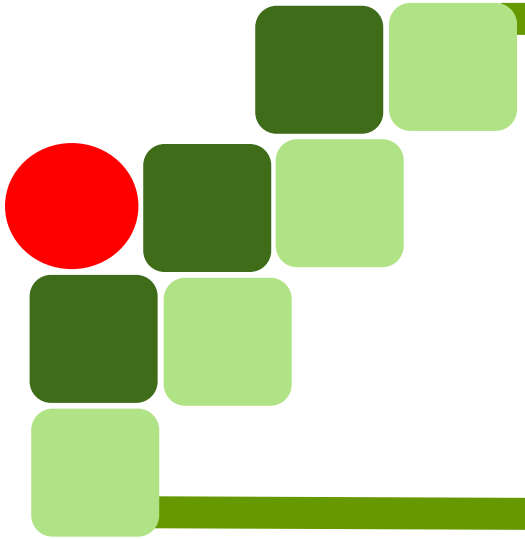
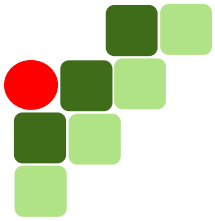


Banco de Dados II

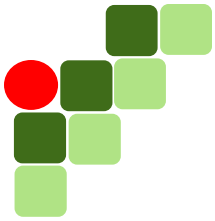
Cristiane Yaguinuma
cristiane.yaguinuma@ifsp.edu.br

- Gerenciamento de usuários e privilégios



Roteiro da aula

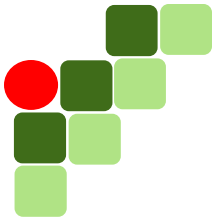
- Gerenciamento de usuários
  - CREATE / ALTER / DROP USER
- Privilégios
  - Privilégios de Sistema
  - Privilégios de Objetos
  - GRANT
  - ROLE
  - REVOKE
- Exercícios



Gerenciamento de usuários

- Para acessar um BD, um usuário deve conectar ao servidor de usando um nome de usuário válido

- Comandos para gerenciar usuários
  - CREATE / ALTER / DROP USER
  - São executados somente por usuários que tenham privilégio de administrador



CREATE USER

```
CREATE USER <nome_usuario>
IDENTIFIED BY <senha>;
```

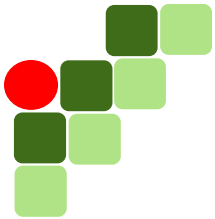
```
CREATE USER USER1
IDENTIFIED BY abc
DEFAULT TABLESPACE USERS
QUOTA 10M ON USERS
TEMPORARY TABLESPACE TEMP;

GRANT CREATE SESSION
TO USER1;
```

ALTER / DROP USER

```
ALTER USER USER1
IDENTIFIED BY senha123;
```

```
ALTER USER USER1 QUOTA UNLIMITED ON USERS;
```

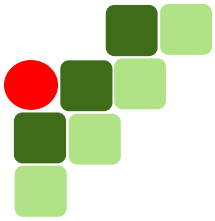
```
DROP USER USER1;

-- se o usuário tiver objetos de BD
DROP USER USER1 CASCADE;
```



Exercícios

- Crie três usuários (deve conectar como SYSTEM):
  - USER1 – senha ‘USER1’
  - USER2 – senha ‘USER2’
  - USER3 – senha ‘USER3’

- Atribua aos usuários criados:
  - DEFAULT TABLESPACE "USERS"
  - TEMPORARY TABLESPACE "TEMP"
  - Com cota de 5M para tablespace USERS
  - Privilégio CREATE SESSION

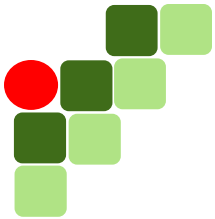


Privilégios

- Privilégios são autorizações para:
  - Executar um tipo específico de comando SQL
  - Acessar um objeto que pertence a outro usuário
  - Executar um pacote PL/SQL

- Privilégios de Sistema
  - Para conseguir acesso ao banco de dados

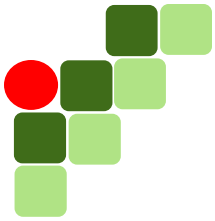
- Privilégios de Objetos
  - Para manipular o conteúdo dos objetos do banco de dados



Privilégios de Sistema

- Existem mais de 100 privilégios de sistema disponíveis no Oracle

- O DBA (administrador do BD – usuário SYSTEM ou SYS) tem privilégios de sistema de alto nível para tarefas como:
  - Criar novos usuários
  - Remover usuários
  - Remover tabelas
  - Fazer backup de tabelas

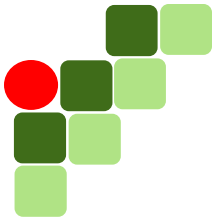


GRANT

- Depois de criar um usuário, o DBA pode conceder privilégios específicos a ele

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

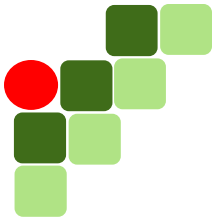
- Um projetista de BD, por exemplo, pode ter os seguintes privilégios de sistema:
  - CREATE SESSION
  - CREATE TABLE
  - CREATE SEQUENCE
  - CREATE VIEW



Privilégios de Sistema

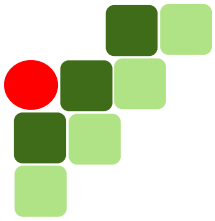
```
-- COMO USUÁRIO SYSTEM
GRANT CREATE SESSION,
      CREATE TABLE,
      CREATE SEQUENCE,
      CREATE VIEW
TO USER1;
```

- Um novo usuário somente pode conectar ao BD se tiver o privilégio CREATE SESSION (Oracle)



Exercícios

- Faça o teste de conexão de USER1 e dos privilégios de sistema recebidos
  - Crie a tabela Emp (emp_id, nome, salario)
  - Crie uma sequência emp_id_seq para gerar valores para emp_id
  - Crie a visão emp_view sobre a tabela Emp que retorne somente emp_id e nome (não retorna salário)



Roles

- Role é um grupo de privilégios relacionados que pode ser concedido aos usuários
- Criação de um role

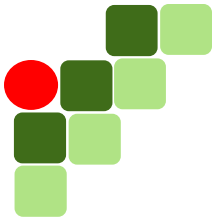
```
CREATE ROLE gerente;
```

- Atribuir privilégios a um role

```
GRANT CREATE TABLE, CREATE VIEW, CREATE SESSION
TO gerente;
```

- Atribuir o role para usuários

```
GRANT gerente TO USER2;
```

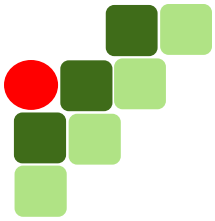


WITH ADMIN OPTION

- Quem recebe o privilégio ou o role pode atribuí-lo para outros usuários
- Pode revogar o privilégio ou o role para outros usuários

```
GRANT CREATE SESSION TO USER2 WITH ADMIN OPTION;
```

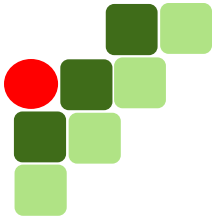
```
GRANT gerente TO USER2 WITH ADMIN OPTION;
```



Privilégios de Objetos

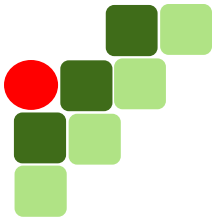
- Um privilégio de objeto é um direito concedido a um usuário ou um role sobre um objeto do BD
  - Atualizar uma tabela
  - Consultar linhas de tabelas
  - Executar um procedimento

- Para conceder um privilégio de objeto
  - O usuário deve ser proprietário do objeto ou
  - Tem o privilégio de sistema GRANT ANY OBJECT PRIVILEGE (DBA) ou
  - Recebeu GRANT com a cláusula WITH GRANT OPTION



Privilégios de Objetos

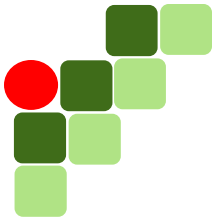
Privilégio de objeto	TABLE	VIEW	SEQUENCE	PROCEDURE
ALTER	✓		✓	
INSERT	✓	✓		
SELECT	✓	✓	✓	
UPDATE	✓	✓		
DELETE	✓	✓		
REFERENCES	✓			
EXECUTE				✓



Privilégios de Objetos

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

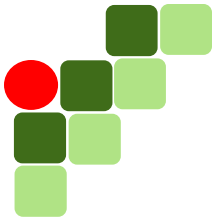
```
GRANT SELECT, UPDATE
ON USER1.emp
TO USER2;
```



Privilégios de Objetos

```
GRANT SELECT
ON HR.DEPARTMENTS
TO PUBLIC;
```

```
GRANT ALL
ON USER1.EMP
TO USER2;
```

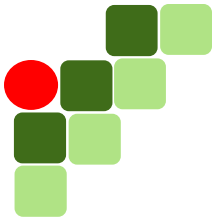


Privilégios sobre colunas específicas

- É possível conceder privilégios INSERT, UPDATE ou REFERENCES sobre colunas específicas de uma tabela

```
GRANT INSERT (department_id, department_name)
ON HR.DEPARTMENTS
TO USER1;
```

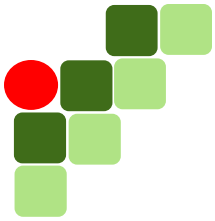
- No caso de INSERT, verifique quais colunas são NOT NULL, para evitar erros de integridade



Privilégios sobre colunas específicas

- Atribuir ao usuário USER2 o privilégio REFERENCES sobre a coluna emp_id da tabela emp do usuário USER1

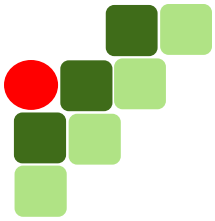
```
GRANT REFERENCES (emp_id)
ON USER1.emp
TO USER2;
```



Privilégios sobre colunas específicas

- Desta forma, o usuário USER2 pode criar uma tabela que referencia a coluna emp_id de USER1

```
CREATE TABLE dependente (
        dep_id NUMBER(6) PRIMARY KEY,
        dep_name VARCHAR2(50),
        emp NUMBER(6)
                REFERENCES USER1.emp(emp_id)
);
```



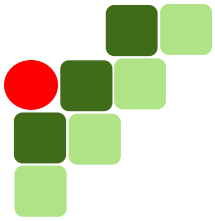
WITH GRANT OPTION

- Atribuir a um usuário a autoridade de conceder seus privilégios sobre o objeto:

```
GRANT SELECT
ON USER1.emp
TO USER2
WITH GRANT OPTION;
```

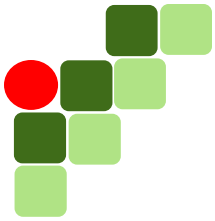
- Assim, USER2 poderá repassar os privilégios recebidos para outros usuários

```
GRANT SELECT
ON USER1.emp
TO USER3;
```



Consultando privilégios concedidos

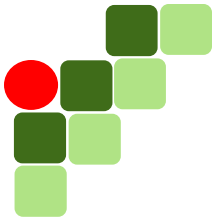
Visão do dicionário de dados	descrição
USER_SYS_PRIVS	Privilégios de sistema concedidos ao usuário
USER_ROLE_PRIVS	Roles acessíveis pelo usuário
USER_TAB_PRIVS_MADE	Privilégios de objeto concedidos
USER_TAB_PRIVS_RECD	Privilégios de objeto recebidos
USER_COL_PRIVS_MADE	Privilégios de objeto concedidos sobre colunas específicas
USER_COL_PRIVS_RECD	Privilégios de objeto recebidos sobre colunas específicas
ROLE_SYS_PRIVS	Privilégios de sistema concedidos a roles
ROLE_TAB_PRIVS	Privilégios de objeto concedidos a roles



Exercícios

- Atribuir ao USER3 os privilégios de:
  - Consultar valores do sequence do USER1
  - inserir e atualizar emp_id e nome da tabela emp de USER1

- Atribuir a qualquer usuário o privilégio de consulta aos dados da view emp_view de USER1

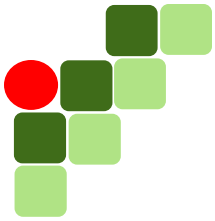


REVOKE

- Para revogar privilégios concedidos a outros usuários

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

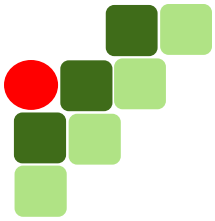
```
REVOKE SELECT
ON HR.DEPARTMENTS
FROM PUBLIC;
```



REVOKE

- Como usuário SYSTEM, revogue os privilégios SELECT e INSERT da tabela DEPARTMENTS concedidos ao usuário USER1:

```
REVOKE SELECT, INSERT
ON HR.DEPARTMENTS
FROM USER1;
```

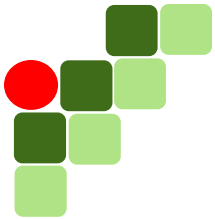


REVOKE e WITH GRANT OPTION

- Quando um privilégio recebido por WITH GRANT OPTION é revogado, os demais GRANTs na sequência são revogados também

```
REVOKE SELECT
ON USER1.emp
FROM USER2;
```

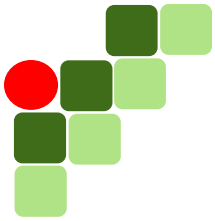
- Assim, todos os usuários que receberam esse GRANT pelo `USER2` também vão perder os privilégios



Exercícios

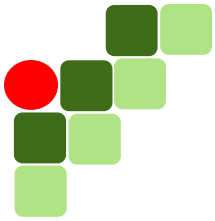
- Revogar o privilégio de inserir na tabela USER1.emp para todos usuários

- Revogar todos os privilégios da tabela USER1.emp para USER3



Resumo

Comando	Ação
`CREATE USER`	Cria um usuário (normalmente por DBA)
`GRANT`	Concede privilégios sobre objetos a outros usuários
`CREATE ROLE`	Cria uma coleção de privilégios (normalmente executado por um DBA)
`ALTER USER`	Modifica o password de um usuário
`REVOKE`	Revoga privilégios sobre objetos de usuário



Referências

- Oracle Database Security Guide
  - Administering User Privileges, Roles, and Profiles
- Oracle® Database Security Guide 11*g* Release 2
  - Configuring Privilege and Role Authorization