



**Universidade Federal de Mato Grosso-UFMT**  
**Sistemas de Informação**  
**Laboratório de Banco de Dados**  
**Prof. Dr. Clóvis Júnior**

# **Controle de Usuários (Segurança)**



## **Data Definition Language - DDLs**



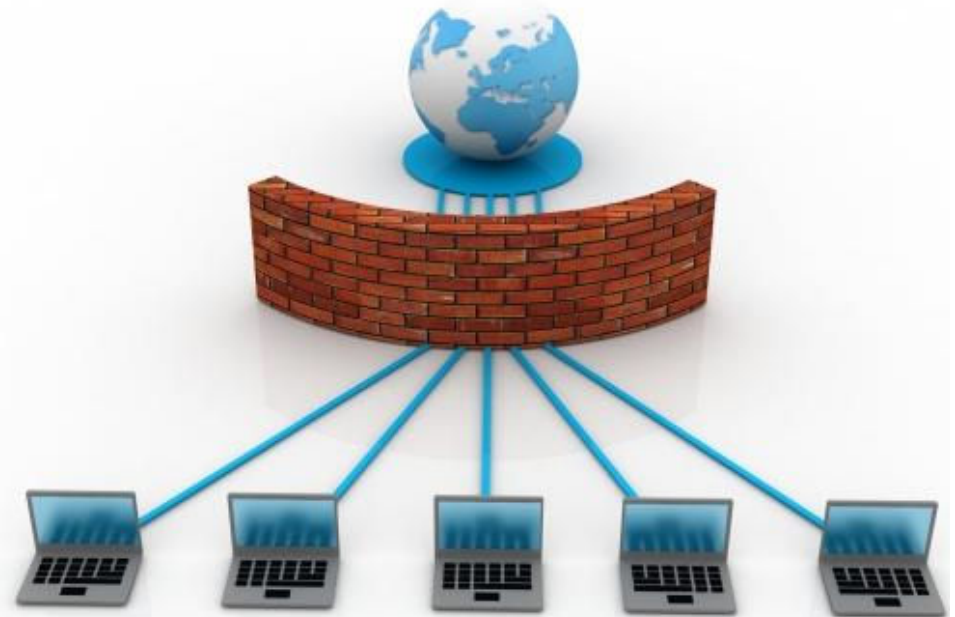
# Segurança em Banco de Dados



**Sistema Gerenciador de  
Bando de Dados**



**Redes de Computadores**



# Por que segurança é importante ?

Acesso não autorizado a servidores,  
bancos de dados e aplicativos;

Worms / Vírus;

Vulnerabilidades de Software;

Intrusão (Roubo/Hacker);

Erro de operação ou usuário;

70% das invasões são internas.

# Quebra de Segurança - Casos

Bank of America Corp. perdeu informações de 1.2 milhões de funcionários federais;

San Jose Medical Group sofreu ataque e roubo de dados referente a 185.000 pacientes;

LexisNexis Group sofreu roubo de dados referente a 310.000 pessoas;

HSBC Britânico: um (verme) worm roubou dados de créditos de 180.000 clientes;

Epsilon: 60 milhões de emails vazados;

monster.com: vazamento de dados;

Visa: prejuízo de US\$ 68 milhões;

Google, Adobe, Yahoo, Symantec.

# Intrusões – Impactos

Imagem e reputação



# Intrusões – Impactos

Perda de confiança de clientes



# Intrusões – Impactos

Benefícios competitivos



# Segurança em Banco de Dados - Camadas

**Cliente**

**Aplicação**

**Web/Apl Server**

**Rede**

**Bando de Dados**

**Sistema Operacional**

**Servidor (Físico)**



# Segurança em Banco de Dados - Recomendações

Evite nomes simples para usuários como “oracle”

Limite o acesso para contas de proprietários do usando mecanismos como “sudo”.

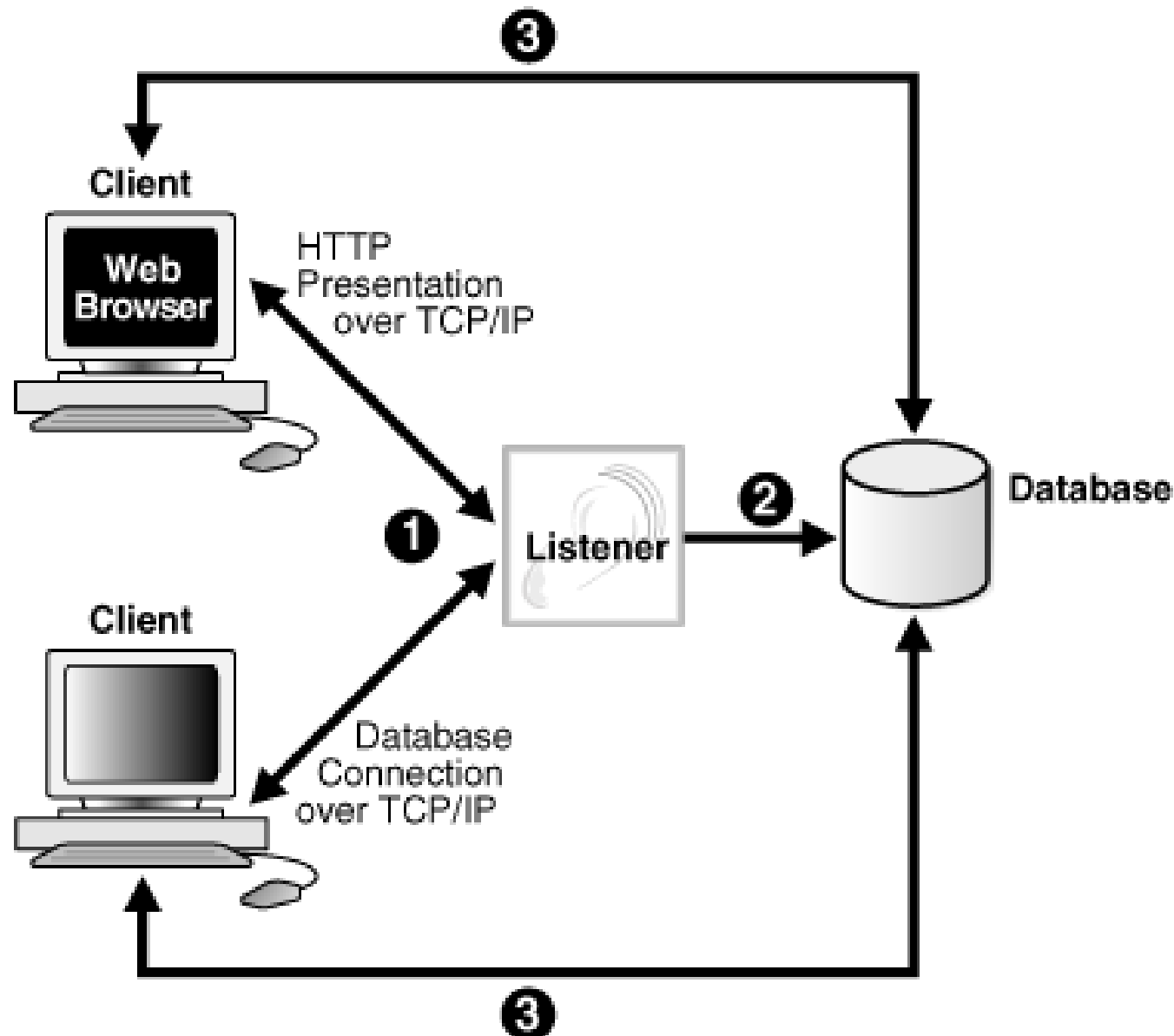
Crie diferentes usuários para cada componente do gerenciador de banco de dados.

Examples:


Oralsnr – listener

Oradb – database

# Listeners






















# Listeners

 **Serviços (local)**

**Logon secundário**

[Parar](#) o serviço  
[Pausar](#) o serviço  
[Reiniciar](#) o serviço

Descrição:  
Ativa a inicialização de processos sob credenciais alternadas. Se este serviço for interrompido, este tipo de acesso por logon não estará disponível. Se este serviço for desativado, quaisquer serviços que dele dependam diretamente não serão iniciados.

Nome ▲	Descrição	Status	Tipo de inicializaçã
 Logon secundário	Ativa a iniciali...	Iniciado	Automático
 Logs e alertas de desempenho	Coleta dados...		Manual
 Machine Debug Manager	Supports loca...	Iniciado	Automático
 Microsoft .NET Framework NGEN v4.0.30319_X86	Microsoft .NE...		Automático
 Mozilla Maintenance Service	O Serviço de ...		Manual
 Net.Tcp Port Sharing Service	Provides abili...		Desativado
 Notificação de eventos de sistema	Rastreia eve...	Iniciado	Automático
 Office Source Engine	Salva os arqu...		Manual
 Office Software Protection Platform	Office Softw...	Iniciado	Manual
 OracleJobSchedulerXE			Desativado
 OracleMTSRecoveryService			Manual
 OracleServiceXE		Iniciado	Manual
 OracleXEClrAgent			Manual
 OracleXETNSListener		Iniciado	Manual
 Plug and Play	Permite que ...	Iniciado	Automático
 Portable Media Serial Number Service	Retrieves the...		Manual
 QoS RSVP	Fornece a fu...		Manual
 Reconhecimento de local da rede (NLA)	Reúne e arm...	Iniciado	Manual
 Remote Packet Capture Protocol v.0 (experimental)	Allows to cap...		Manual

# Segurança em Banco de Dados - Recomendações

Usuários de instalação devem ser locais;

Somente associe administradores de banco de dados a grupos como ORA\_DBA / OSDBA;

Verificar contas de usuários criadas durante a instalação (default);

Verificar senhas fracas.

# Acesso ao Banco de Dados

Criar papéis manualmente (customizar).

Utilize senhas para proteger DML.

Sempre verifique usuários com privilégios como:  
“all privileges”, “any”, “with admin”, “with grant”.

# Acesso ao Banco de Dados

Sempre verifique concessões para DDL “CREATE LIBRARY”, “ALTER SYSTEM” ou “CREATE PROCEDURE”.

Verifique concessões “CREATE ANY DIRECTORY”.

Verifique quais usuários tem concessão para: “CREATE JOB” or “CREATE ANY JOB” privilege (10G).

Monitore objetos armazenados na tablespace SYSTEM.

# Acesso ao Banco de Dados

Verifique a necessidade de manter privilégios em papéis (role) como: RESOURCE, CONNECT, “CREATE ANY TRIGGER”.

Verifique quais usuários tem acesso ao dicionário de dados.

Verifique quais usuários tem privilégios como “SELECT ANY TABLE”.

```
select * from USER_ROLE_PRIVS where USERNAME='SAMPLE';
```

# Segurança em Rede de Trabalho

Criar listeners separados para diferentes grupos de usuários.

Configure o Oracle para utilizar firewall nativo (Windows, Linux etc)

Limite as conexões a pequenas listas de IPs.



# Leitura Recomendada

Oracle Database Security Benchmark -  
[http://www.cisecurity.org/bench\\_oracle.html](http://www.cisecurity.org/bench_oracle.html)

SANS Oracle Database Checklist -  
[http://www.sans.org/score/checklists/Oracle\\_Database\\_Checklist.pdf](http://www.sans.org/score/checklists/Oracle_Database_Checklist.pdf)

Oracle Security Papers -  
<http://www.petefinnigan.com/orasec.htm>

Oracle 10G – Security Guide  
Protecting Oracle Databases – white paper

# Sites Recomendados

<http://www.petefinnigan.com/>

<http://www.cisecurity.org/>

<http://www.protegrity.com/>

<http://www.nextgenss.com/>

<http://www.appsecinc.com/>

<http://www.sans.org/>

<http://www.iss.net/>

<http://www.securityfocus.com/>

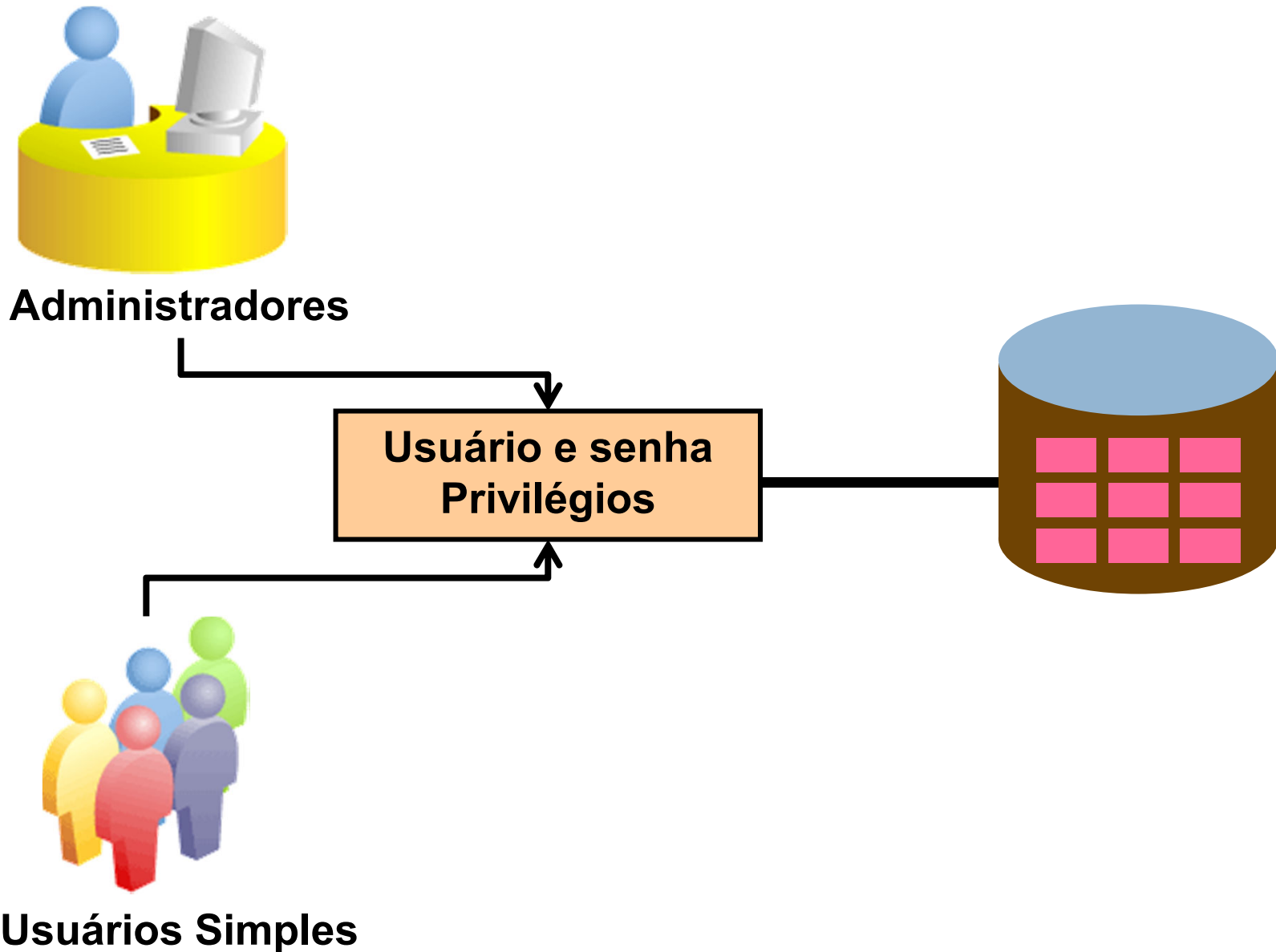
<http://otn.oracle.com/deploy/security>

<http://www.computerworld.com/securitytopics/security>

# Controle de Usuários

- Objetivos:
  - Diferenciar privilégios de sistema de privilégios de objetos.
  - Concessão de privilégios a tabelas.
  - Visão de privilégios em dicionário de dados.
  - Concessão de papéis (roles).
  - Distinção entre privilégios e regras.

# Controle de Acesso a Usuários

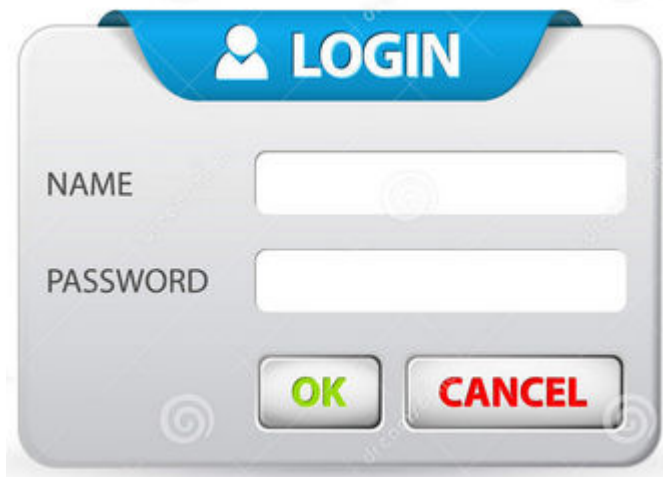


# Controle de Acesso a Usuários

## Segurança do Banco de Dados

Segurança de Sistema

Login e  
Controle de Acesso



LOGIN

NAME

PASSWORD

OK CANCEL

Segurança de dados

Tabelas e Colunas

	Col 1	Col 2	Col 3	Col 4	Col 5
Row 1	1	2	3	4	5
Row 2	1	2	3	4	5
Row 3	1	2	3	4	5
Row 4	1	2	3	4	5
Row 5	1	2	3	4	5
Row 6	1	2	3	4	5

# Privilégios

- Privilégios de sistema: concessão de acesso ao banco de dados;
- Privilégios de dados: manipulação do conteúdo dos dados no banco de dados;

# Privilégios de Sistema

- Mais de 100 privilégios disponíveis.
- A administração do banco de dados consiste em privilégios de alto nível como:
  - Criação/Remoção de usuário.
  - Criação/Remoção de tabelas.
  - Cópia de segurança de dados em tabelas.



Universidade Federal de Mato Grosso-UFMT  
Sistemas de Informação  
Laboratório de Banco de Dados  
Prof. Clóvis Júnior

# Áreas de Trabalho (Tablespace)





# Estrutura do Banco de Dados

## Processos

Aplicativos	Processos	Desempenho	Rede	Usuários
Nome da imagem	Nome de usuário	CPU	Uso de m...	
mdm.exe	SYSTEM	00	960 K	
mspaint.exe	Clovis	00	12.428 K	
ONENOTEM.EXE	Clovis	00	328 K	
oracle.exe	SYSTEM	00	8.716 K	
OSPPSVC.EXE	NETWORK SERVICE	00	1.484 K	

## Armazenamento



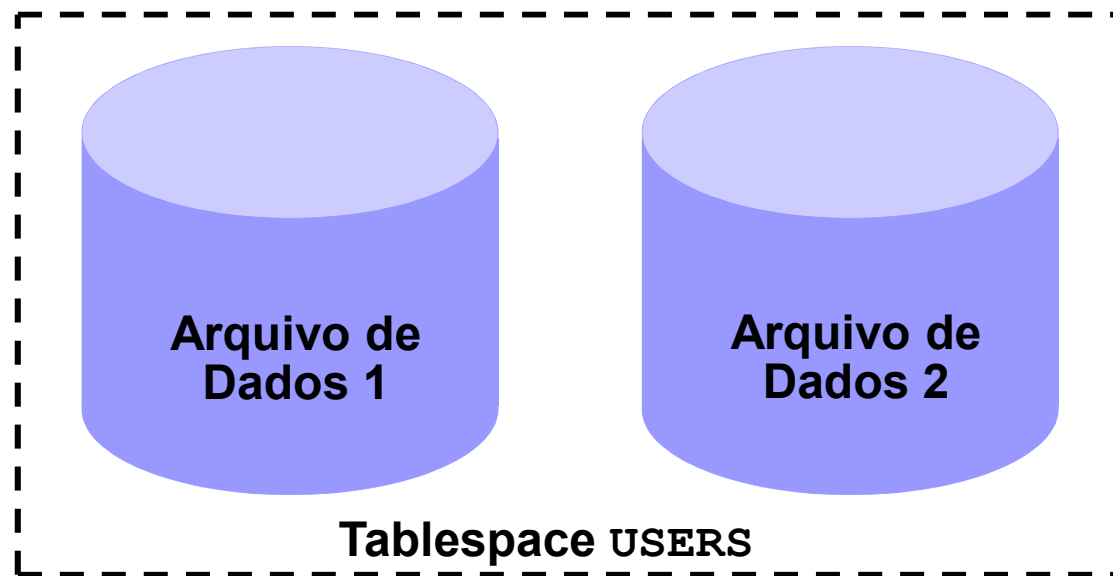
## Instância

OracleJobSchedulerXE		Desativado	Sistema local
OracleMTSRecoveryService		Manual	Sistema local
OracleServiceXE	Iniciado	Manual	Sistema local
OracleXEClrAgent		Manual	Sistema local
OracleXETNSListener	Iniciado	Manual	Sistema local

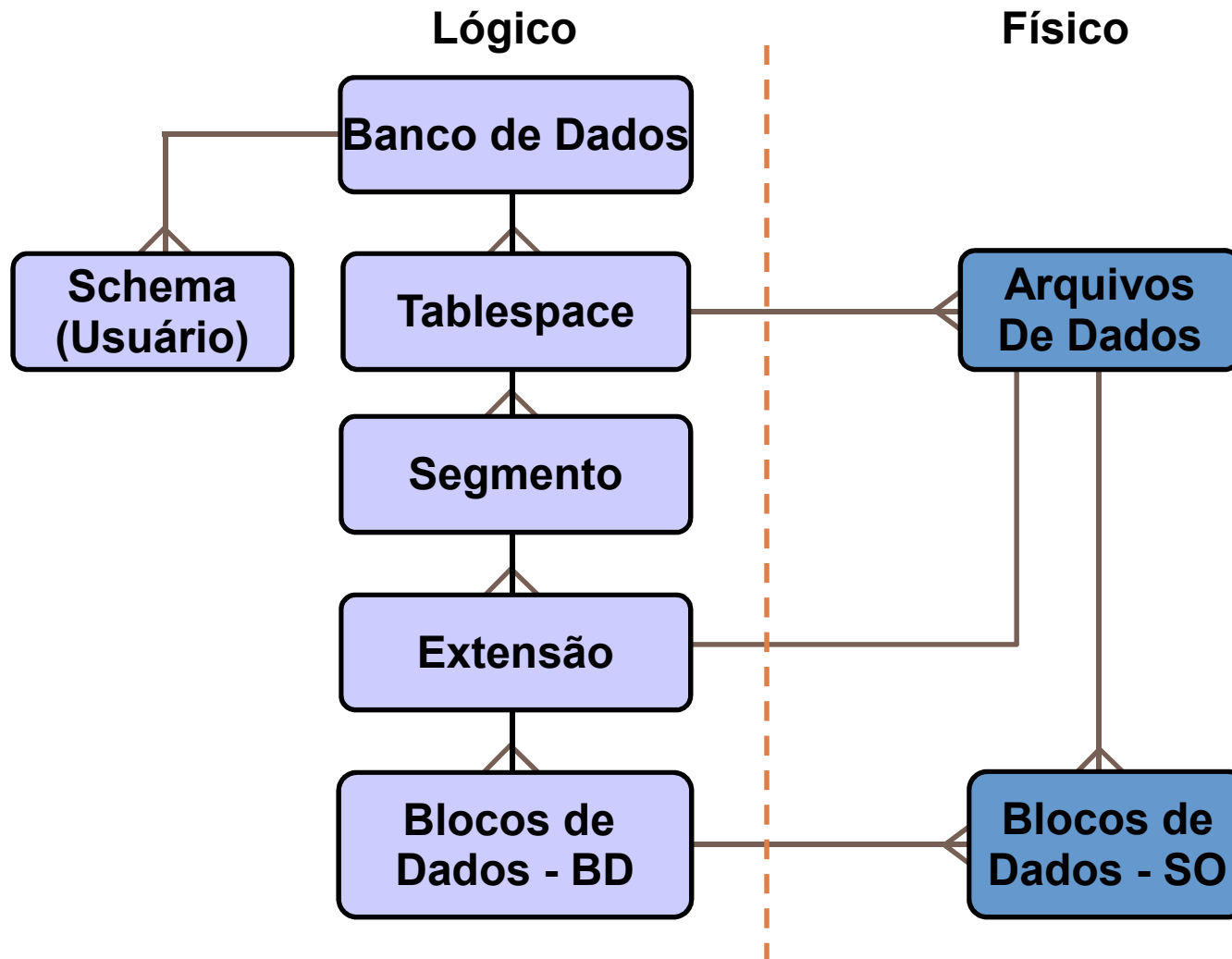
# Tablespaces e Arquivos de Dados

Tablespaces consistem de um ou mais arquivos de dados.

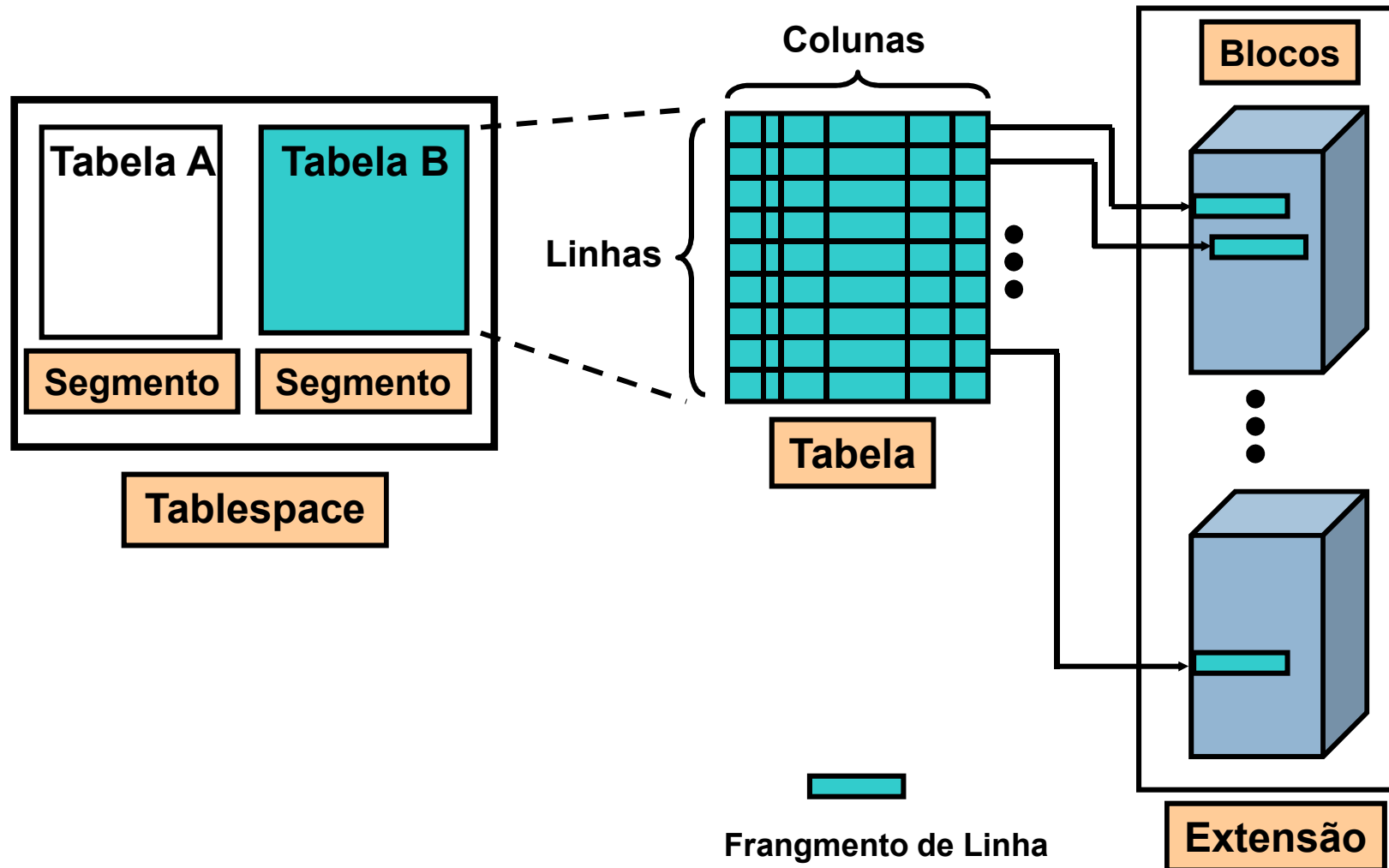
Arquivos de dados pertencem a um única tablespace.



# Estrutura Física e Lógica do BD



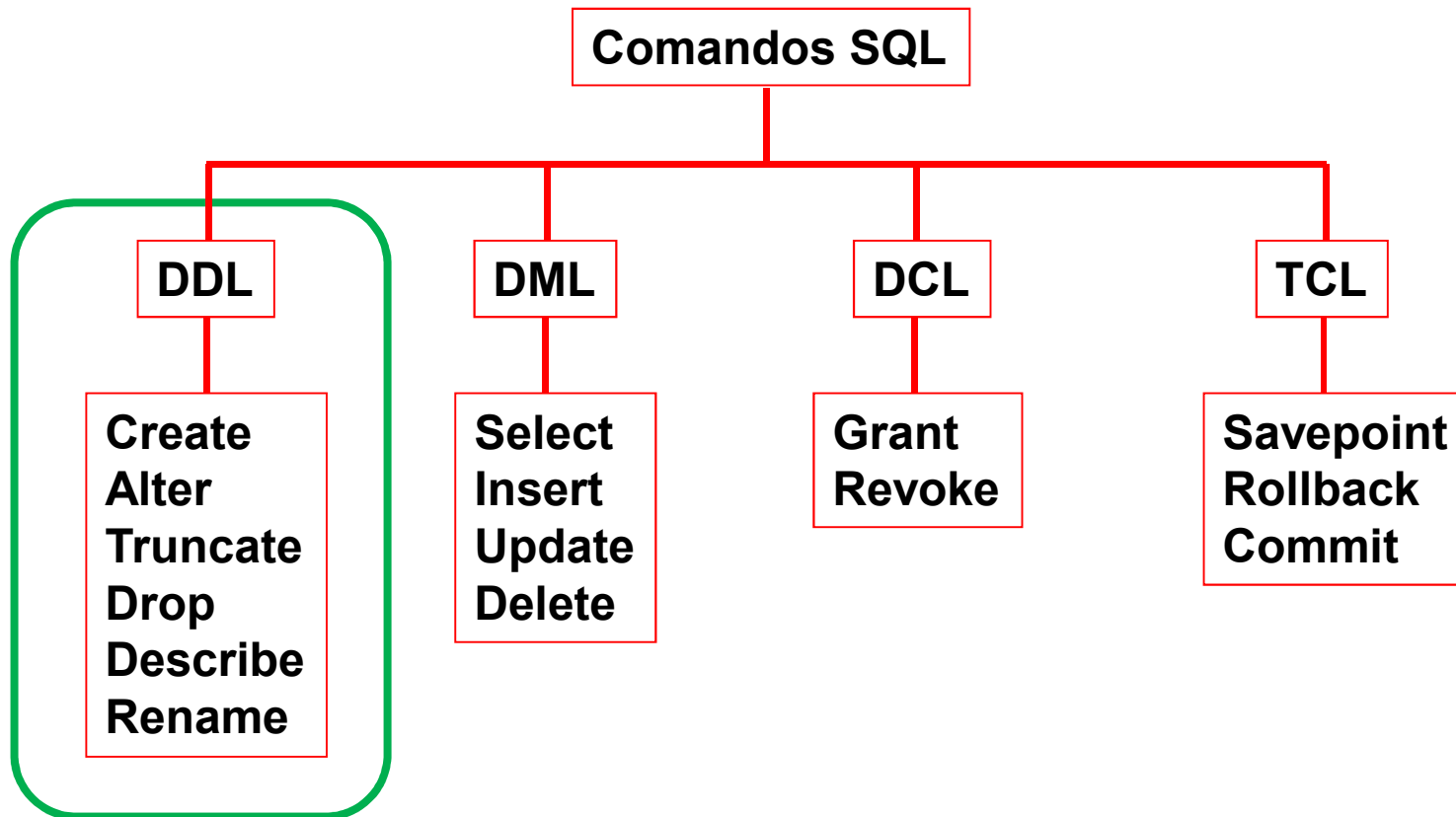
# Armazenamento de Dados em Tabelas



# Tablespaces SYSTEM and SYSAUX

- SYSTEM e SYSAUX são tablespaces obrigatórias;
- São criadas na instalação do banco de dados;
- Devem sempre estar online;
- Tablespace SYSTEM é usada pelo core;
- Tablespace SYSAUX é usada para componentes adicionais (como Enterprise Manager Repository).

# Data Definition Language



# Data Definition Language

**CREATE**



**ALTER**



**DROP**



# **Ações com Tablespaces - Criação**

```
create tablespace Dados datafile  
'c:\Oraclexe\dados.ora' size 300m  
autoextend ON next 10m;
```

```
Create user aluno2 identified by abc  
Default tablespace dados;
```

```
Grant dba,resource,connect to aluno2;
```



# Ações com Tablespaces - Exclusão

**Drop tablespace Dados;**



# Ações com Tablespaces - Visualização

**SELECT name FROM v\$tablespace**



<b>NAME</b>
SYSTEM
UNDO
SYSAUX
USERS
TEMP

# Estrutura do CREATE - DDLs

CREATE (Cria estruturas no banco de dados)

CREATE TABLESPACE NomeTableSpace;

CREATE USER NomeUsuario;

CREATE TABLE MinhaTabela(coluna tipo);

CREATE SEQUENCE MinhaSequencia:

# Estrutura do DROP e ALTER - DDLs

DROP (remove estruturas do banco de dados);

DROP TABLE Command: Todos os dados da  
tabelas serão perdidos;

DROP TABLE MinhaTabela;

DROP SEQUENCE Command:

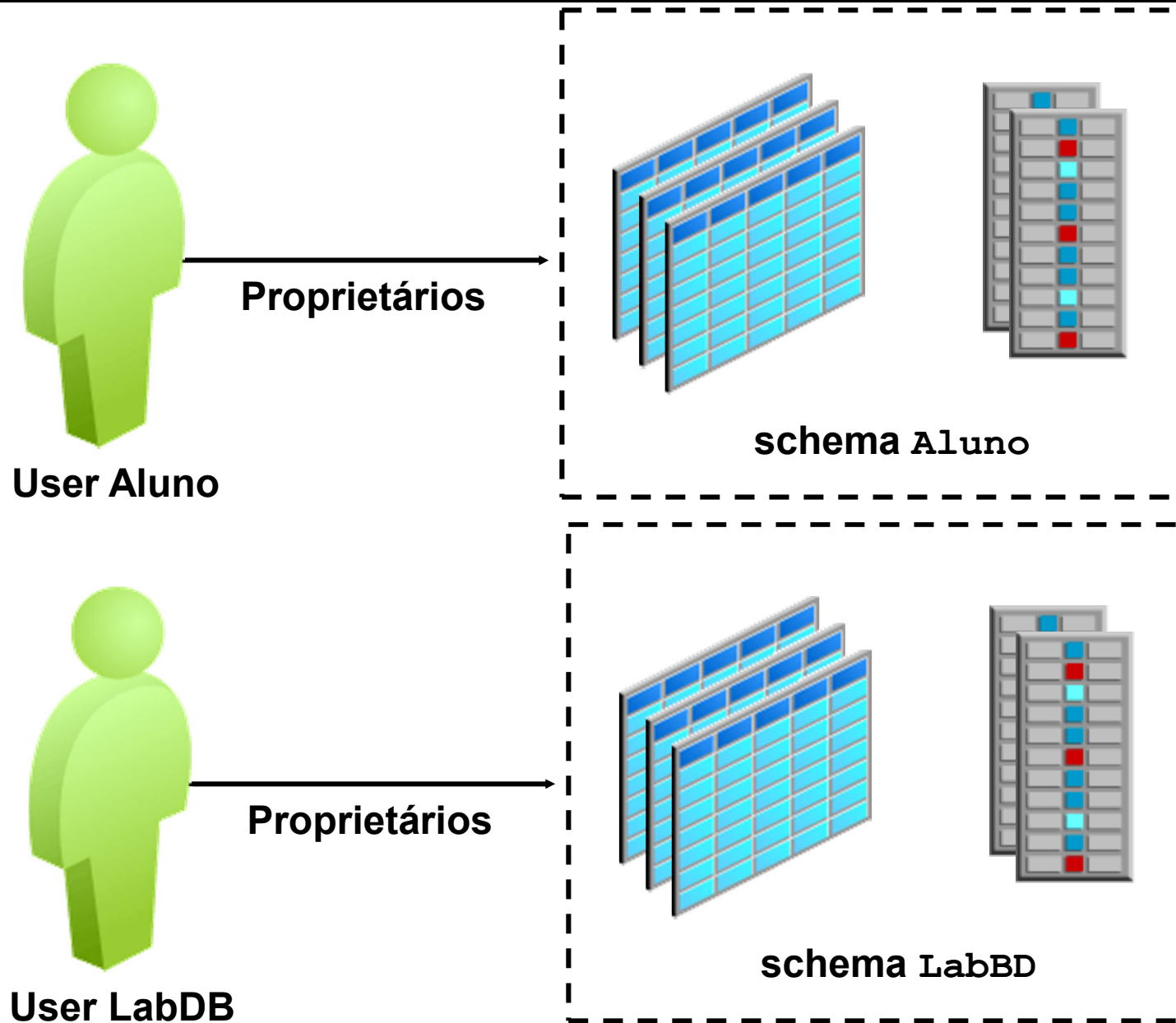
DROP SEQUENCE MinhaSequencia;

ALTER TABLE: Utilizado para  
modificar/remover/adicionar colunas;

ALTER TABLE MYTABLE DROP COLUMN MyColumn;

ALTER TABLE MYTABLE ADD C1 NUMBER(4);

# Schema



# Criação de Usuários

```
CREATE USER user  
IDENTIFIED BY password;
```

```
CREATE USER LBD IDENTIFIED BY abc DEFAULT  
TABLESPACE Dados QUOTA UNLIMITED ON Dados;
```

# Privilégios de Usuários de Sistema

- DBA pode atribuir privilégios específicos para usuários.

```
GRANT privilege [, privilege...]  
TO user [, user| role, PUBLIC...];
```

- Desenvolvedores de aplicação podem receber concessões de privilégios para:
  - CREATE SESSION (criar sessão)
  - CREATE TABLE (criar tabela)
  - CREATE SEQUENCE (criar sequencias)
  - CREATE VIEW (criar visões)
  - CREATE PROCEDURE (criar procedimentos)

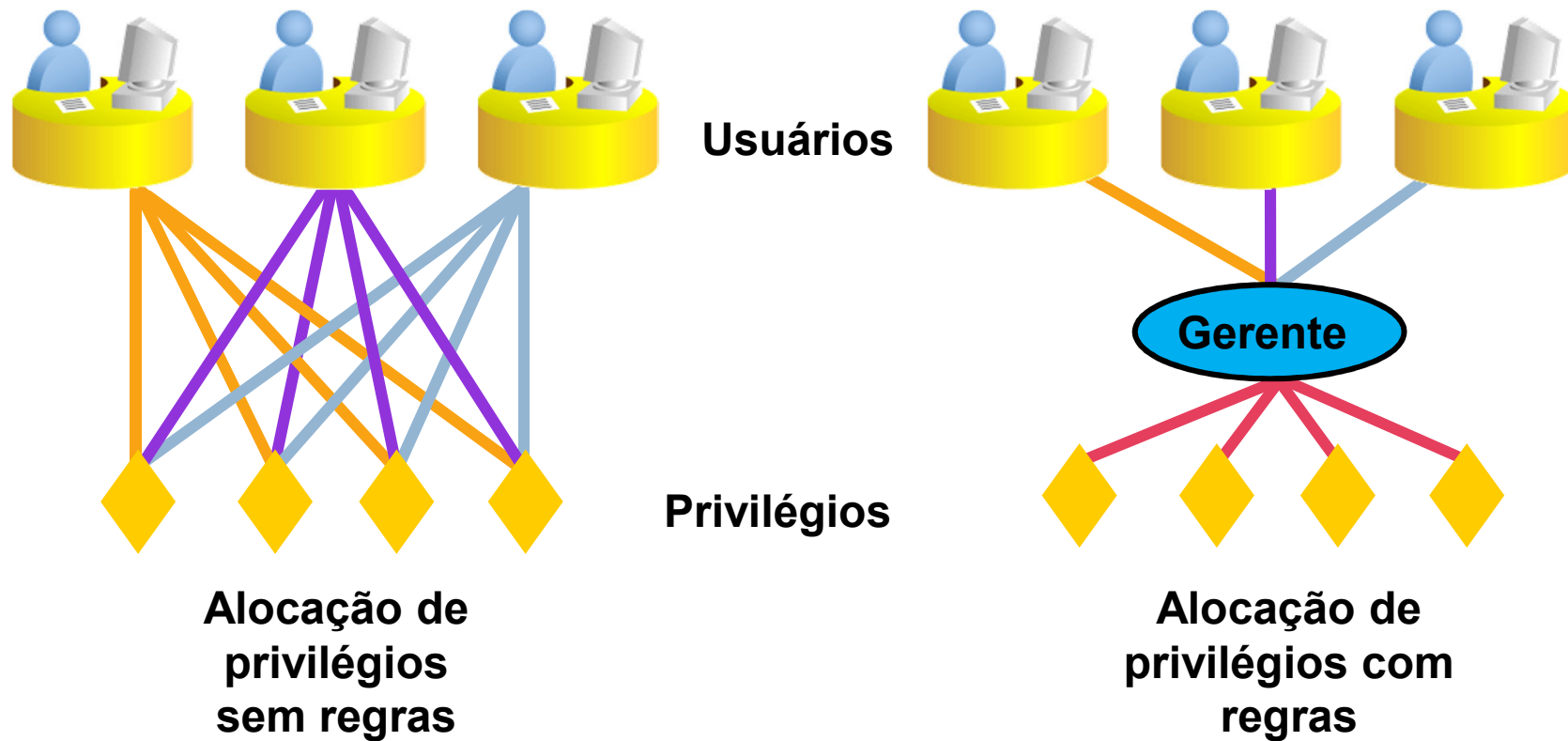
# Concessão de Privilégios de Sistema

- Especificação de privilégios (DBA).

```
GRANT dba, resource, connect TO LBD;  
Grant succeeded.
```



# Roles (Papeis)



# Benefícios de Roles (Papeis)

Facilidade no gerenciamento de privilégios

Gerenciamento dinâmico de privilégios

Disponibilização seletiva de privilégios



# Criação de Roles (Papeis)

```
CREATE ROLE gerente;
```

Role created.

```
GRANT create table, create view  
TO gerente;
```

Grant succeeded.

```
GRANT gerente TO NOME;
```

Grant succeeded.

# Alteração de Senha

- Usuários e senhas iniciais são definidas por DBAs.
- Modificações de senhas podem ser realizadas pelo próprio usuário (ALTER USER).

```
ALTER USER LBD  
IDENTIFIED BY EFG;  
User altered.
```

# Privilégios de Objetos

Privilégio (Objeto)	Tabela	View	Sequence	Procedure
ALTER	√		√	
DELETE	√	√		
EXECUTE				√
INDEX	√			
INSERT	√	√		
REFERENCES	√			
SELECT	√	√	√	
UPDATE	√	√		

# Privilégios de Objetos

- Privilégios dependem do tipo de objeto.
- Proprietários tem controle total sobre o objeto.
- Proprietários podem conceder privilégios específicos para outros usuários.

```
GRANT      object_priv [ (columns) ]  
ON         object  
TO         { user | role | PUBLIC }  
[WITH GRANT OPTION] ;
```

# Concessão de Privilégios para Objetos

- Concessão de consultas para tabela FUNCIONARIOS.

```
GRANT  select
ON      funcionarios
TO      maria;
Grant succeeded.
```

- Concessão de privilégios para atualização de colunas específicas à usuários e roles.

```
GRANT  update (Nome_departamento, CodigoCidade)
ON      departamentos
TO      usuario1, gerente;
Grant succeeded.
```

# Concedendo Privilégios

- Transfere concessões com os privilégios.

```
GRANT  select, insert
ON      departments
TO      usuario1
WITH    GRANT OPTION;
Grant succeeded.
```

- Permite que todos os usuários do sistema consultemos dados da tabela DEPARTAMENTOS do usuário LBD.

```
GRANT  select
ON      lbd.departments
TO      PUBLIC;
Grant succeeded.
```



# Revogando Privilégios

- Privilégios concedidos a usuários podem ser excluídos ou revogados (REVOKE).
- Concessões de privilégios pode ser revogadas (WITH GRANT OPTION).

```
REVOKE {privilege [, privilege...] | ALL}
ON      object
FROM    {user[, user...] | role | PUBLIC}
[CASCADE CONSTRAINTS];
```

# Criação de Tabelas

```
CREATE TABLE nome_tabela □  
    ( { nome_coluna data_type [  
    DEFAULT default_expr ] [ column_constraint [,  
    ... ] ] | table_constraint } [, ... ] )
```

# Tipos de Dados

Linguagens de  
Programação

Oracle

**String**

**CHAR**

**Varchar**

**Varchar2**

**Integer**

**Integer**

**Real**

**Number**

**Decimal**

**(Depende da Ling. Prog.)**

**Date**

**Inexistente**

**Long**

**Inexistente**

**Long Raw**

## Criação de Tabelas

```
Create table Cliente  
( codigo number(5),  
  nome varchar2(50),  
  salario number(8,3)  
);
```

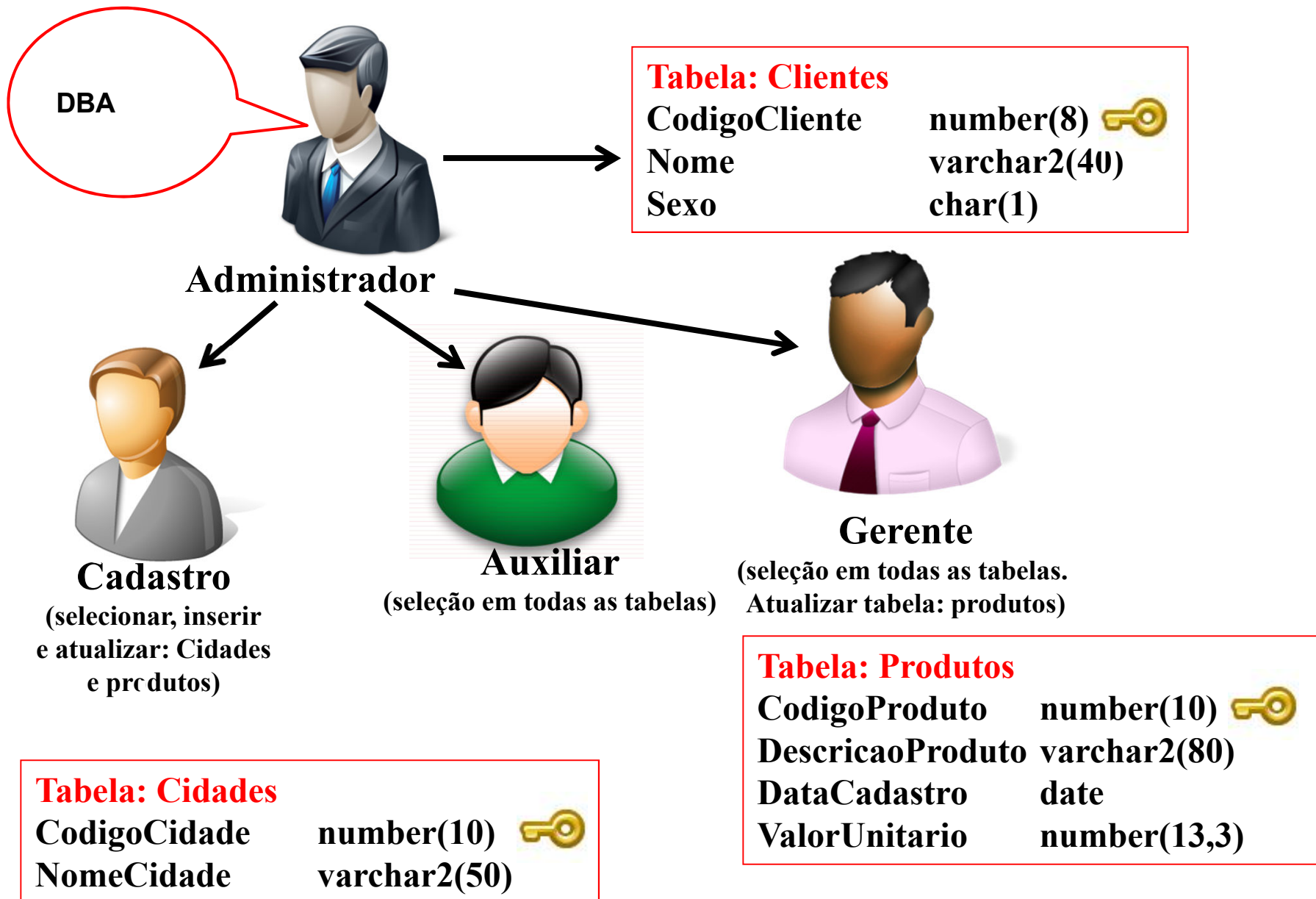
# Inserção de Dados em Tabelas

```
INSERT INTO clientes (Codigo,Nome,Salario)  
VALUES (1,'José dos Santos',500);
```

```
INSERT INTO clientes (Codigo,Nome,Salario)  
VALUES (2,'Marina da Silva',600);
```

```
INSERT INTO clientes (Codigo,Nome,Salario)  
VALUES (3,'Carlos de Souza',700);
```

# Exercícios: Privilégios para Usuários - Estoque



# Exercícios: Privilégios para Usuários - Universidade

