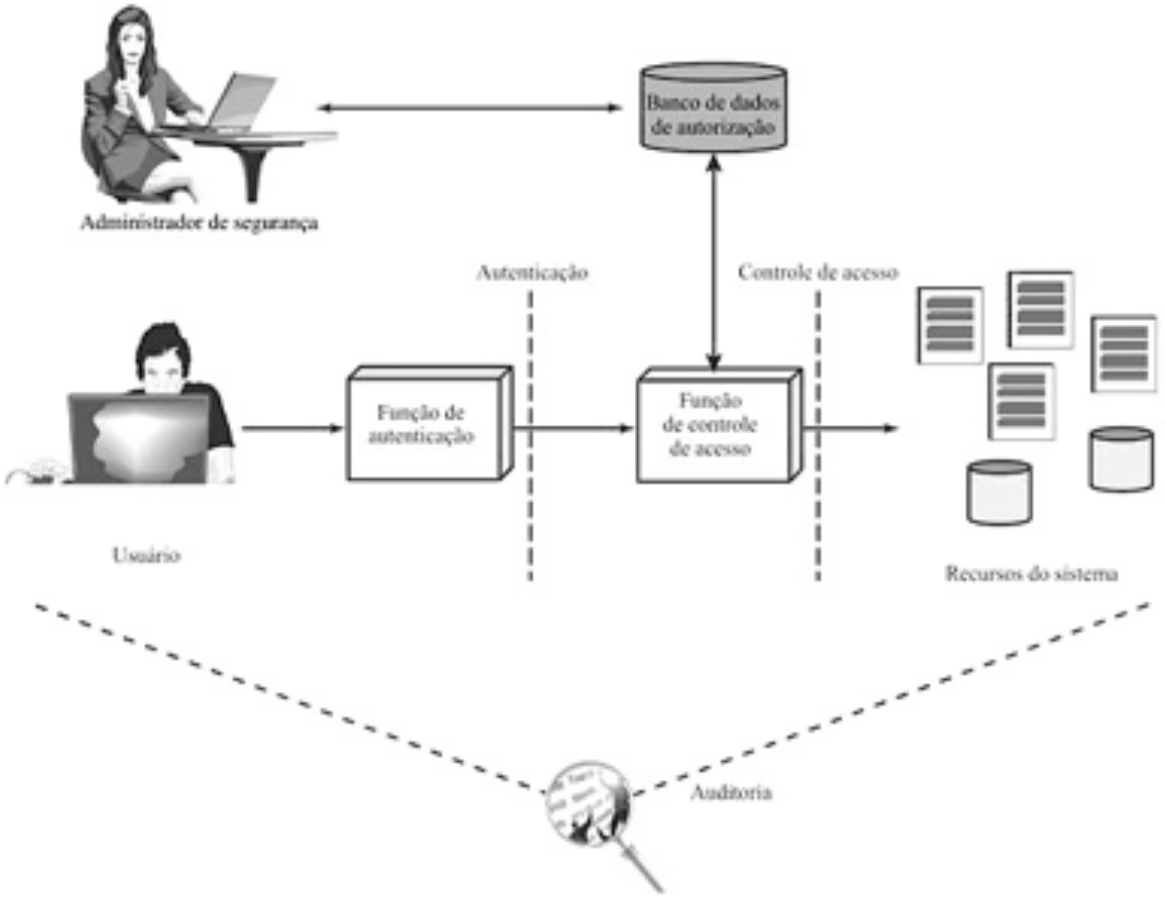
Controle de Acesso

Introdução

Controle de Acesso

- "Prevenção do uso não autorizado de um recurso, incluindo a prevenção do uso de um recurso de maneira não autorizada"
- Aspecto central da segurança de computadores
- Assume a existência de usuários e grupos
  - Autenticação no sistema
  - Associação de direitos de acesso a determinados recursos do sistema

Princípios de controle de acesso



Políticas de Controle de Acesso

- Controle de acesso discricionário (Discretionary Access Control — DAC): entidade pode ter direitos de acesso que lhe permitem, por sua própria vontade, habilitar outra entidade a acessar algum recurso
- Controle de acesso mandatório (Mandatory Access Control — MAC): entidade que está autorizada a acessar um recurso não pode habilitar outra entidade a acessar aquele recurso
- Controle de acesso baseado em papéis (RBAC): Controla o acesso com base nos papéis que os usuários desempenham dentro do sistema

Políticas de Controle de Acesso

- Controle de acesso discricionário (Discretionary Access Control — DAC): entidade pode ter direitos de acesso que lhe permitem, por sua própria vontade, habilitar outra entidade a acessar algum recurso
- Controle de acesso mandatório (Mandatory Access Control — MAC): entidade que está autorizada a acessar um recurso não pode habilitar outra entidade a acessar aquele recurso
- Controle de acesso baseado em papéis (RBAC): Controla o acesso com base nos papéis que os usuários desempenham dentro do sistema

Definições mutuamente não-excludentes

Políticas de Controle de Acesso

Requisitos/Princípios de Controle de Acesso

- **Entrada Confiável**: necessidade de autenticação
- **Especificações mais ou menos detalhadas**: diferentes níveis de granularidade
- **Privilégio mínimo**: menor conjunto possível de recursos
- **Separação de deveres**: etapas de uma função crítica distribuídas entre diferentes usuários
- **Políticas abertas e fechadas**: white vs black list
- **Combinações de políticas e resolução de conflitos**: cenários de aplicação de mais de uma política
- **Políticas administrativas**: quem pode adicionar, eliminar ou modificar as regras de autorização
- **Controle dual**: duas pessoas precisam atuar para completar um processo (cofre com duas chaves)

Elementos de Controle de Acesso

- Sujeito: entidade capaz de acessar objetos
  - Classes típicas de acesso: proprietário, grupo e global
- Objeto: recurso cujo acesso é controlado
  - Exemplos: arquivos, registros, programas etc.
- Direito de acesso: modo pelo qual o objeto é acessado
  - Exemplos: leitura, escrita, execução, remoção, criação, busca

Controle de Acesso Discricionário

Controle de Acesso Discricionário

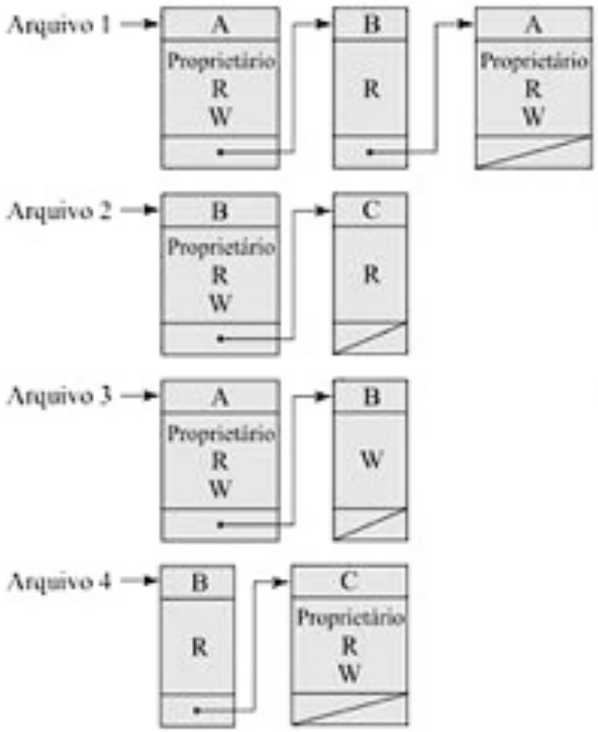
- Todo objeto possui um proprietário que define os direitos de acesso a este objeto
- Direitos de acesso frequentemente definidos por meio de uma matriz de acesso
  - sujeitos em uma dimensão (linhas)
  - objetos em outra dimensão (colunas)
  - cada célula especifica os direitos de acesso do sujeito àquele objeto
- Em geral, a matriz de acesso é esparsa

Estruturas de dados de DAC

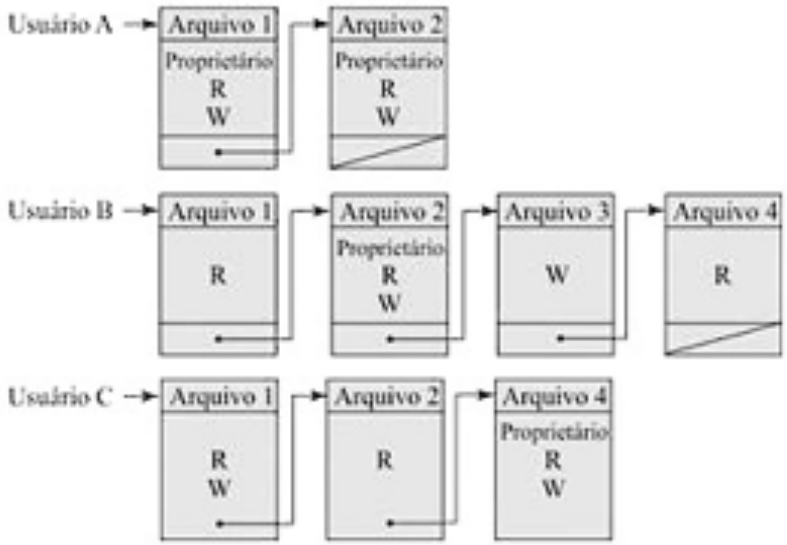
		OBJETOS			
		Arquivo 1	Arquivo 2	Arquivo 3	Arquivo 4
SUJEITOS	Usuário A	Proprietário Leitura Escrita		Proprietário Leitura Escrita	
	Usuário B	Proprietário	Proprietário Leitura Escrita	Escrita	Leitura
	Usuário C	Leitura Escrita	Leitura		Proprietário Leitura Escrita

(a) Matriz de acesso

Estruturas de dados de DAC



(b) Listas de controle de acesso para os arquivos da parte (a)

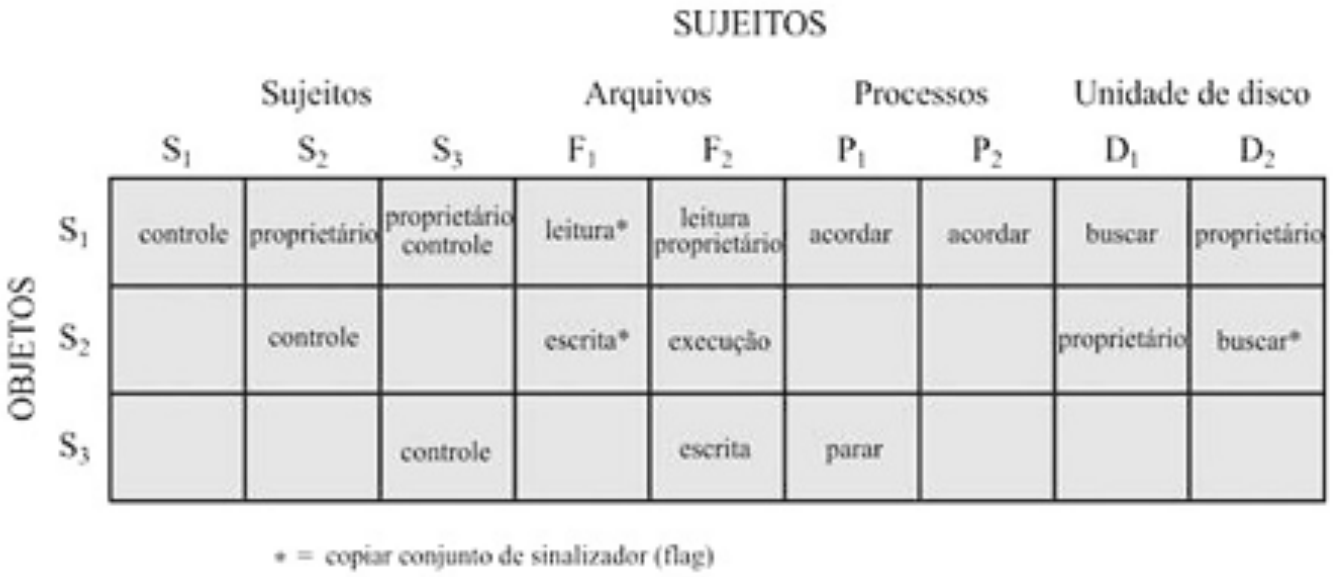


(c) Listas de capacidades para os arquivos da parte (a)

Tabela de Controle de Acesso [SAND94]

Sujeito	Modo de acesso	Objeto
A	Proprietário	Arquivo 1
A	Leitura	Arquivo 1
A	Escrita	Arquivo 1
A	Proprietário	Arquivo 3
A	Leitura	Arquivo 3
A	Escrita	Arquivo 3
B	Leitura	Arquivo 1
B	Proprietário	Arquivo 2
B	Leitura	Arquivo 2
B	Escrita	Arquivo 2
B	Escrita	Arquivo 3
B	Leitura	Arquivo 4
C	Leitura	Arquivo 1

Modelo de Controle de Acesso

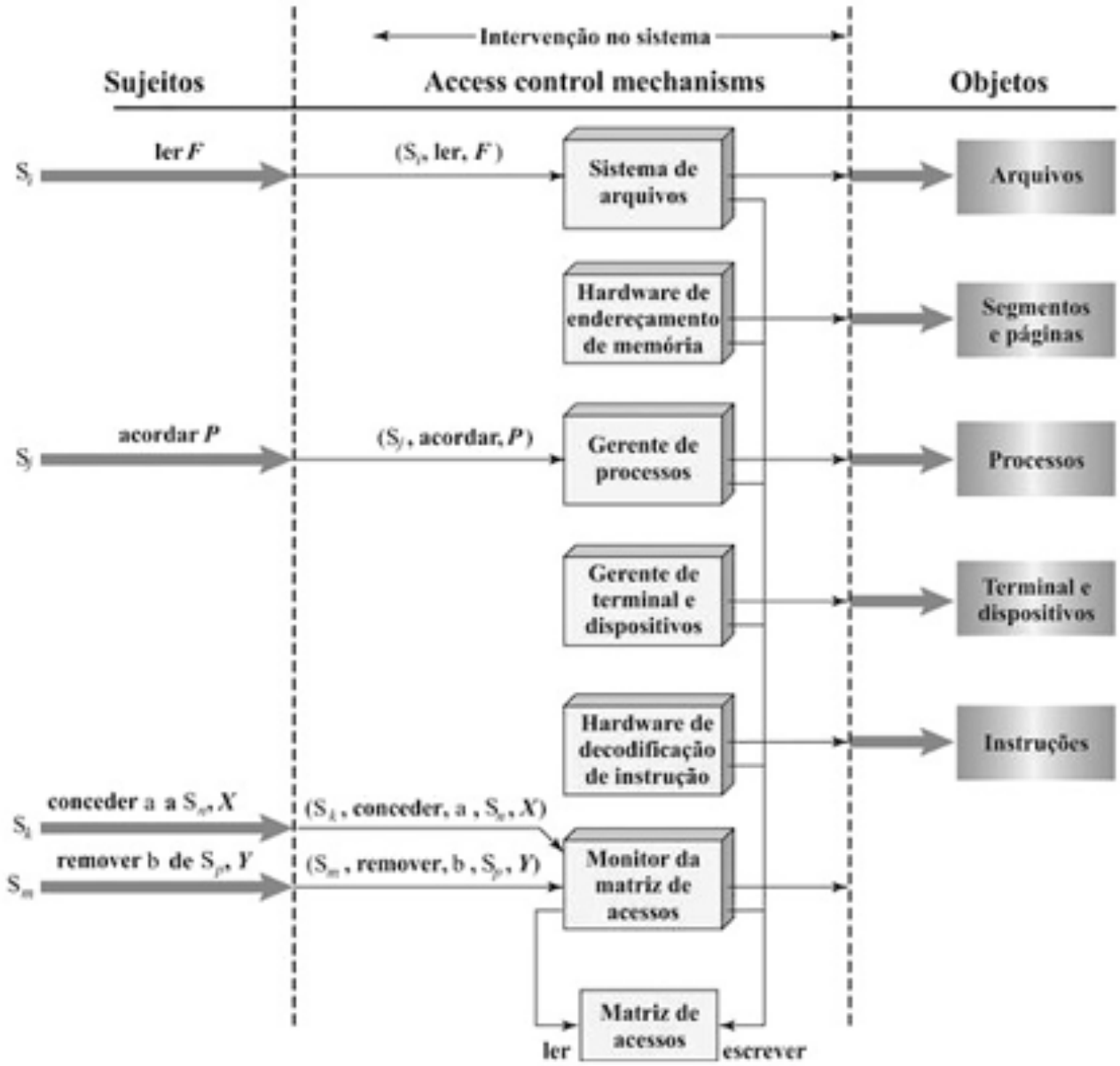


SUJEITOS

OBJETOS	Sujeitos			Arquivos		Processos		Unidade de disco	
	S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
S_1	controle	proprietário	proprietário controle	leitura*	leitura proprietário	acordar	acordar	buscar	proprietário
S_2		controle		escrita*	execução			proprietário	buscar*
S_3			controle		escrita	parar			

* = copiar conjunto de sinalizador (flag)

Função de Controle de Acesso

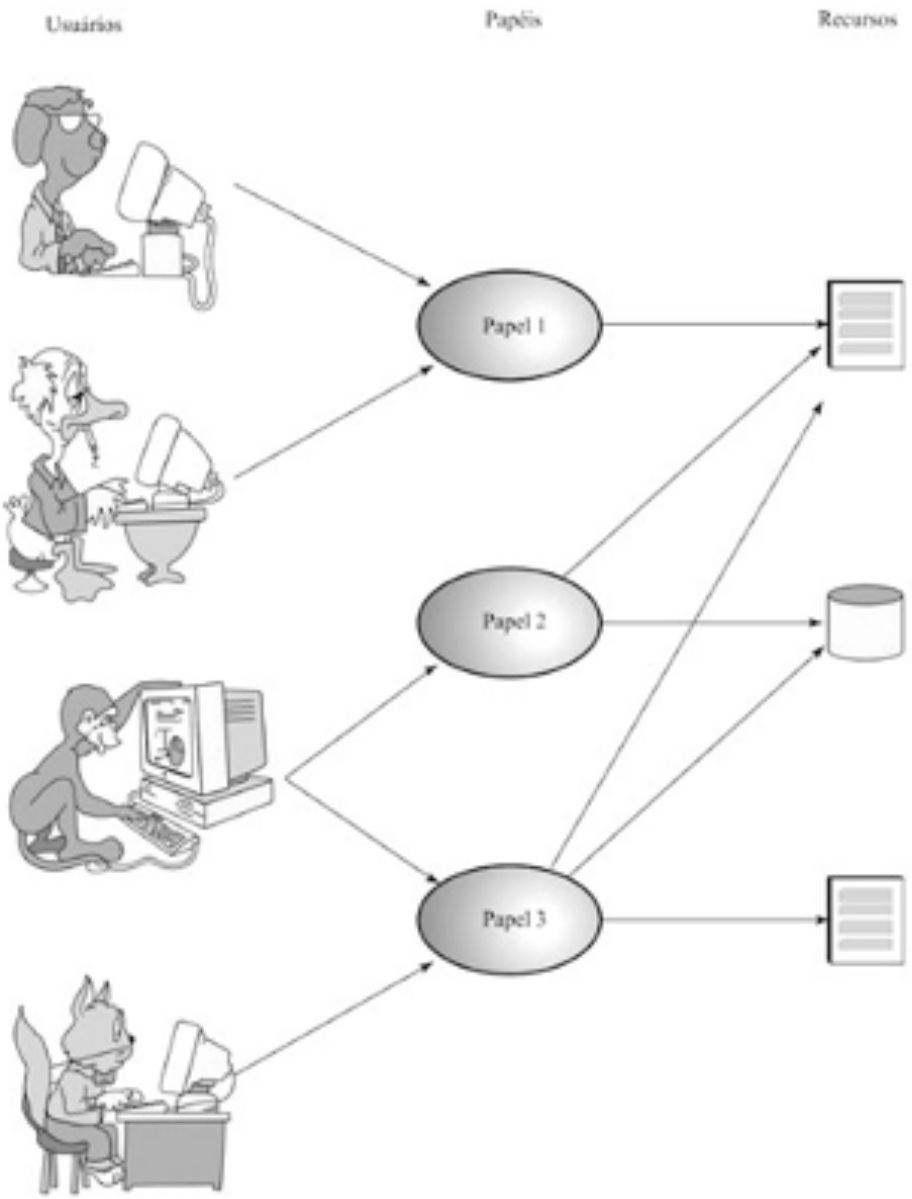


Controle de Acesso Baseado em Papéis

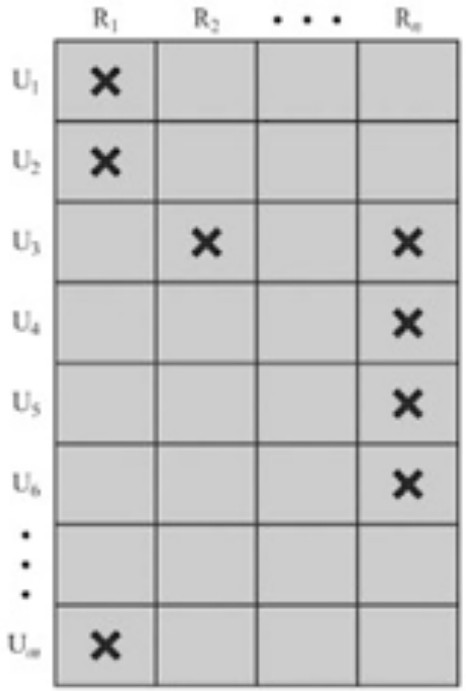
Controle de Acesso Baseado em Papéis

- Baseado nos "papéis" que usuários podem assumir em um sistema
  - Não depende diretamente da identidade
- Os direitos de acesso estão atribuídos a "papéis" – e não a usuários individuais
  - Matriz de acesso do RBAC para "papéis" é similar à matriz de acesso de DAC para "sujeitos"
  - Papéis podem ser tratados como objetos – hierarquia de papéis
- Relações "muitos para muitos" entre papéis e usuários
- RBAC tem uso comercial disseminado, pesquisa ativa e reconhecimento técnico
  - FIPS 140-2 exige suporte a RBAC

Controle de Acesso baseado em papéis



Controle de Acesso baseado em papéis

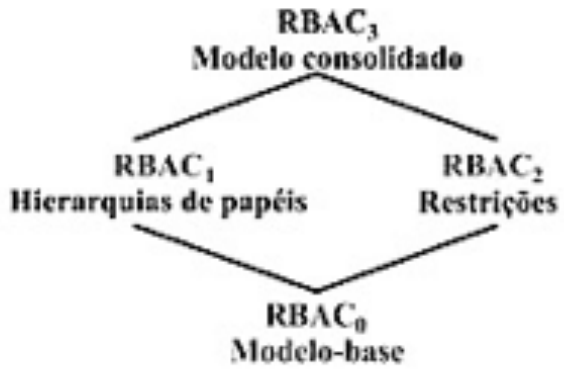


OBJETOS

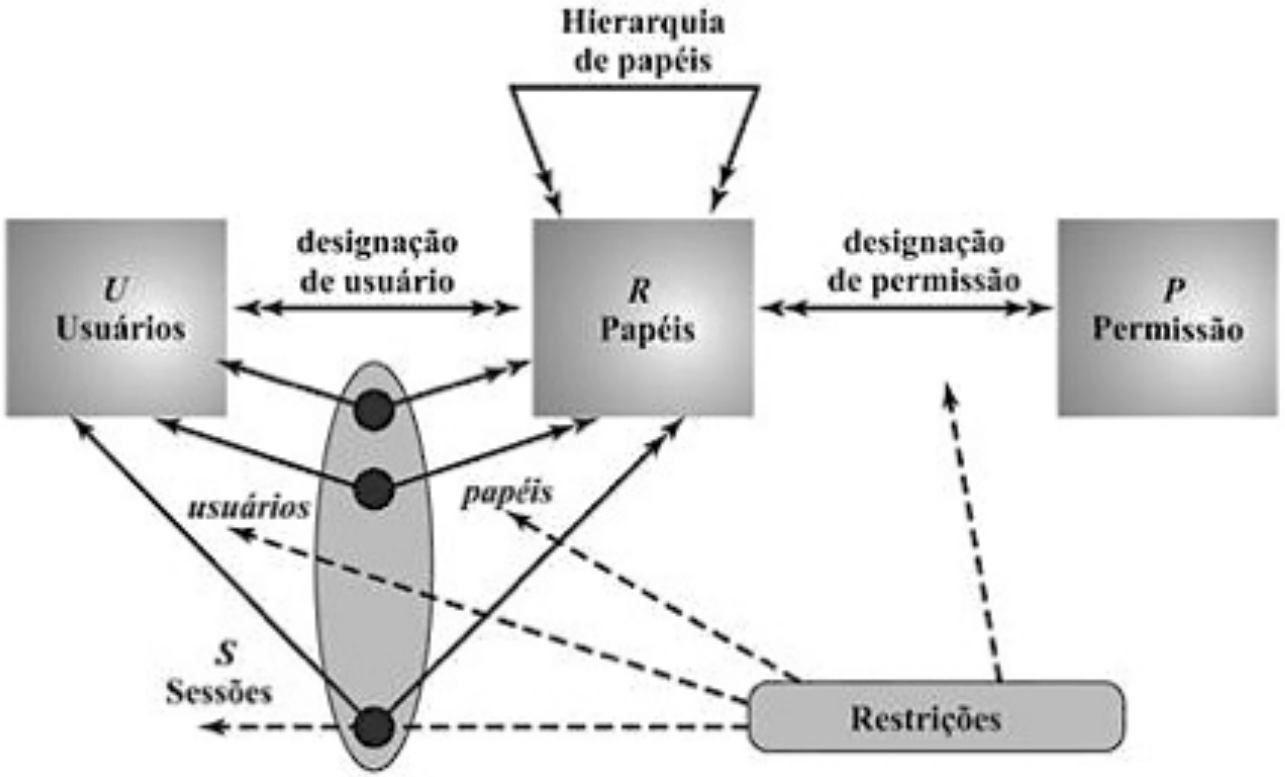
PAPÉIS	R1	R2	Rn	F1	F2	P1	P2	D1	D2
R1	controle	proprietário	proprietário controle	leitura*	leitura proprietário	acordar	acordar	buscar	proprietário
R2		controle		escrita*	execução			proprietário	buscar*
. . .									
Rn			controle		escrita	parar			

Modelos de Referência para RBAC

- $RBAC_0$: Funcionalidades mínimas para sistema RBAC
- $RBAC_1$: $RBAC_0$ + hierarquia de papéis
- $RBAC_2$: $RBAC_0$ + restrições sobre configurações
- $RBAC_3$: $RBAC_1$ + $RBAC_2$



Modelo consolidado RBAC(3)



Modelo-base: $RBAC_0$

- Quatro tipos de entidades em um sistema $RBAC_0$
  - Usuário: indivíduo com acesso a sistema computacional - cada indivíduo tem um ID de usuário a ele associado.
  - Papel: função definida no sistema computacional ou organização que o controla - normalmente, associada a cada papel há uma descrição da autoridade e da responsabilidade conferidas a esse papel e a qualquer usuário que assuma esse papel
  - Permissão: aprovação de modo de acesso em particular a um ou mais objetos - termos equivalentes são direito de acesso, privilégio e autorização.
  - Sessão: mapeamento entre um usuário e um subconjunto ativado do conjunto de papéis atribuídos a um usuário.

Hierarquia de papéis: $RBAC_1$

› O $RBAC_1$ permite reproduzir a hierarquia de papéis típica das organizações
  – Funções com maior responsabilidade agregam/acumulam permissões para acesso a recursos

Restrições: $RBAC_2$

- Restrições fornecem uma forma de adaptar o RBAC às políticas administrativas e de segurança específicas de uma organização
- Uma restrição é uma relação definida entre papéis ou uma condição relacionada a papéis
- Tipos de restrições
  - papéis mutuamente exclusivos
  - cardinalidade
  - papéis com pré-requisitos

Tipos de restrições

- Papéis mutuamente exclusivos
  - um usuário só pode ser designado para um único papel do conjunto de papéis
  - limitação poderia ser estática ou dinâmica
  - provê suporte a uma separação de deveres e capacidades dentro de uma organização
- Cardinalidade
  - número máximo com relação a papéis
  - Ex.: número máximo de usuários que podem ser designados a determinado papel - o papel de líder de projeto ou o papel de chefe de departamento poderia ser limitado a um único usuário
  - também pode impor uma restrição ao número de papéis aos quais um usuário é designado ou ao número de papéis que um usuário pode ativar para uma única sessão
- Pré-requisito
  - usuário só pode ser designado a determinado papel se já estiver designado a algum outro papel especificado
  - pode ser usado para estruturar a implementação do conceito do privilégio mínimo.