



UNIDADE IV

Sistemas Operacionais Abertos e Mobile

Prof. Me. Michel Fernandes

Sistema de arquivos

Arquivos

- Constituídos por informações logicamente relacionadas e podem representar instruções ou dados.
- Os arquivos são gerenciados pelo SO de maneira a facilitar o acesso dos usuários ao seu conteúdo. A parte do SO responsável por essa gerência é o Sistema de Arquivos que é a parte mais visível do SO, pois a manipulação de arquivos é frequente.

Visões do sistema de arquivos

Visão do usuário:

- Como os arquivos são nomeados?
- Quais são as operações permitidas?
- Como o diretório é implementado?

Visão do implementador:

- Como os arquivos e diretórios são armazenados?
- Como o espaço em disco é gerenciado?
- Como tornar o sistema eficiente e confiável?

Organização de arquivos

- Consistem em como os dados são internamente armazenados e sua estrutura pode variar de acordo com o tipo de informação contida no arquivo.
- A forma mais simples de organizar é por meio de uma sequência não estruturada de bytes, em que o Sistema de Arquivos não impõem nenhuma estrutura lógica para os dados.
- A aplicação define toda a organização e critérios.
- Vantagens: flexibilidade para criar diferentes estruturas de dados.
 - As organizações mais conhecidas e implementadas são: Sequencial e a Indexada.

Operações de entrada e saída

- O Sistema de Arquivos disponibiliza um conjunto de rotinas que permite às aplicações realizarem operações de E/S, como tradução de nomes em endereços, leitura e gravação de dados, criação e eliminação de arquivos.
- As rotinas de E/S tem como função disponibilizar uma interface simples e uniforme entre a aplicação e os diversos dispositivos.

ROTINA	DESCRIÇÃO	ATRIBUTOS
CREATE	Criação de arquivos	São informações de controle de cada arquivo. Variam dependendo o Sistema de Arquivos, porém estes estão presentes em quase todos os sistemas: Tamanho, Proteção, Identificação do criador, Data da criação.
OPEN	Abertura de um arquivo	
READ	Leitura de um arquivo	
WRITE	Gravação de um arquivo	
CLOSE	Fechamento de um arquivo	
DELETE	Eliminação de um arquivo	

Tipos de arquivos

Arquivos regulares:

- São aqueles que contêm informações dos usuários.

Diretórios:

- São arquivos responsáveis por manter a estrutura do Sistema de Arquivos.

Arquivos especiais de caracteres:

- São aqueles relacionados com E/S e utilizados para modelar dispositivos seriais de E/S.
 - Ex.: impressora, interface de rede, terminais.

Arquivos especiais de bloco:

- São aqueles utilizados para modelar discos.

Métodos de acesso a arquivos

Dependendo de como o arquivo está organizado, o Sistema de Arquivos poderá recuperá-lo de diferentes maneiras:

- Acesso Sequencial – Utilizados para arquivos em fitas magnéticas e o acesso era restrito à leitura dos registros na ordem em que eram gravados e os novos registros eram gravados no final de cada arquivo.
- Acesso Direto – Surgiu com os discos magnéticos, permitia a leitura/gravação de um arquivos diretamente na sua posição, era realizado por meio do No. Do.
 - Acesso Indexado ou Acesso por chave – Tem como base o acesso direto. O arquivo deve possuir uma área de índice onde existam ponteiros para os diversos registros. Caso a aplicação deseje acessar um registro, deve especificar uma chave por meio da qual o sistema pesquisará na área de índice o ponteiro correspondente e assim é realizado um acesso direto ao registro desejado.

Estrutura de diretório

- É como o Sistema de Arquivos organiza logicamente os diversos arquivos contidos em um disco, onde armazena informações como: localização física etc.
- Quando um arquivo é aberto, o SO procura sua entrada na estrutura de diretórios, armazenando as informações sobre os atributos e a localização de um arquivo em uma tabela mantida na memória principal.
- A implementação mais simples de uma estrutura de diretórios é chamada de Nível Único, onde só existe um único diretório contendo todos os arquivos do disco.
 - É bastante limitado, pois não permite que os usuários criem arquivos com o mesmo nome, o que ocasionaria conflito no acesso aos arquivos.

Estrutura lógica de um diretório

A organização pode ser feita das seguintes maneiras:

- Nível único (Single level).
- Dois níveis (Two level).
- Hierárquica ou Árvore.
- Grafos.

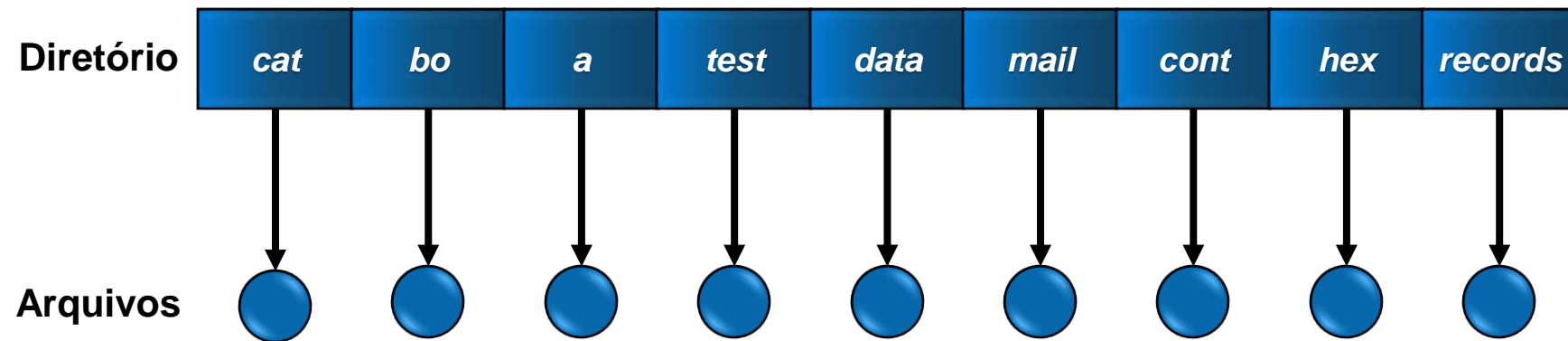
Estrutura lógica de um diretório

Diretório de um nível:

- Apenas um diretório contém todos os arquivos: diretório raiz ou root directory.
- Computadores antigos utilizavam esse método, pois eram monousuários.

Vantagens:

- simplicidade;
- eficiência.



Estrutura lógica de um diretório

Diretório de um nível:

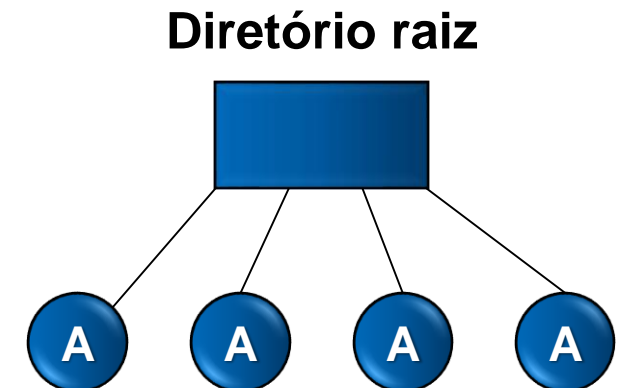
- 4 arquivos;
- três diferentes proprietários.

Desvantagens:

- Sistemas multiusuários: diferentes usuários podem criar arquivos como o mesmo nome.

Exemplo:

- Usuários A e B criam, respectivamente, um arquivo mailbox.
- Usuário B sobrescreve o arquivo do usuário A.



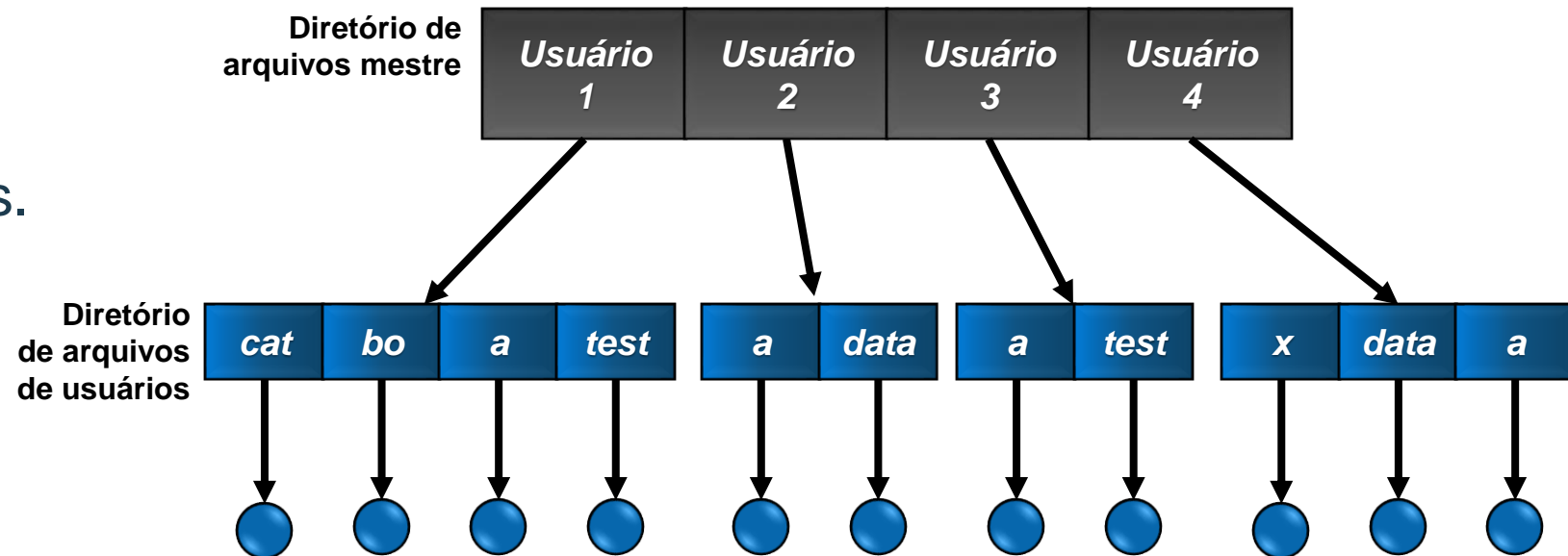
Estrutura lógica de um diretório

Diretório de dois níveis:

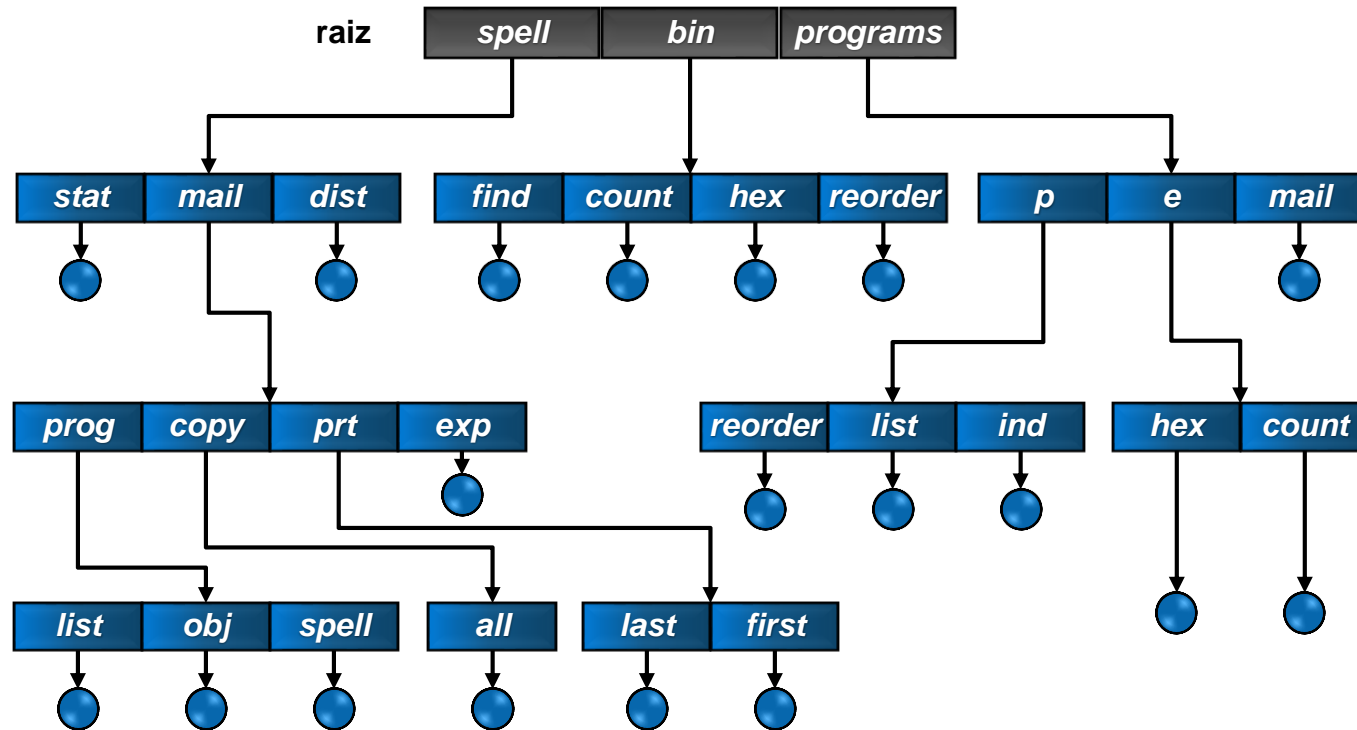
- Cada usuário possui um diretório privado.
- Sem conflitos de nomes de arquivos.
- Procedimento de login de identificação.
- Compartilhamento de arquivos.
- Programas executáveis do sistema.

Desvantagem:

- Usuário com muitos arquivos.



Estrutura lógica de um diretório



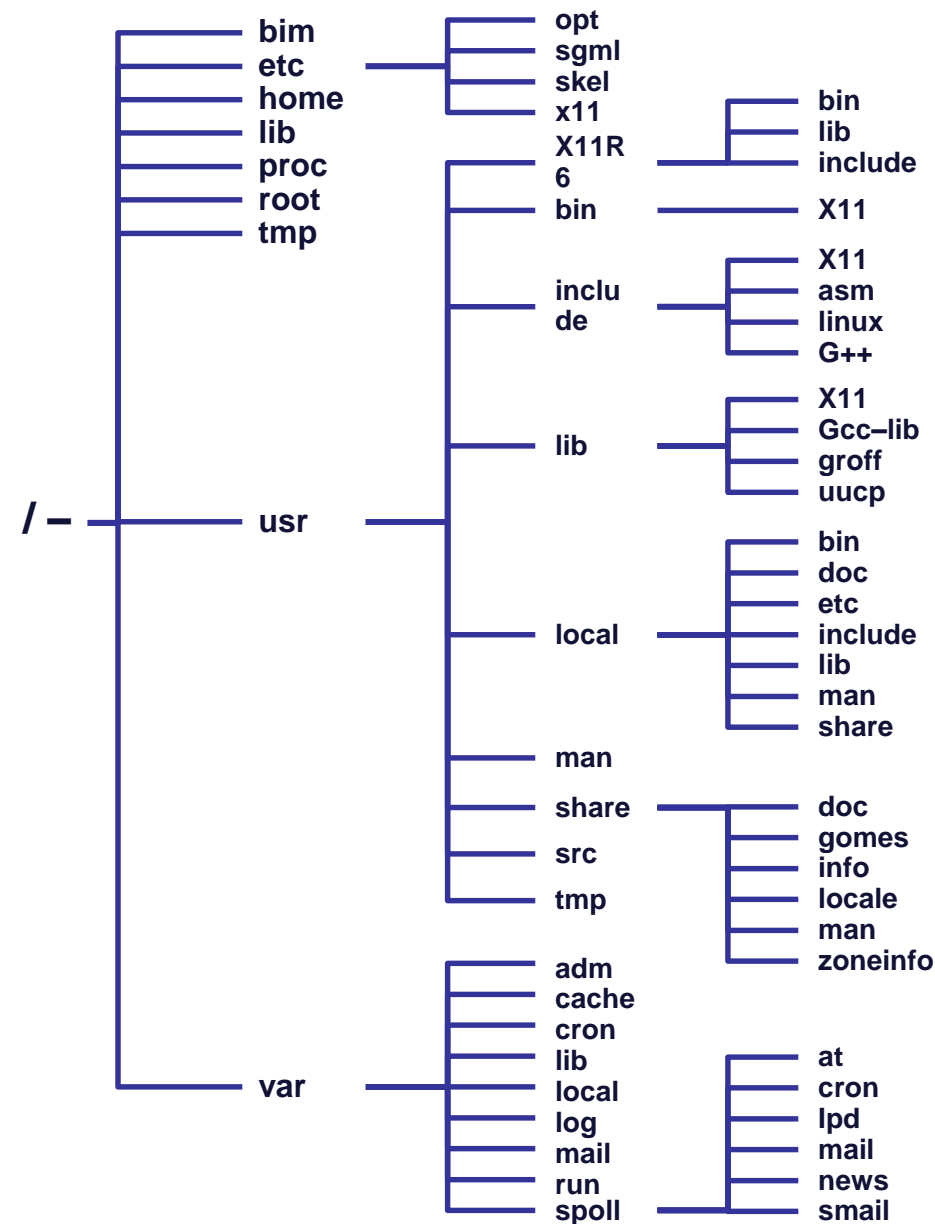
Fonte: adaptado de:
Silberschatz *et al*, 2015.

Diretório Hierárquico ou em Árvore:

- Hierarquia de diretórios → árvore de diretórios.
- Usuários podem querer agrupar seus arquivos de maneira lógica, criando diversos diretórios que agrupam arquivos.
- Sistemas operacionais modernos utilizam esse método.
- A árvore tem um diretório raiz e cada arquivo no sistema tem um nome de caminho exclusivo.
- Flexibilidade.

Estrutura lógica de um diretório

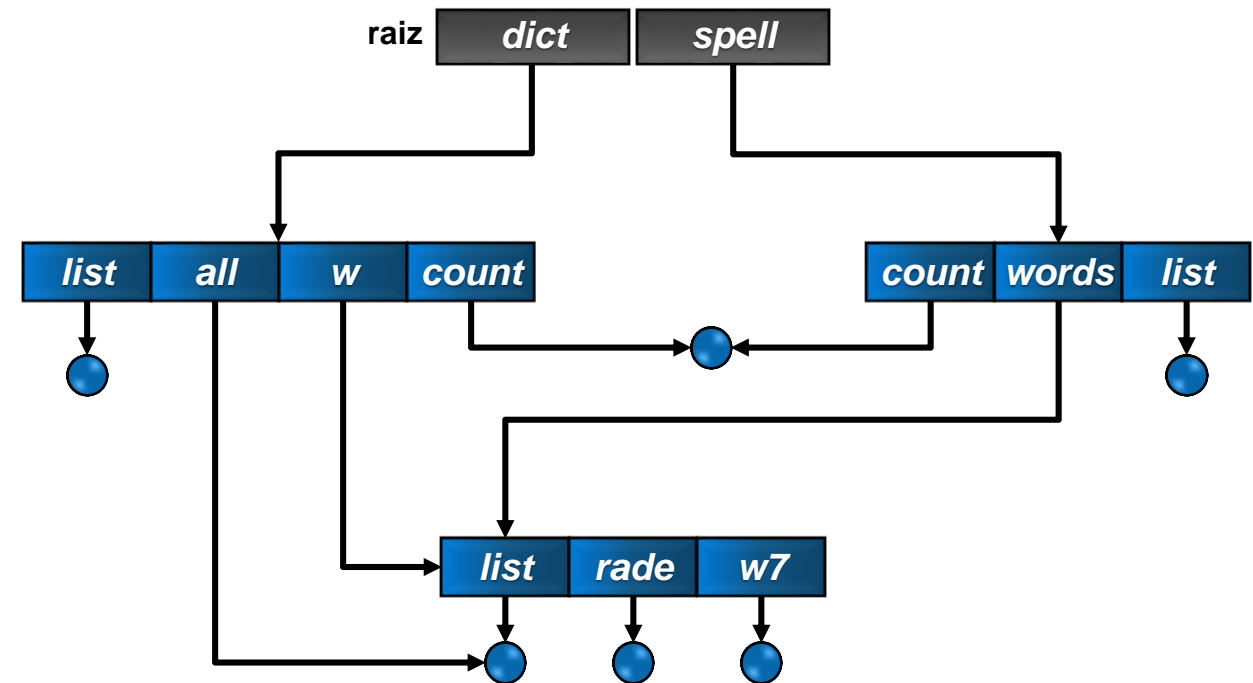
- A figura representa uma parte da árvore de diretórios típica de um sistema Linux, cuja estrutura é definida nas normas Filesystem Hierarchy.



Estrutura lógica de um diretório

Diretórios em Grafo:

- Um grafo acíclico permite que os diretórios compartilhem subdiretórios e arquivos.
- O compartilhamento é particularmente importante para os subdiretórios.
 - Um novo arquivo criado por uma pessoa aparecerá automaticamente em todos os subdiretórios compartilhados.



Interatividade

Sobre o sistema de diretórios hierárquicos, considere as seguintes afirmações:

- I. A árvore tem um diretório raiz e cada arquivo no sistema tem um nome de caminho exclusivo.
- II. Um diretório ou subdiretório contempla somente um conjunto de arquivos.
- III. Ao permitir que um usuário defina seus próprios subdiretórios, essa organização de diretórios possibilita que o usuário imponha uma estrutura aos seus arquivos.

É correto o que se afirma em:

- a) I, apenas.
- b) I e II, apenas.
- c) I e III, apenas.
- d) II e III, apenas.
- e) I, II e III.

Resposta

Sobre o sistema de diretórios hierárquicos, considere as seguintes afirmações:

- I. A árvore tem um diretório raiz e cada arquivo no sistema tem um nome de caminho exclusivo.
- II. Um diretório ou subdiretório contempla somente um conjunto de arquivos.
- III. Ao permitir que um usuário defina seus próprios subdiretórios, essa organização de diretórios possibilita que o usuário imponha uma estrutura aos seus arquivos.

É correto o que se afirma em:

- a) I, apenas.
- b) I e II, apenas.
- c) I e III, apenas.
- d) II e III, apenas.
- e) I, II e III.

Gerência de espaço livre em disco

- A forma mais simples de implementar uma estrutura de espaços livres é por meio de uma tabela denominada Mapa de Bits (BITMAP). Cada entrada na tabela é associada a um bloco do disco representado por um Bit, podendo assumir valor igual a 0 (bloco livre) ou 1 (bloco ocupado).
- Uma segunda maneira é encadear todos os blocos livres do disco, em que cada bloco possui uma área para armazenar o endereço do próximo bloco.
 - Outra solução leva em consideração que blocos contíguos são geralmente alocados e liberados simultaneamente, mantendo uma tabela com o endereço do 1º Bloco e o n. de blocos livres contíguos que seguem.

Gerência de alocação de espaço livre em disco

- Alocação contígua: armazena um arquivo em blocos sequenciais dispostos no disco. O sistema localiza um arquivo por meio do endereço do 1º bloco.
- Seu principal problema é a alocação de espaço livre para novos arquivos. Caso um arquivo deva ser criado com um determinado tamanho, é necessário existir uma quantidade suficiente de blocos contíguos no disco para a realização de alocação.

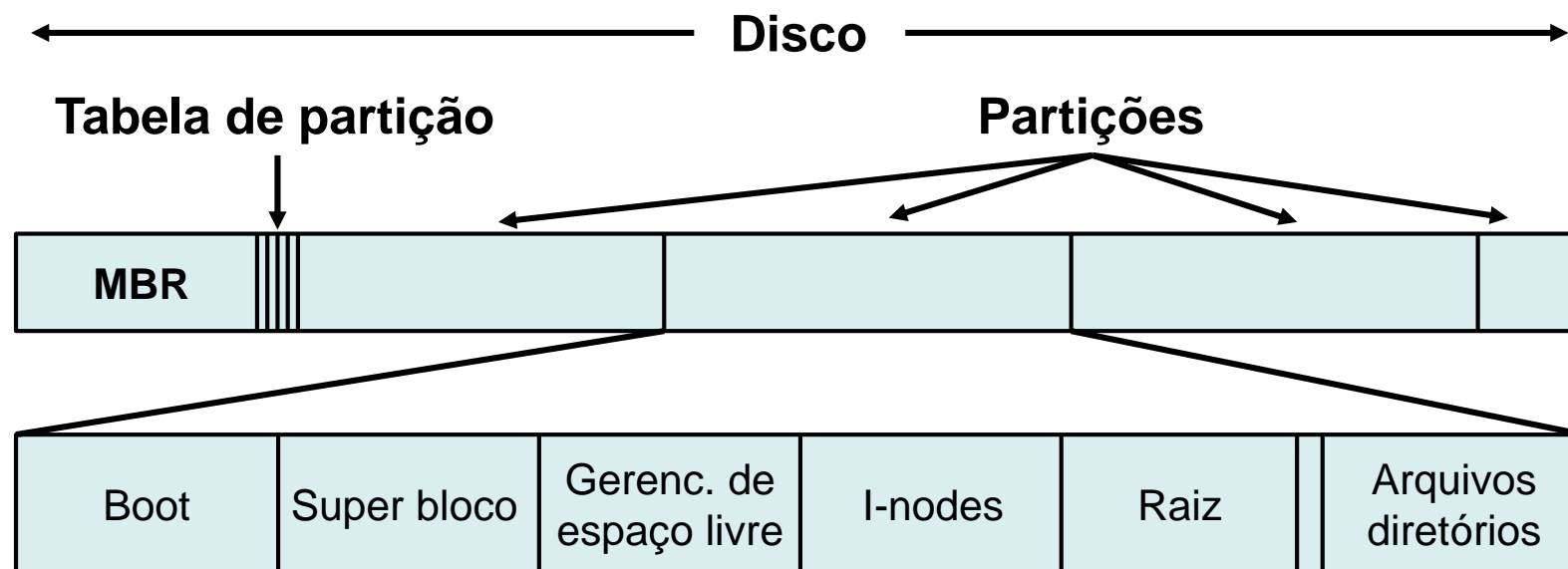
Existem estratégias de alocação para selecionar qual segmento será alocado:

- FIRST-FIT – O primeiro segmento livre com tamanho suficiente será alocado.
 - BEST-FIT – Seleciona o menor segmento livre disponível com tamanho suficiente para armazenar o arquivo.
 - WORST-FIT – O maior segmento é alocado. Entretanto, cria problemas de fragmentação do espaço livre.

Layout do sistema de arquivos

Arquivos são armazenados em discos.

- Discos podem ser divididos em uma ou mais partições, com sistemas de arquivos independentes.
- Setor 0 do disco é destinado ao MBR Master Boot Record que é responsável pela tarefa de boot do computador.
- MBR possui a tabela de partição com o endereço inicial e final de cada partição.
- BIOS lê e executa o MBR.



Layout do sistema de arquivos

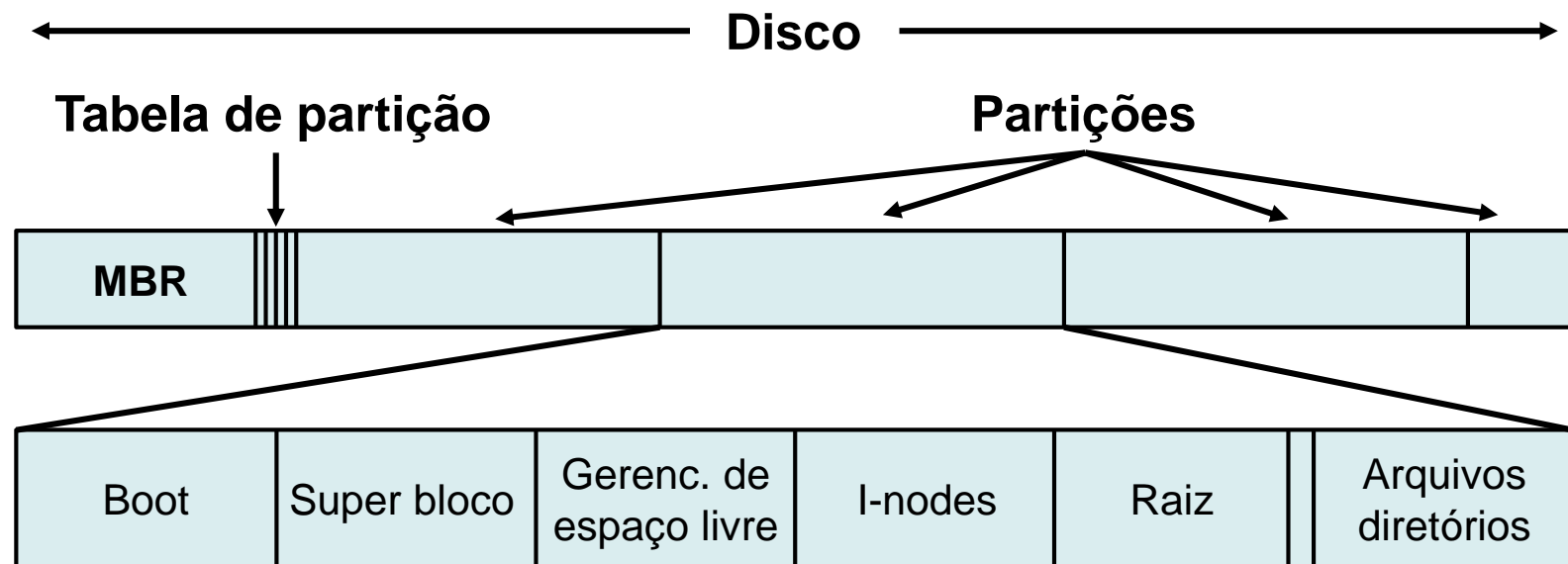
Programa na MBR

- Localiza a partição ativa.
- Lê seu primeiro bloco (bloco de boot).
- Executa esse bloco.

- Toda partição tem um bloco de boot.

Programa no bloco de boot:

- Carrega o SO daquela partição.



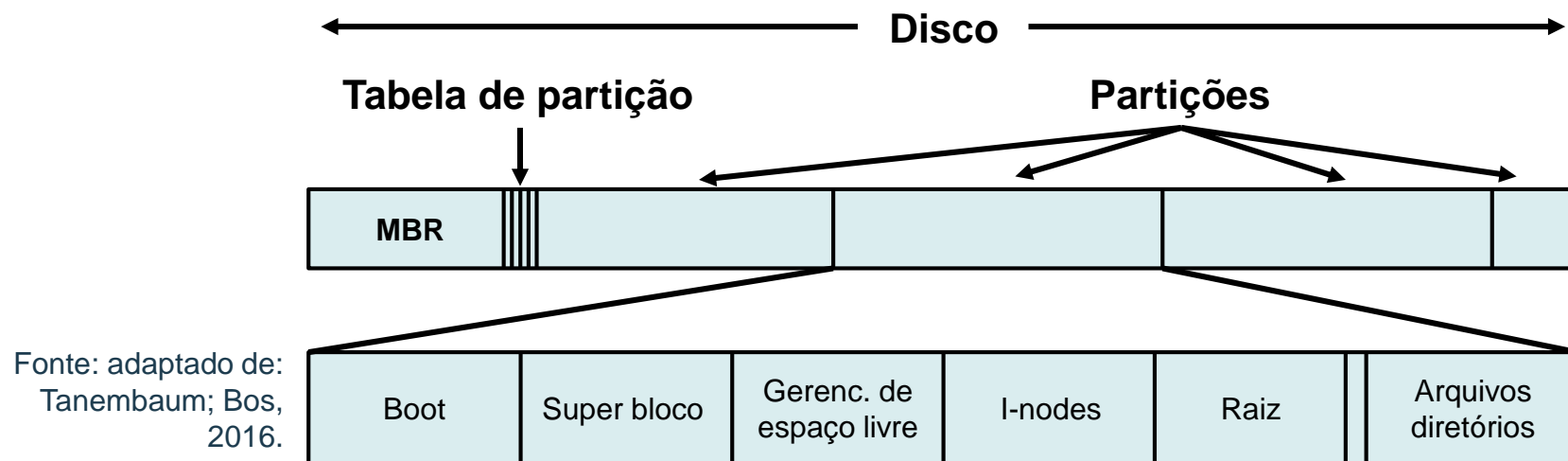
Layout do sistema de arquivos

Superbloco

- Contém parâmetros (tipo do SA, número de blocos, ID do sistema de arquivos) sobre o sistema de arquivos.
- Lido para a memória no boot ou quando o sistema de arquivos é manipulado pela 1ª vez.

Gerenciamento de espaço livre

- Contém informações sobre os blocos livres do disco (mapa de bits / *bitmap* ou lista encadeada).



Layout do sistema de arquivos

I-nodes

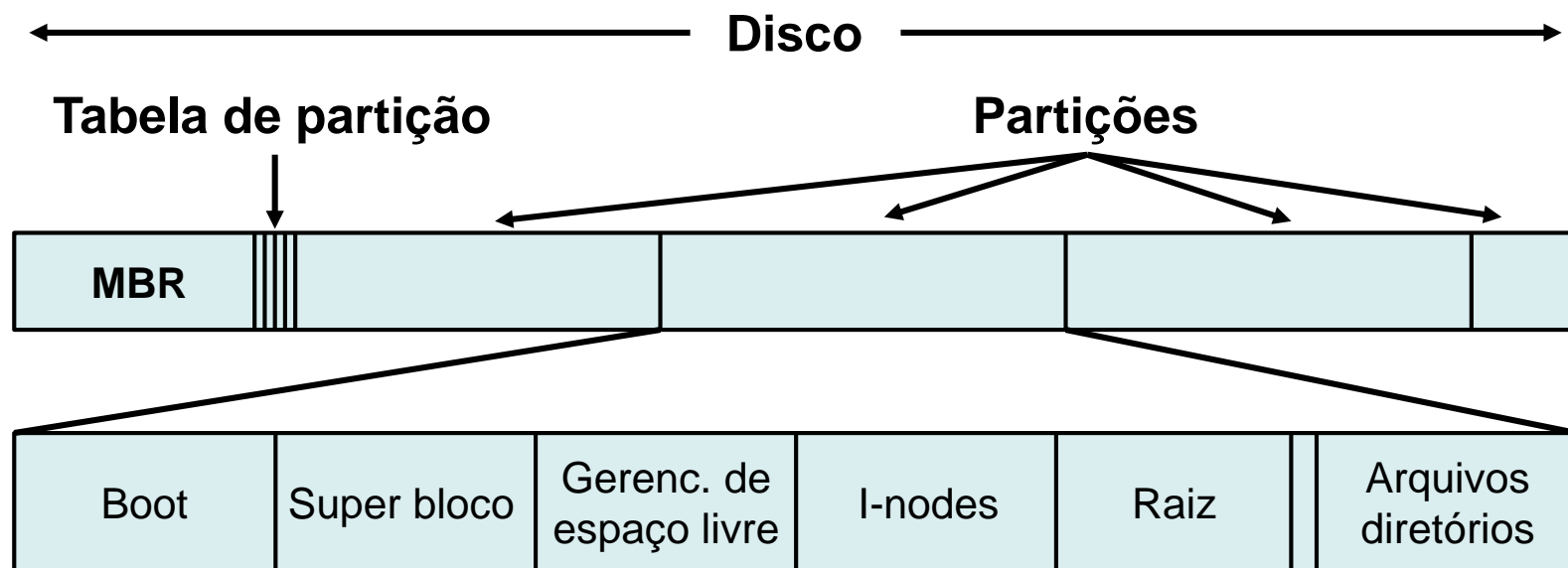
- Estruturas de dados (vetor) contendo informações sobre os arquivos.

Raiz

- Diretório raiz árvore de diretórios.

Arquivos diretórios

- Demais arquivos e diretórios.



Métodos de alocação de arquivos

Como os arquivos são alocados no disco?

Diferentes técnicas utilizadas pelos Sistemas Operacionais:

- Alocação contínua.
- Alocação com lista encadeada.
- Alocação com lista encadeada utilizando tabela na memória (FAT).
- I-Nodes.

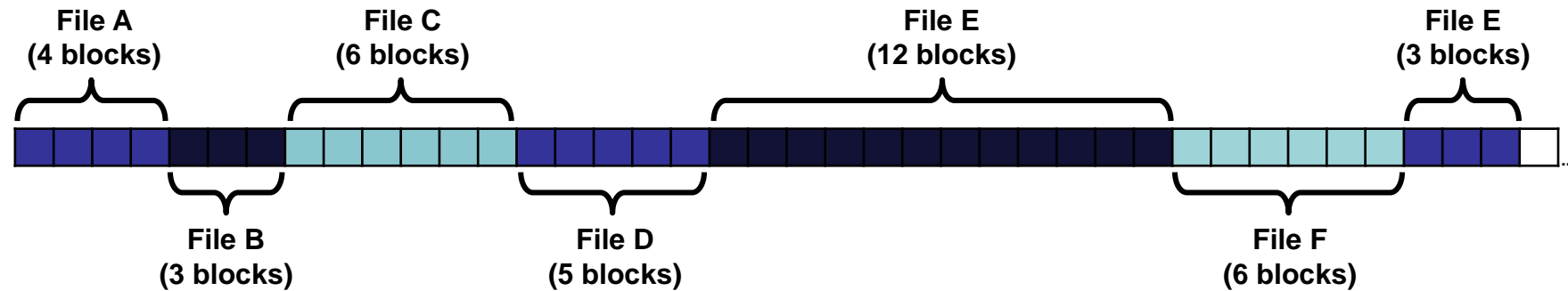
Métodos de alocação de arquivos – Alocação contínua

Método mais simples:

- Armazena arquivos de forma contínua no disco.

Exemplo: com blocos de 1 Kb, um arquivo de com 80 Kb:

- Será alocado em 80 blocos consecutivos.
- Utilizando inicialmente em HDs e, posteriormente, em CD-ROMs.



Métodos de alocação de arquivos – Alocação contínua

Vantagens:

Simples de implementar:

- Basta conhecer o endereço do 1º bloco e o número de blocos do arquivo para:
 - Saber onde está o arquivo.

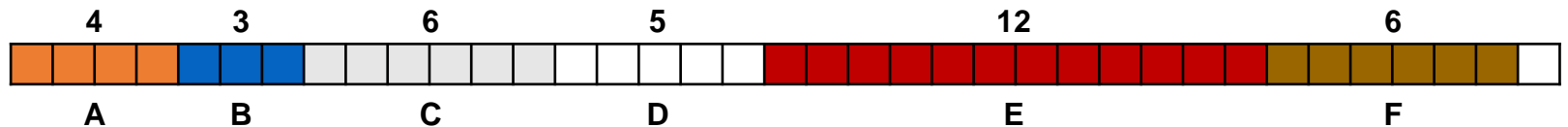
- Alto desempenho na leitura.
- Um seek (para o primeiro bloco).
- Depois segue movimento natural.

Métodos de alocação de arquivos – Alocação contínua

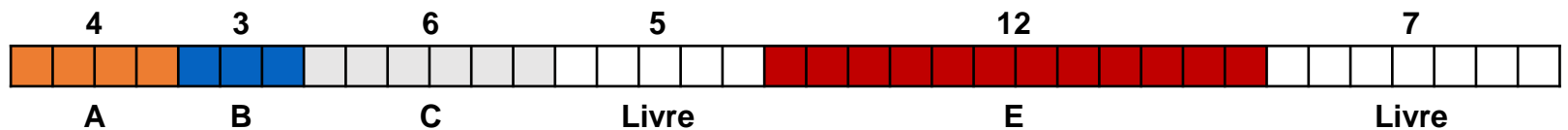
Desvantagens

- Ao longo do tempo, o disco se torna fragmentado.
- Compactação é uma operação de alto custo computacional.
- Reúso de espaços com atualização da lista de espaços livres.
- Problemas com a fragmentação nos blocos.
 - Conhecimento prévio do tamanho final do arquivo para alocar o espaço necessário.

37 Bloco

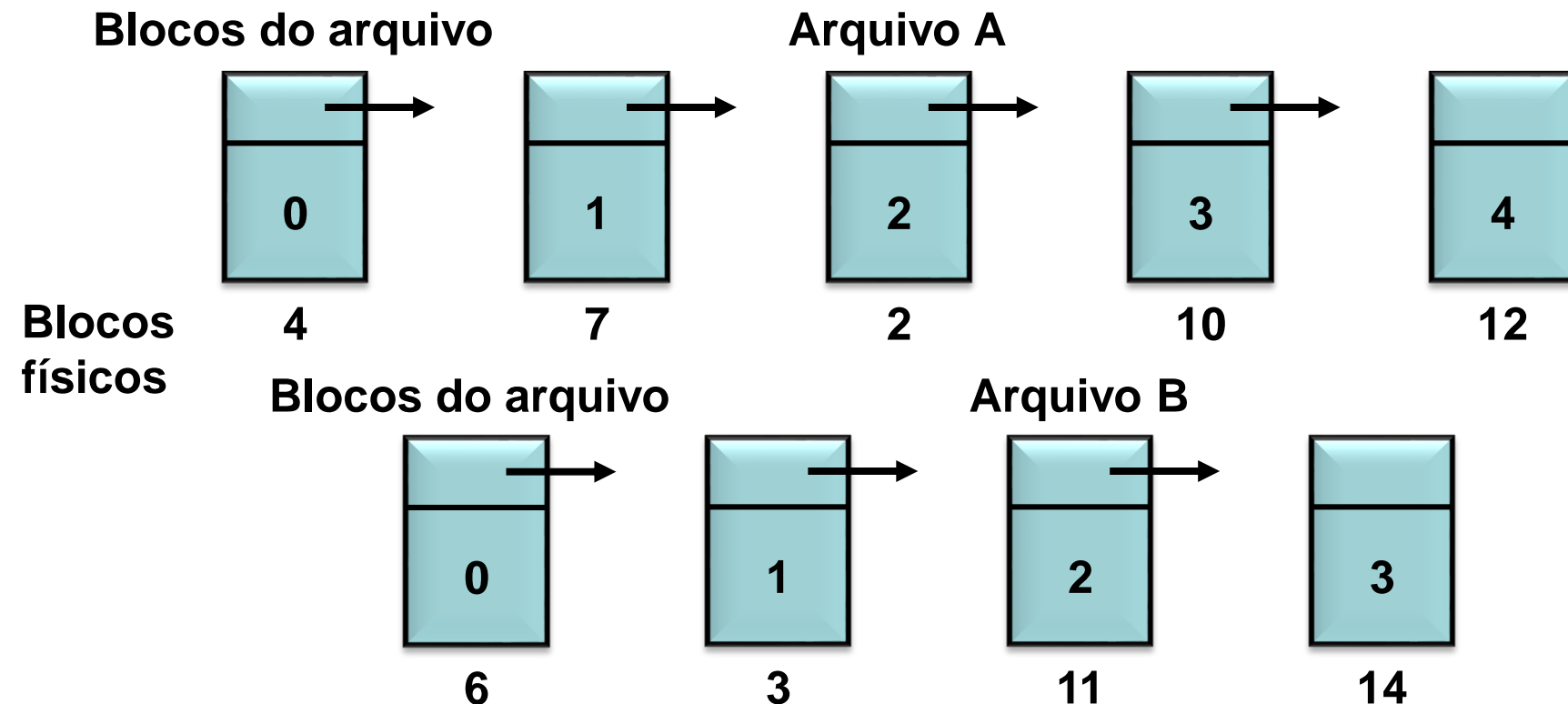


Removendo os arquivos D e F...



Métodos de alocação de arquivos – Alocação com lista encadeada

- A primeira palavra de cada bloco é um ponteiro para o bloco seguinte.
- O restante do bloco é destinado aos dados.
- Apenas o endereço em disco do primeiro bloco do arquivo é armazenado.
- Serviço de diretório é responsável por manter esse endereço.



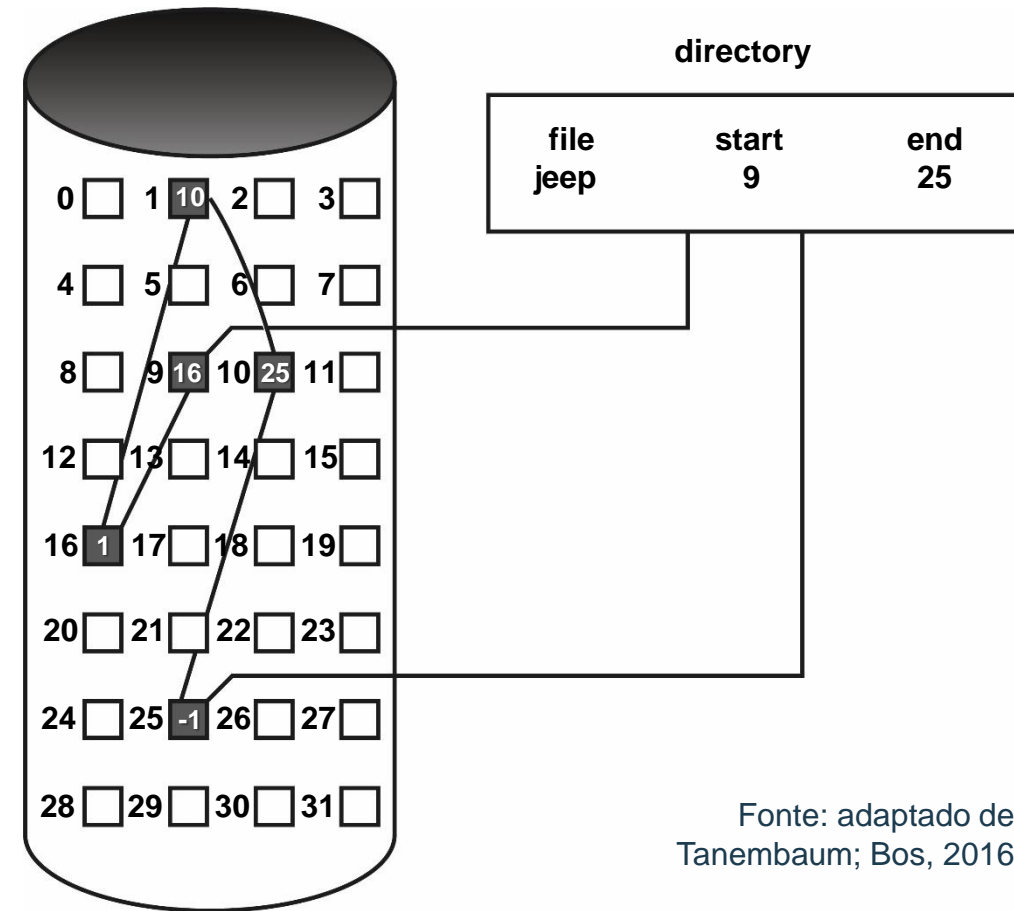
Métodos de alocação de arquivos – Alocação com lista encadeada

Desvantagens:

- Acesso aos arquivos é feito aleatoriamente, tornando o processo mais lento.
- A informação armazenada em um bloco não é mais uma potência de dois, pois existe a necessidade de se armazenar o ponteiro para o próximo bloco.

Vantagens:

- Não se perde espaço com a fragmentação externa.
- Basta informação do endereço inicial e tamanho do bloco.



Métodos de alocação de arquivos – Alocação com lista encadeada utilizando uma tabela na memória

- O ponteiro é colocado em uma tabela na memória ao invés de ser colocado no bloco FAT, tabela de alocação de arquivos File Allocation Table.
- Assim, todo o bloco está disponível para alocação de dados.
- Serviço de diretório é responsável por manter o início do arquivo (bloco inicial).
- MS DOS e família Windows 9 x (exceto WinNT Win 2000 e WinXP NTFS).
 - Acesso aleatório se torna mais fácil devido ao uso da memória.

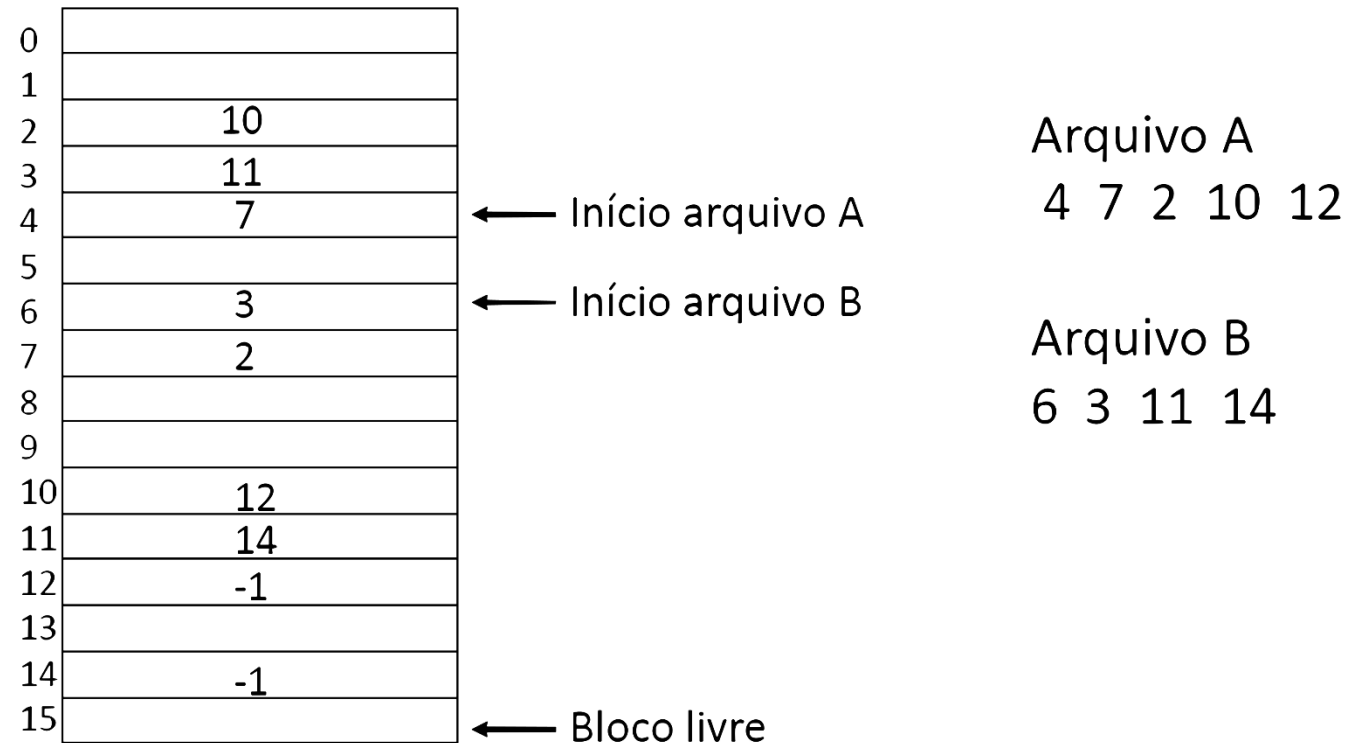
Métodos de alocação de arquivos – Alocação com lista encadeada utilizando uma tabela na memória

Desvantagem:

- Toda a tabela deve estar na memória.
- Exemplo: Com um disco de 20 Gb com blocos de 1 Kb, a tabela precisa de 20 milhões de entradas, cada qual com 3 bytes (para permitir um acesso mais rápido, cada entrada pode ter 4 bytes) ocupando entre 60 a 80 Mb da memória.

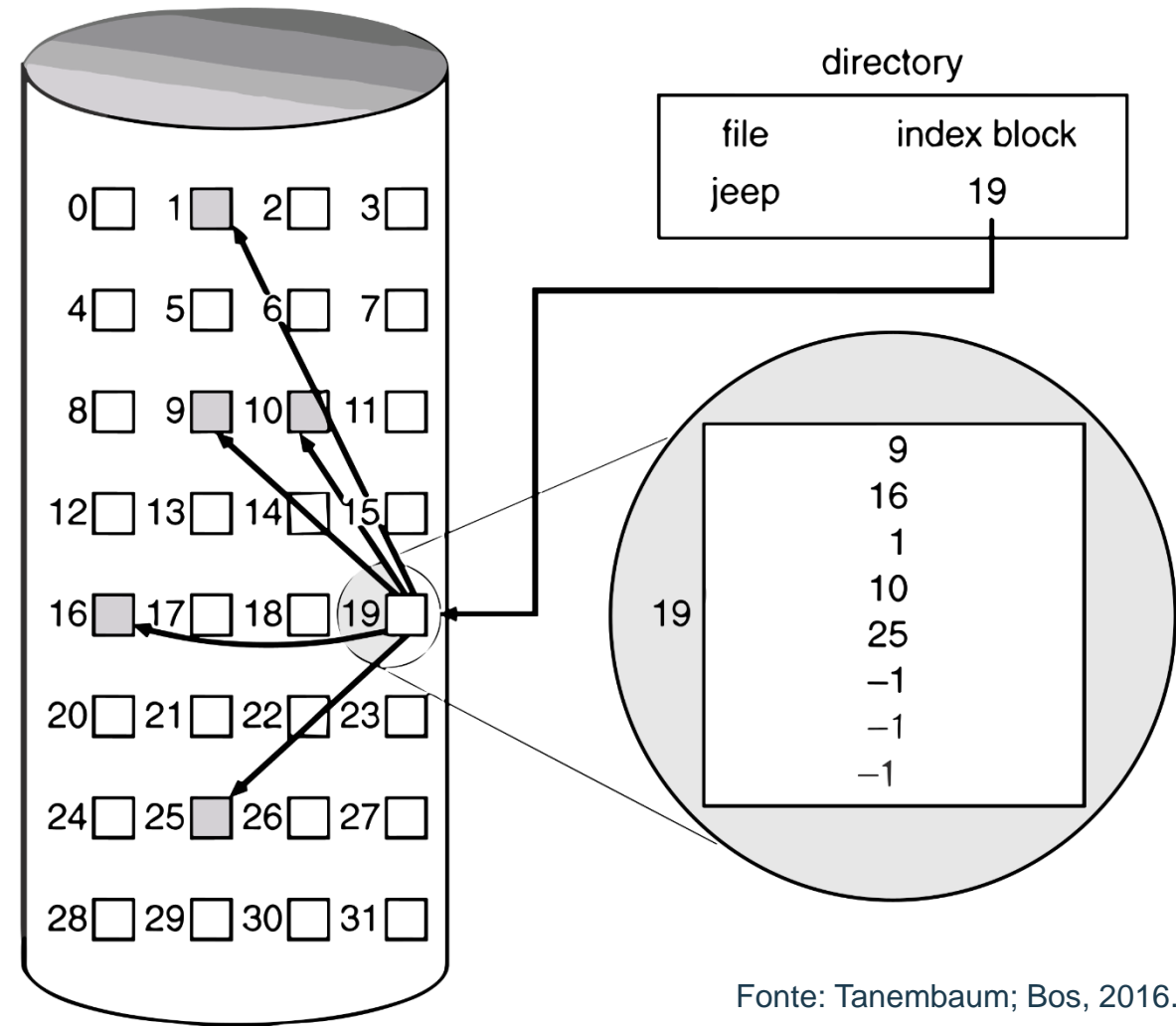
Vantagem:

- Maior velocidade de acesso à tabela.



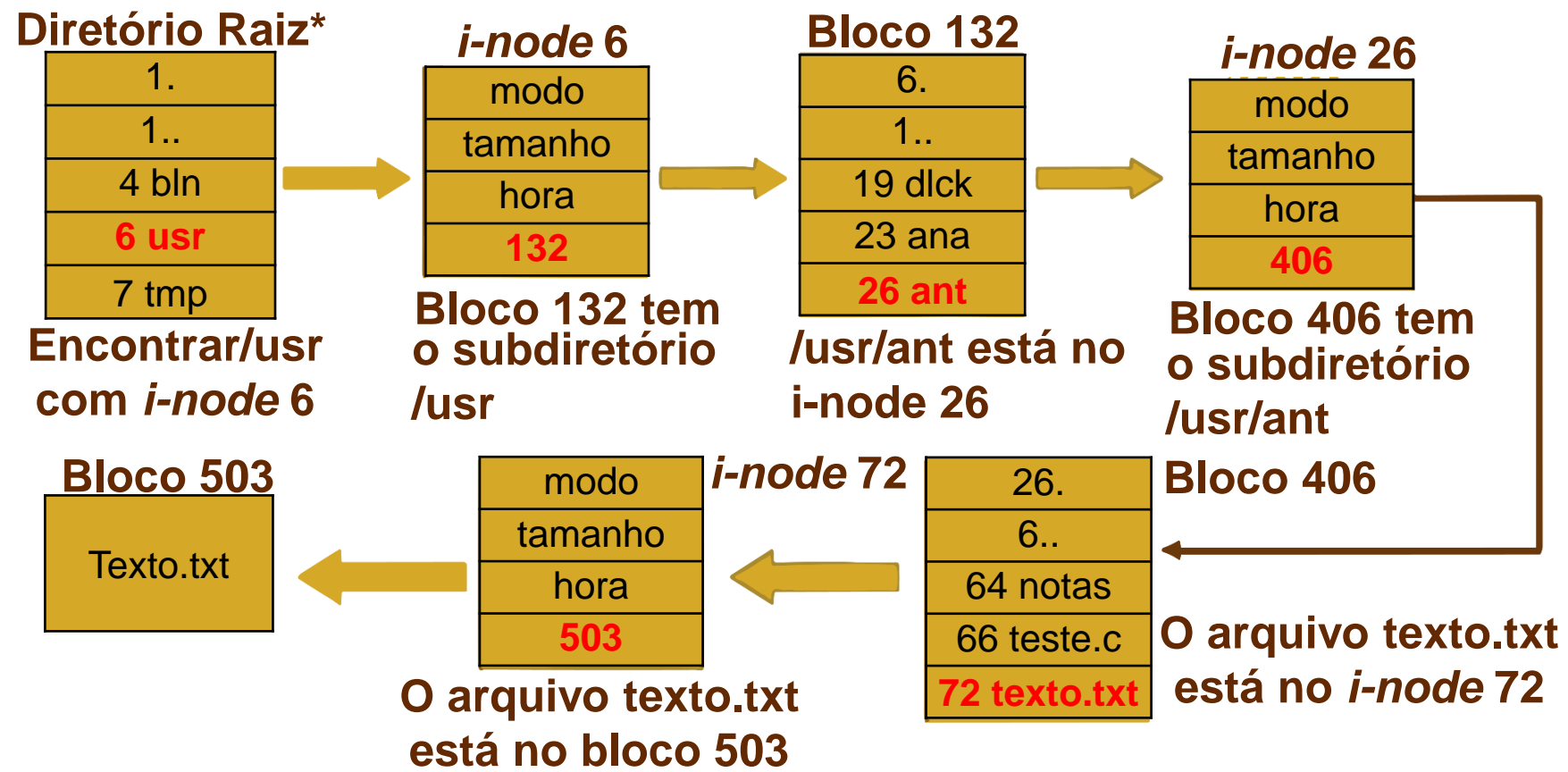
Métodos de alocação de arquivos – I-Nodes

- Cada arquivo possui uma estrutura de dados chamada I-Node (index node) que lista os atributos e endereços em disco dos blocos do arquivo.
- Assim, dado o I-Node de um arquivo é possível encontrar todos os blocos desse arquivo.
- Se cada I-Node ocupa n bytes e k arquivos podem estar abertos ao mesmo tempo, portanto, o total de memória ocupada é kn bytes.
- UNIX e Linux.



Métodos de alocação de arquivos – I-Nodes

- Exemplo: Leitura do arquivo /usr/ant/texto.txt



Fonte: Tanenbaum; Bos, 2016.

Métodos de alocação de arquivos – I-Nodes

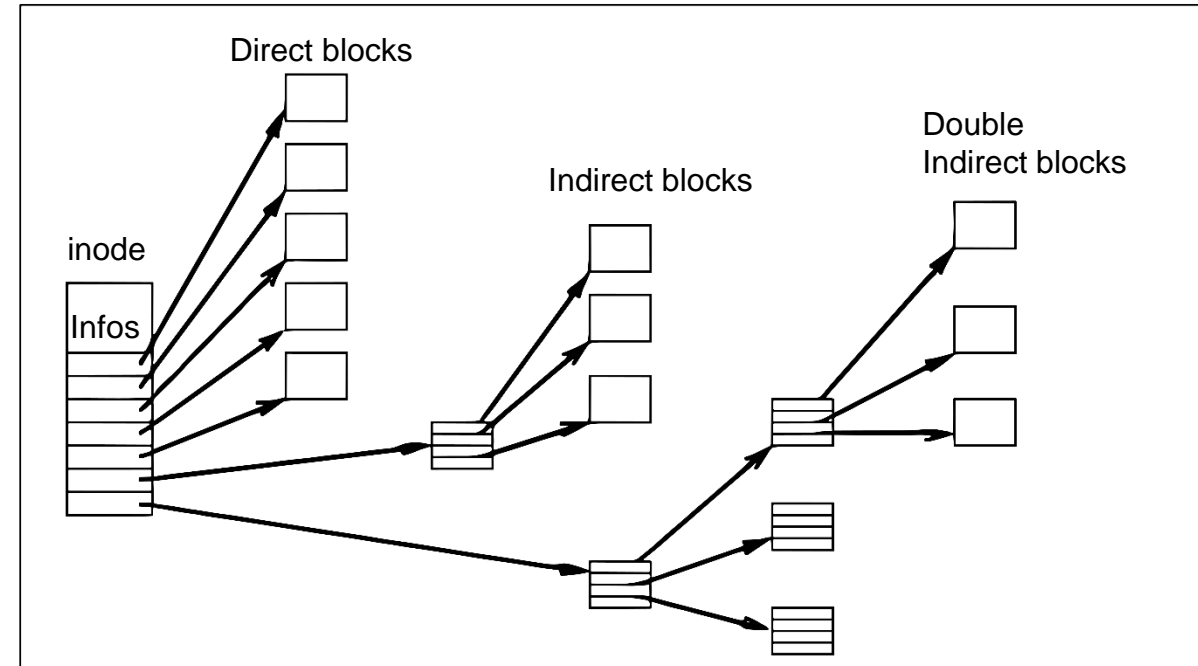
- Espaço de memória ocupado pelos I-Nodes é proporcional ao número de arquivos abertos enquanto o espaço de memória ocupado pela tabela de arquivos é proporcional ao tamanho do disco.

Vantagem:

- O I-Node somente é carregado na memória quando o seu arquivo está aberto (em uso).

Desvantagem:

- O tamanho do arquivo pode aumentar muito.
- Solução: reservar o último endereço para outros endereços de blocos.



Interatividade

Qual é o nome da estrutura do sistema de arquivos que possui a tabela de partição com o endereço inicial e final de cada partição?

- a) I-Nodes.
- b) MBR.
- c) FAT.
- d) Diretório Raiz.
- e) Grafos.

Resposta

Qual é o nome da estrutura do sistema de arquivos que possui a tabela de partição com o endereço inicial e final de cada partição?

- a) I-Nodes.
- b) **MBR.**
- c) FAT.
- d) Diretório Raiz.
- e) Grafos.

Sistema de arquivos no Linux

- Sistema de arquivos é responsável pelo gerenciamento das informações que são gravadas em uma determinada partição do disco.
- O sistema GNU/Linux trabalha com uma grande variedade de sistemas de arquivos.

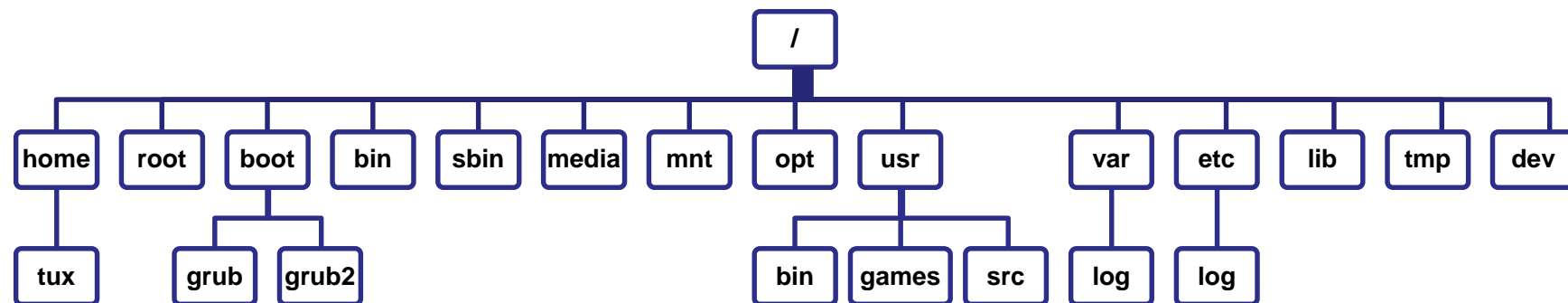
Sistema de arquivos e diretórios

O sistema de arquivos é responsável pelo gerenciamento das informações que são gravadas em uma determinada partição do disco. O sistema GNU/Linux trabalha com uma grande variedade de sistemas de arquivos. Seguem alguns:

- EXT2: É conhecido como SecondExtendedFileSystem e por utilizar blocos do mesmo tamanho para armazenar os arquivos.
- EXT3: Permite utilizar o sistema de cotas e pode trabalhar com blocos de 1, 2 e 4 kilobytes.
- EXT4: Podem facilmente ser convertidos para o formato ext4 e conta com melhorias no desempenho e na capacidade de armazenamento.

Sistema de arquivos e diretórios

- Devido à existência de diversas distribuições disponíveis, foi preciso realizar uma padronização nos diretórios encontrados.
- Essa padronização é conhecida como File System Hierarchy Standard (FHS).
- Essa estrutura está dividida de forma hierárquica, em que cada diretório possui uma finalidade diferente.



Estrutura do FHS. Fonte: autoria própria.

Situação de falha no sistema de arquivo

- Imagine a situação em remoção de um arquivo em um ambiente Linux.

Passos:

- Remoção do arquivo de seu diretório.
- Liberação do I-Node para o conjunto de I-Nodes livres.
- Devolução dos blocos livres no disco.

E se o sistema parar ao final da primeira etapa?

- I-Nodes com blocos não acessíveis e não realocáveis.

E ao final da segunda etapa?

- Os blocos serão perdidos.

Solução: Journaling

- Técnica para criar certa robustez diante das falhas.
 - Mantém-se um log ou jornal.
 - Info do que o sistema de arquivos irá fazer.
 - Antes que ele efetivamente o faça.
 - Se o sistema falhar antes de executar o trabalho:
 - Fazer depois da inicialização.
-
- Sistema de arquivos Journaling.
 - NTFS (Windows) e ext3 em diante (Linux).

Journaling – Funcionamento

Na operação de remoção de arquivo, haverá uma entrada no log com as 3 operações a serem realizadas:

- Remoção da entrada no diretório.
 - Liberação dos I-Nodes.
 - Liberação dos blocos.
-
- Gravação do log no disco.
 - Leitura da memória para verificar a integridade.
 - Somente então as operações têm início.
 - Quando uma é concluída, sua entrada do log é marcada.
 - Logs são excluídos periodicamente ou quando cheios.

Interatividade

No Linux é implementada uma área no sistema de arquivos responsável pelos registros de informações de arquivos e das respectivas atividades básicas, que foram realizadas em um determinado arquivo. Qual é o nome dessa área?

- a) I-Node.
- b) Estrutura em árvore.
- c) Journaling.
- d) FHS.
- e) Partição.

Resposta

No Linux é implementada uma área no sistema de arquivos responsável pelos registros de informações de arquivos e das respectivas atividades básicas, que foram realizadas em um determinado arquivo. Qual é o nome dessa área?

- a) I-Node.
- b) Estrutura em árvore.
- c) **Journaling.**
- d) FHS.
- e) Partição.

Proteção de Sistemas Operacionais

- Mecanismo destinado ao controle do acesso de programas e ao controle de processos ou de usuários aos recursos definidos por um sistema de computação.
- Processos que executam no SO necessitam ser adequadamente autorizados.

Necessário forma padronizada para:

- solicitar acesso;
- conceder (ou não);
- suspender ou abortar processo solicitante.

Proteção de Sistemas Operacionais

Por que investir em segurança de um sistema operacional?

Motivos:

- Para proteger o sistema e garantir que ele permaneça operando de forma adequada.
- Para assegurar que o acesso e o uso da informação sejam realizados em conformidade com políticas previamente estabelecidas.
- Nem todas as violações de segurança ocorrem de modo intencional! Usuários com pouco conhecimento a respeito de um sistema computacional podem causar distúrbios.

Proteção de Sistemas Operacionais

Essas políticas e regras podem ser estabelecidas de várias maneiras:

- pela introdução de itens no projeto do sistema;
 - pelo gerenciamento do sistema;
 - pelas atitudes de proteção dos usuários individuais em relação aos seus próprios arquivos e programas.
-
- **Mecanismo:** estamos interessados em descrever a maneira como algo é feito.
 - **Política:** estamos interessados em definir o que deve ser feito (e não em estabelecer o modo como algo é feito).
 - Política e mecanismo são complementares, o objetivo geral de um administrador é a definição de políticas com foco na descrição dos mecanismos, que devem apresentar flexibilidade.

Princípios em Sistemas Operacionais

- Princípio geral pode ser usado em todo um projeto.
- O princípio geral simplifica o processo de tomada de decisões e mantém o sistema “como um todo” consistente e de fácil entendimento.
- Princípio muito aplicado: princípio do privilégio mínimo, o qual determina que programas, usuários e subsistemas recebam apenas os privilégios necessários e suficientes para a execução de suas tarefas.
 - Usando esse princípio, o gerenciamento de usuários requer a criação de uma conta separada para cada usuário, que dê apenas os direitos de acesso que tal usuário precisa.

Princípio do privilégio mínimo

- Gerenciamento de usuário ocorre por meio de listas de controle de acesso ou ACLs.
- Maioria dos sistemas operacionais atuais implementam as ACLs.
- Uma ACL é uma lista de permissões referentes a dado objeto, sejam componentes de hardware ou entidades de software.
 - Uma ACL especifica quais usuários e/ou processos podem acessar dado objeto e define quais operações tal usuário pode fazer com esse objeto. Cada item em uma ACL especifica um usuário (ou um processo) e uma ou mais operações.
 - RBAC (Role-Based Access Control): atribuições de permissões aos usuários definidas a partir de operações que tenham significado para a empresa que utiliza o RBAC.

Princípio de só saber/poder o necessário

- Pode ser usado para complementar o princípio do privilégio mínimo.
- A cada usuário que tenha as permissões necessárias de segurança é dado acesso apenas aos objetos computacionais estritamente necessários para que tal usuário cumpra suas missões e só até que elas sejam cumpridas.
 - Event logs: registram todas as atividades de proteção e de segurança do sistema computacional, possibilitam que o programador, o administrador do sistema ou o auditor legal rastreiem tudo o que acontece no sistema, o que serve para comprovar (ou não) sua segurança e sua integridade.

Domínios de proteção

- Modelo convencional para se analisar a implementação de proteção.
- Processo irá trabalhar dentro de um domínio de proteção, que determina o que o processo pode fazer e o que o processo não pode fazer.

A associação entre um processo e um domínio pode ser:

- estática; ou
- dinâmica.

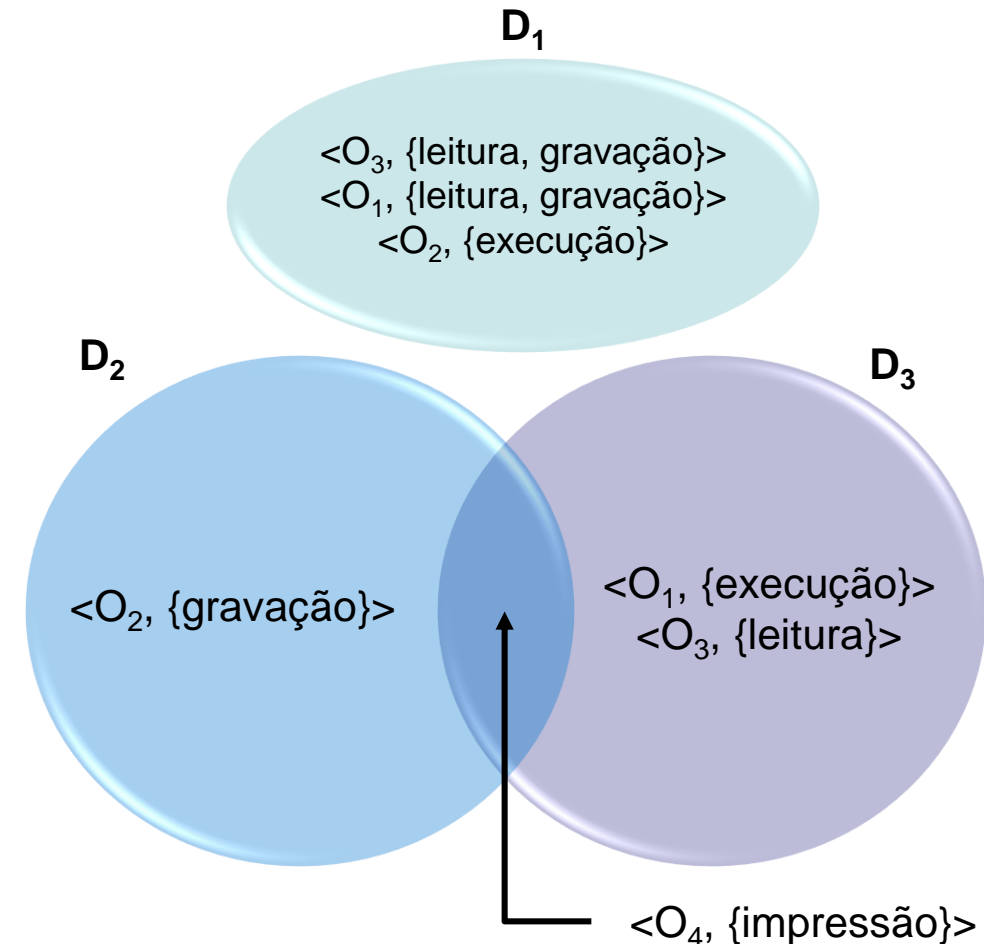


Figura mostra sistema com
três domínios de proteção.
Fonte: autoria própria.

Domínios de proteção

- Em Unix e Windows Server, os domínios são representados pelos usuários.
- Permuta de domínio corresponde à alteração temporária da identificação do usuário.
- No Linux, alteração do bit setuid.

Segurança

- **Proteção:** Problema estritamente interno, que se resume a como fornecer acesso controlado a programas e a dados armazenados em um sistema de computação.
- **Segurança:** Além do sistema de proteção adequado, também necessita que o ambiente externo no qual o sistema computacional opera seja considerado.
- Sistema de proteção será ineficiente caso a autenticação de usuários for comprometida ou se usuários não autorizados conseguirem invadir o sistema.

Segurança total é um ideal inatingível, pois sempre pode ocorrer alguma situação imprevisível que comprometa a segurança.

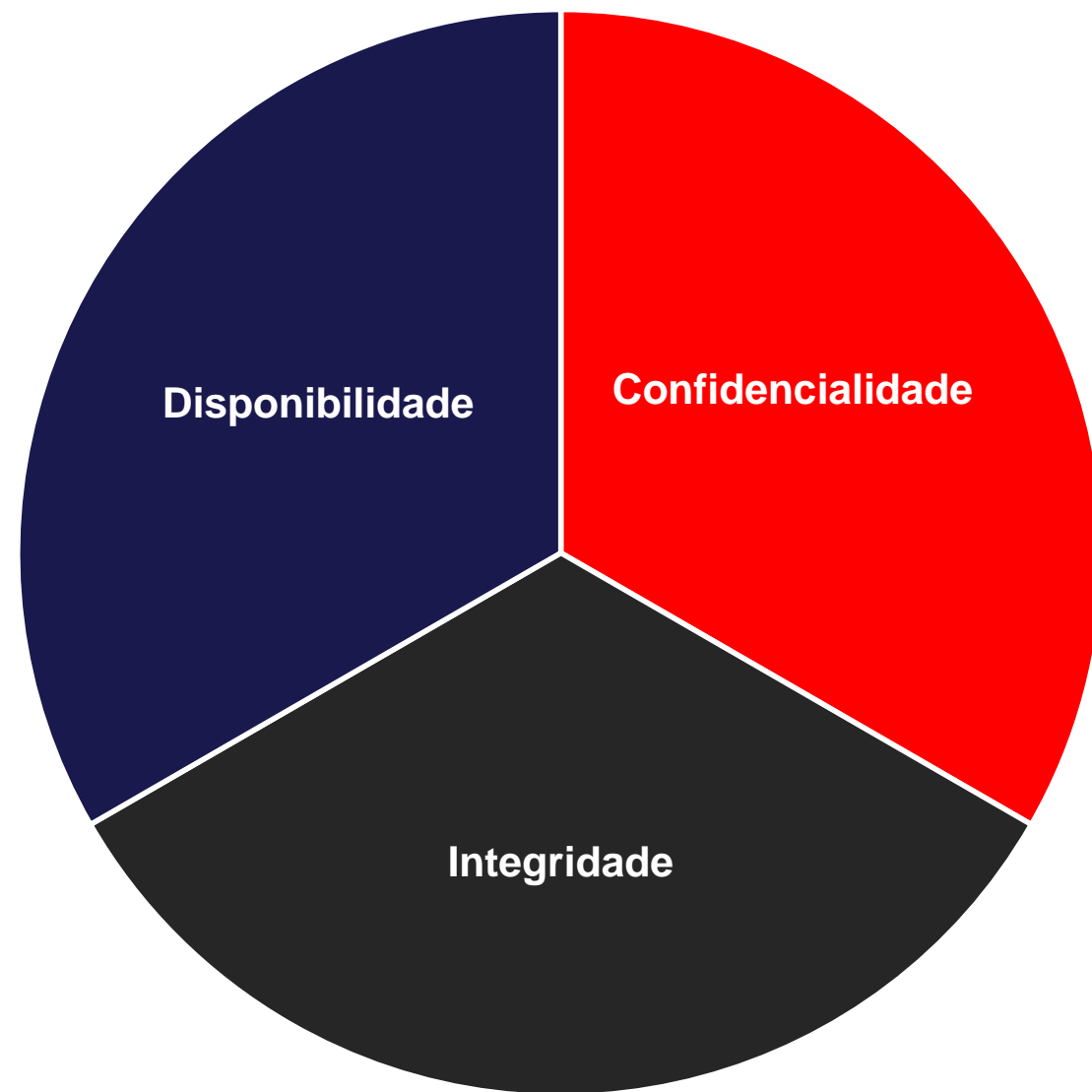
Segurança

Violações da segurança do sistema ou sua má utilização podem ser classificadas em:

- intencionais (maliciosas); ou
 - acidentais.
-
- **Atacante (ou invasor):** quem tenta (ou consegue) violar a segurança de um sistema computacional intencionalmente.
 - **Ameaça:** possibilidade de uma violação de segurança de um sistema computacional, tal como a descoberta de uma vulnerabilidade.
 - **Ataque:** tentativa de violar a segurança de um sistema computacional.

Segurança

- **Confidencialidade.** Termo relativo à manutenção das restrições que foram autorizadas sobre o acesso e a divulgação de informações e à privacidade de indivíduos.
- **Integridade.** Termo relativo à prevenção contra alterações ou destruições impróprias de informações.
- **Disponibilidade.** Termo relativo à garantia do acesso e da utilização da informação de maneira rápida e confiável.



Tipos de violações acidentais e maliciosas da segurança

- **Violação de sigilo.** Trata-se da duplicação não autorizada de informações.
- **Violação de integridade.** Trata-se de um tipo de violação em que os dados são modificados de forma não intencional e/ou não autorizada.
- **Violação de disponibilidade.** Trata-se de um tipo de violação em que os dados não são modificados, mas, sim, destruídos.
- **Furto de serviço.** Trata-se de um tipo de violação em que o objetivo do invasor é se aproveitar de algum recurso computacional de forma não autorizada.
- **Recusa de serviço.** Trata-se de um tipo de violação em que o invasor visa impedir que um sistema continue operando normalmente e oferecendo sua funcionalidade.
 - Exemplos: DoS, ou “Denial of Service”.
DDoS, ou “Distributed Denial of Service”.

Ataques a parques computacionais

- Ataques mais comuns a parques computacionais: **Personificação**.
- Um participante de uma comunicação finge ser alguém que não é. Por meio da personificação, o agressor viola a autenticação da identidade e pode então obter acesso que não receberia.
- Outro tipo de ataque frequente: **Reexecução**.
- O invasor realiza a interceptação e a gravação de uma transmissão de dados e faz com que essa gravação seja executada “de novo”, com o objetivo de tentar repetir o resultado da transmissão original.

Segurança em SOs

- Quantidade de vulnerabilidades mapeadas nos sistemas operacionais.
- Questão da segurança de sistemas operacionais ainda é complexa.
- Um sistema operacional não é apenas um único software, mas uma coleção enorme de programas com finalidades específicas.

Fonte: adaptado de:
<https://cryptoid.com.br/protacao-de-dados/eset-analisou-quais-tipos-de-vulnerabilidades-foram-mais-relatadas-nos-computadores-sistemas-operacionais-e-aplicativos-no-ultimo-ano/>

	Nome do sistema operacional	Nome do fabricante	Tipo de produto	Número de vulnerabilidades históricas
1	Debian Lmux	Debian	OS	7489
2	Android	Google	OS	4902
3	Fedora	Fedoraproject	OS	4108
4	Ubuntu Linux	Canonical	OS	3709
5	Mac Os X	Apple	OS	3101
6	Linux Kernel	Linux	OS	3034
7	Windows 10	Microsoft	OS	3016
8	Iphone Os	Apple	OS	2863
9	Windows Server 2016	Microsoft	OS	2786
10	Windows Server 2008	Microsoft	OS	2445

Interatividade

De acordo com o princípio do privilégio mínimo, quais privilégios um usuário deve receber?

- a) Somente privilégio de leitura.
- b) Nenhum privilégio será concedido.
- c) Somente privilégios necessários para execução de suas tarefas.
- d) Todos os privilégios de um administrador do sistema.
- e) O usuário poderá consultar, executar, salvar arquivos, mas não poderá modificá-los.

Resposta

De acordo com o princípio do privilégio mínimo, quais privilégios um usuário deve receber?

- a) Somente privilégio de leitura.
- b) Nenhum privilégio será concedido.
- c) Somente privilégios necessários para execução de suas tarefas.
- d) Todos os privilégios de um administrador do sistema.
- e) O usuário poderá consultar, executar, salvar arquivos, mas não poderá modificá-los.

Referências

- CÓRDOVA JUNIOR, R. S.; LEDUR, C. L.; MORAIS, I. S. de. *Sistemas operacionais*. Porto Alegre: Grupo A, 2019.
- FURUKAWA, F.; NUNES, R. *Fundamentos de sistemas operacionais*. São Paulo: Editora Sol, 2011.
- MACHADO, F. B.; MAIA, L. P. *Arquitetura de sistemas operacionais*. 5. ed. Rio de Janeiro: LTC, 2013.
- MAZIERO, C. A. *Sistemas operacionais: conceitos e mecanismos [recurso eletrônico]*. Curitiba: DINF/UFPR, 2019.
 - OLIVEIRA, R. S.; CARISSIMI, A. S.; TOSCANI, S. S. *Sistemas operacionais*, v. 11. 4 ed. Porto Alegre: Bookman: 2010.
 - SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE, G. *Fundamentos de sistemas operacionais*. 9. ed. Rio de Janeiro: LTC, 2015.

Referências

- TANENBAUM, S. A.; WOODHULL, S. *Sistemas operacionais: projetos e implementação – o livro do Minix*. 3. ed. Porto Alegre: Bookman, 2008.
- TANENBAUM, A. S.; BOS, H. *Sistemas operacionais modernos*. 4. ed. São Paulo: Pearson: 2016.

ATÉ A PRÓXIMA!