão associadas.

Sistemas de detecção de Intrusão:

São sistemas inteligentes, capazes de detectar tentativas de invasões em tempo real.

Não só detectam, como também podem aplicar acções contra o ataque. É necessário fazer uma actualização diária, uma vez que todos os dias surgem novos tipos de ataques. Outros há, onde são empregues técnicas de inteligência artificial, para que detectem sempre novos ataques.

Logs: São registos gerados pelos sistemas ou aplicações com informações dos eventos ocorridos. Dependendo do sistema e do hardware, a geração dos logs pode tornar-se lenta. Servem de prova contra um possível invasor detectado.

Antivírus:

Trata-se de um software que verifica a existência de vírus em computadores, pastas ou ficheiros e, ao encontrá-lo tenta removê-lo.

Numa primeira tentativa, apenas remove o vírus e, caso não o consiga, remove o ficheiro, depois da autorização do utilizador.

Fica carregado em memória, e quando detecta um vírus avisa o utilizador imediatamente.

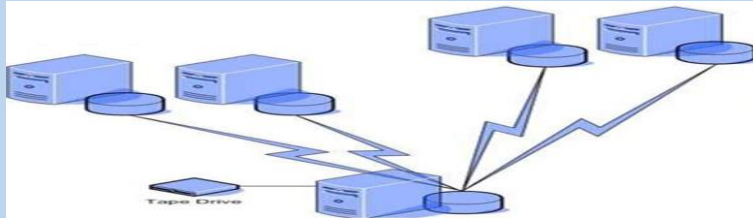
Deve-se actualizar semanalmente a base de dados do antivírus.



Backup e Restore:

Servem para fazer cópias de segurança de dados e programas.

A frequência dos Backups deve ser avaliada pelo administrador do sistema, com base na velocidade de criação, modificação dos dados e programas.



Segurança Interna

Procura assegurar a confidencialidade e a integridade dos dados a partir dos acessos de dentro da rede.

Requer cuidados especiais, a “desconfiança” é a palavra de ordem, em relação aos utilizadores internos.

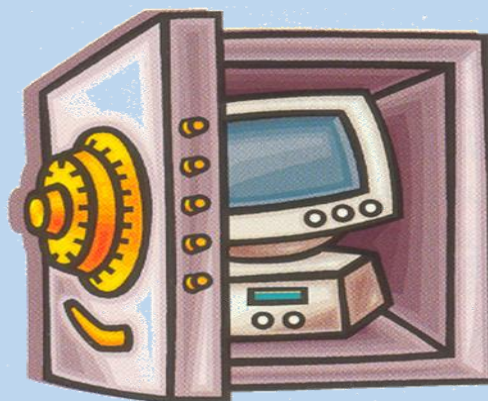
A maior parte das invasões partem do meio interno das organizações.

Políticas de Segurança

Uma política de segurança deverá ser técnica e organizacionalmente executável.

Deverá definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistema e do pessoal de direcção.

Deverá também ser flexível para se adaptar às alterações da organização.



Regras para definir Políticas de Segurança

Ser facilmente acessível a todos os membros da organização;

Definir objectivos de segurança;

Justificar as opções tomadas;

Definir os papéis dos diversos agentes da organização;

Especificar as consequências do não cumprimento das regras definidas;

Definir o nível de privacidade garantido aos utilizadores;

Identificar os contactos para o esclarecimento de dúvidas;

Definir o tratamento das situações de omissão;

O documento que define a política de segurança deverá deixar de fora todo e qualquer aspecto técnico de implementação do sistema de segurança.