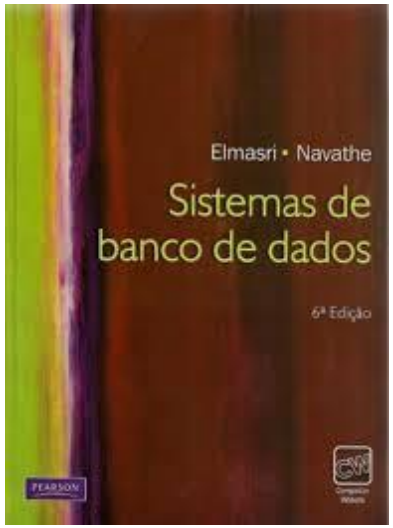
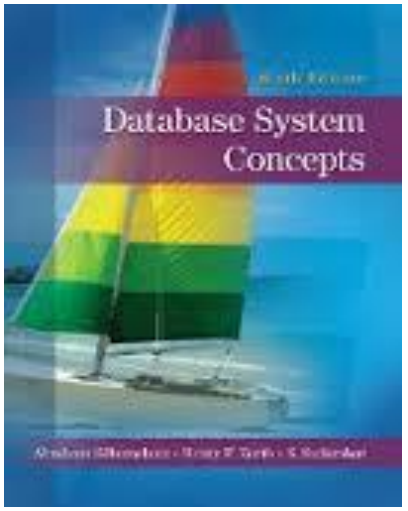
Unidade 24 – Noções de Segurança de Banco de Dados

Prof. Aparecido V. de Freitas
Doutor em Engenharia
da Computação pela EPUSP
aparecidovfreitas@gmail.com

Bibliografia



Sistemas de Banco de Dados
Elmasri / Navathe 6ª edição



Sistema de Banco de Dados
Korth, Silberschatz – Sixth Editon

Introdução

- ✓ Uma das maiores preocupações em computação tem sido **segurança da informação;**
- ✓ Nos dias atuais, com o uso da **Internet** os sistemas tornam-se onipresentes, entretanto também **vulneráveis** a ataques maliciosos;
- ✓ Portanto, os SGBDs trazem **uma camada de segurança** que visa compor o arsenal de segurança da informação numa corporação.

Introdução

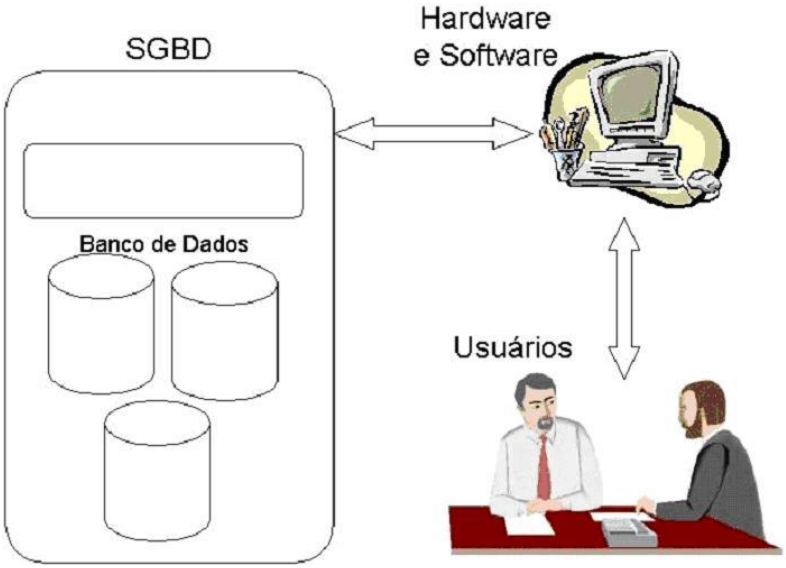
- ✓ **Segurança** em Banco de dados diz respeito à **proteção** do banco de dados contra **acesso/alteração intencionais** ou **não,** utilizando-se ou **não** de meios computacionais;

- ✓ **Áreas envolvidas:**
  - roubo e fraude
  - perda de confidencialidade e privacidade
  - perda de integridade
  - perda de disponibilidade

Introdução

- ✓ O **subsistema** de **segurança** é responsável por **proteger** o BD contra o **acesso** não autorizado;

- ✓ Formas de acesso não autorizado:
  - leitura não autorizada
  - modificação não autorizada
  - remoção de dados não autorizada



Introdução

- O **DBA** (**Data Base Administrator**, ou **super user**) tem plenos poderes para conceder e revogar privilégios a usuários.

  - Criação de contas
  - Concessão/Revogação de privilégios
  - Definição do nível de segurança

Introdução

- Controles de segurança **computacionais**

  - ✓ Adiciona-se **uma camada** à segurança provida pelo SO
  - ✓ **Autorização e autenticação**
  - ✓ Backup e recovery
  - ✓ Integridade
  - ✓ Stored procedures
  - ✓ Criptografia
  - ✓ Auditoria
  - ✓ Views

Procedimentos de Segurança

- Política de **segurança** e plano de **contigência**;
- Posicionamento **seguro** de equipamentos;
- Controle de acesso **física**;
- **Manutenção**.

Abordagens para Segurança

- **Controle de acesso mandatório:**
  - ✓ A cada **usuário** é dado um **certo nível de acesso**
    - Por exemplo: **DBA**, administradores, usuários avançados e usuários clientes;
    - Cada classe com um determinado conjunto de possibilidades pré-definidas.
- **Controle de acesso discreto:**
  - ✓ Um dado **usuário** tem direitos de acesso (**privilégios**) diferentes em **objetos** diferentes
    - Por exemplo: o usuário **Andre** só pode ler as tabelas Cliente e Produto e executar o procedimento CalculaTotalDeCompras

Privilégios

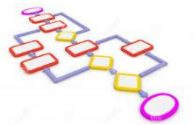
Proteçao	Privilégio	Aplica-se a
Ver	SELECT	Tabelas métodos invocados
Criar	INSERT	Tabelas
Modificar	UPDATE	Tabelas
Remover	DELETE	Tabelas
Referenciar	REFERENCES	Tabelas
Ativar	TRIGGER	Tabelas
Executar	EXECUTE	Stored procedures

Controle de Acesso

- ✓ Perante um **acesso indevido**, o que se espera do **SGBD** é o mesmo tratamento dado à tentativa de acesso à uma tabela **inexistente** (“**no such table**”).

- ✓ Portanto, se um usuário tentar acessar uma tabela no qual ele não tem privilégios para tal o erro deverá ser do tipo:

“Either no such table or you have no privilege on the table”



Criação de usuários

- O criador de um objeto é o **dono do objeto** e assim tem **todos** os **privilégios** sobre o objeto, podendo autorizar a outros usuários alguns (ou todos) destes privilégios.

- O usuário tem um **auth_ID** criado pelo **DBA**:

  CREATE USER usuario

  IDENTIFIED BY senha

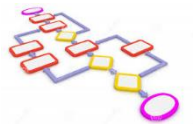
  - Alguns **SGBDs** permitem que o usuário use o **mesmo login e senha do SO;**
  - **Simplifica** a autenticação;

- Quando um usuário é criado, ele tem associado a ele um conjunto de objetos dos quais ele é dono e sobre os quais pode definir o controle de acesso.

- **Privilégios** são atribuídos/revogados para:
  - **Usuários**
  - **Papéis** (Roles)

Privilégios de Sistema do Usuário

- ✓ Depois de criar um usuário, o DBA pode conceder privilégios de sistema específicos a ele.
  - ✓ **GRANT privilegio1 [, privilegio2...]**
  - ✓ **TO usuario1 [, usuario2 | perfil, PUBLIC...];**
- ✓ Por exemplo, dois usuários (**user25415** e **user2398**) desenvolvedores de aplicativos podem ter os privilégios de sistema a seguir:
  - ✓ CREATE SESSION
  - ✓ CREATE TABLE
  - ✓ CREATE SEQUENCE
  - ✓ CREATE PROCEDURE
  - ✓ GRANT CREATE SESSION, CREATE TABLE, CREATE SEQUENCE, CREATE PROCEDURE TO **user25415**, **user2398**



Usuários e Papéis

- ✓ **Papel** (Role)
  - É um identificador ao qual atribui-se um **conjunto** de privilégios;
  - Um papel pode ser associado a diferentes usuários;
  - Pode-se inclusive ao criar um papel usar **outros papéis** já cadastrados.

Criando, Designando e Mantendo Atribuições

- ✓ Exemplo de criação de papel (**ROLE**):

CREATE ROLE desenvolvedores;

GRANT CREATE SESSION TO desenvolvedores;
GRANT CREATE TABLE TO desenvolvedores;
GRANT CREATE PROCEDURE TO desenvolvedores;

GRANT SELECT, **UPDATE ON** tabela01 **TO** desenvolvedores;

GRANT desenvolvedores TO 3521-João;

DROP ROLE desenvolvedores;

Privilégios de Objeto

- ✓ Permite aos usuários executarem ações que afetam os dados

Privilégios de Objeto	Table	View	Sequence
ALTER	X		X
DELETE	X	X	
INDEX	X		
INSERT	X	X	
REFERENCES	X		
SELECT	X	X	X
UPDATE	X	X	

Papéis - ROLES

- ✓ Existem papéis padrão na maioria dos SGBD:

CONNECT	**CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE SYNONYM, CREATE SEQUENCE, CREATE DATABASE LINK, CREATE CLUSTER, ALTER SESSION**
RESOURCE	CREATE TABLE, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, CREATE TYPE, CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR
SCHEDULER_ADMIN	CREATE ANY JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER
DBA (ou superuser)	Inclui a maioria dos privilégios de sistema, várias outras atribuições. Não deve ser concedida a usuários que não são administradores.

Revoke

- ✓ Para **revogar** a autorização, o comando **revoke** é usado.
- ✓ Ele toma a forma quase idêntica àquela do comando grant:

Exemplos

- ✓ **revoke** select on agencia from U1, U2, U3
- ✓ **revoke** update on deposito from U1
- ✓ **revoke** references (nome-agencia) on agencia from U1

Autorização em Banco de Dados

- ✓ Com a opção WITH GRANT OPTION, um usuário que tem concedido algum privilégio pode passar esse privilégio para outros usuários.