Aula 2

Sistema Gerenciador de Banco de Dados (SGBD)

Profª Vívian Ariane Barausse de Moura

Conversa Inicial

- Visão geral de um banco de dados
  - Conceitos para o funcionamento de um BD
- Tarefas administrativas de um DBA
  - O usuário administrador
  - Criação de usuários e definições de papéis
  - Permissão de autenticação e autorização
- Aspectos de administração dos SGDBs
  - Segurança, ameaças, confidencialidade, disponibilidade, integridade, auditoria, recuperação de dados

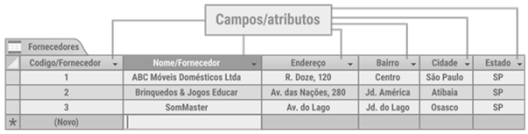
Visão geral de um SGBD

- O desempenho de um SGBD em consultas feitas comumente em operações de atualização típicas é a medida definitiva do projeto de um banco de dados
- Um administrador de banco de dados pode melhorar o desempenho medindo o tamanho do *pool* de *buffers* ou a frequência dos pontos de verificação ou adicionando *hardware* para eliminar tais gargalos

- Utiliza as terminologias: campos de registro, registros (linhas) e tabela de dados
- O campo de um registro é a menor unidade destinada ao armazenamento de valores existente em um arquivo ou tabela de um banco de dados e que pode ser referenciado por um programa aplicativo

- **Os tipos de dados básicos: caractere, numérico (com ou sem casas decimais), data, hora e lógico (valores do tipo verdadeiro ou falso)**

Figura 1 – Campos/atributos de uma tabela de banco de dados

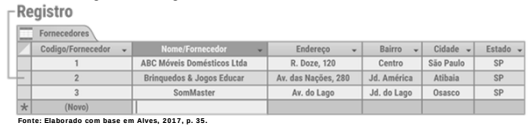


Codigo/Fornecedor	Nome/Fornecedor	Endereço	Bairro	Cidade	Estado
1	ABC Móveis Domésticos Ltda	R. Doze, 120	Centro	São Paulo	SP
2	Brinquedos & Jogos Educar	Av. das Nações, 280	Jd. América	Atibaia	SP
3	SomMaster	Av. do Lago	Jd. do Lago	Osasco	SP
(Novo)					

Fonte: Elaborado com base em Alves, 2017, p. 34.

- **Um registro (ou linhas) é o conjunto de campos que possuem valores de uma tabela**
- **Cada linha da tabela representa um registro. Nesse sentido, a tabela como um todo se resume a um agrupamento de linhas (registros) que são divididas em colunas (campos)**

Figura 2 – Registros de uma tabela de banco de dados



Codigo/Fornecedor	Nome/Fornecedor	Endereço	Bairro	Cidade	Estado
1	ABC Móveis Domésticos Ltda	R. Doze, 120	Centro	São Paulo	SP
2	Brinquedos & Jogos Educar	Av. das Nações, 280	Jd. América	Atibaia	SP
3	SomMaster	Av. do Lago	Jd. do Lago	Osasco	SP
(Novo)					

Fonte: Elaborado com base em Alves, 2017, p. 35.

- **Tabelas de dados: conjunto ordenado de registros/linhas. Cada registro possui o mesmo número de colunas (campos)**
- **Um banco de dados pode ser formado por uma ou mais tabelas, e cada uma deve ser definida de tal forma que somente possa conter um tipo de informação**
- **As aplicações normalmente utilizam várias tabelas do banco de dados. Exemplo: na geração de um relatório de vendas no mês ou o boletim escolar dos alunos**

Figura 3 – Gráfico da hierarquia de tabelas, registros e campos

Fonte: Elaborado com base em Alves, 2014, p. 36.

Figura 4 – Exemplo de definição de tabela de dados em SQL

```
CREATE TABLE cliente (
  Codigo_Cliente int(11) NOT NULL,
  Nome_Cliente varchar(50) default NULL,
  Tipo_Pessoa char(1) default NULL,
  RG char(12) default NULL,
  Orgao_Emissor varchar(6) default NULL,
  CPF char(14) default NULL,
  CNPJ char(18) default NULL,
  Inscricao_Estadual char(15) default NULL,
  Endereco varchar(50) default NULL,
  Numero char(5) default NULL,
  Bairro varchar(40) default NULL,
  Complemento varchar(20) default NULL,
  Cidade varchar(40) default NULL,
  Estado char(2) default NULL,
  CEP char(9) default NULL,
  DDD char(3) default NULL,
  Telefone char(16) default NULL,
  FAX char(16) default NULL,
  EMail char(80) default NULL,
  Site char(80) default NULL,
  Situacao char(1) default NULL,
  Data_Cadastro date default NULL,
  Nome_Fantasia varchar(30) default NULL,
  Controle_Edicao char(1) default NULL,
  PRIMARY KEY (Codigo_Cliente)
);
```

Fonte: Elaborado com base em Alves, 2014, p. 36.

Tarefas DBA – o usuário administrador

- **O DBA é responsável por autorizar o acesso ao banco de dados, coordenar e monitorar seu uso e adquirir recursos de *software* e *hardware* conforme a necessidade**
- **Questões de utilização do sistema: segurança e tempo de resposta, dependendo do tamanho do banco de dados e da organização. O DBA é auxiliado por uma equipe**

- **Projeto dos esquemas conceitual e físico: interagir com os usuários do sistema para compreender quais dados devem ser armazenados no SGBD e como eles serão mais provavelmente utilizados**
- **Segurança e autorização: assegurar que o acesso não autorizado aos dados não seja permitido**

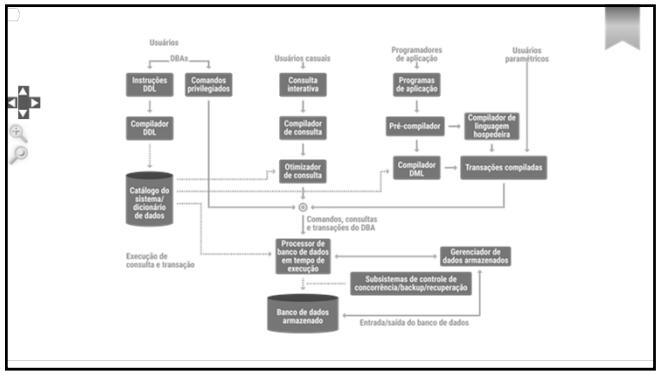
- **Disponibilidade de dados e recuperação de falhas: deve tomar medidas para assegurar que, caso o sistema falhe, os usuários possam continuar a acessar o máximo possível dos dados não corrompidos**
- **Sintonização do BD: as necessidades dos usuários evoluem, o DBA é responsável por modificar o banco de dados para assegurar desempenho adequado conforme os requisitos sofrem alterações**

Quadro 1 – Ações do DBA

Criação de conta	Essa ação cria conta e senha para um usuário ou grupo de usuários para permitir acesso ao SGBD
Concessão de privilégio	Essa ação permite que o DBA conceda certos privilégios a determinadas contas
Revogação de privilégio	Essa ação permite que o DBA revogue (cancele) alguns privilégios que foram dados anteriormente a certas contas
Atribuição de nível de segurança	Essa ação consiste em atribuir contas do usuário ao nível de liberação de segurança apropriado

Fonte: Elaborado com base em Elsmari; Navathe, 2011, p. 565.

- **Figura 5 – Módulos componentes de um SGBD e suas interações**



Tarefas DBA – criação de usuários e definições de papéis

- O DBA tem conta de usuário especial, o usuário efetua o *login* para acessar
- O SGBD, então, grava em um arquivo, denominado *log* do sistema, qualquer operação efetuada pelo usuário, como consulta, edição de dados ou inclusão de registros
- Esse recurso facilita a auditoria do sistema, no caso de haver alguma suspeita de adulteração das informações de forma indevida

Criação de usuários

- Todo usuário é criado baseado no princípio do privilégio mínimo, o que implica acesso restrito
- Uma conta de usuário tem uma série de atributos que pode ser definida no momento de sua criação ou alterada posteriormente

Criação de usuários

- Comando CREATE USER pelo administrador de banco de dados

Figura 6 – Criação de um novo usuário

```
CREATE USER 'USERWPA',
```

Fonte: Elaborado com base em Alves, 2014, p. 144.

- O banco de dados utiliza o conceito de conjunto de privilégios mínimos ao criar um usuário
- Parte do princípio de que o usuário é criado, mas não tem privilégio para executar nenhuma tarefa até receber os privilégios necessários para isso
- O banco de dados relacionais permite o gerenciamento de privilégios dos usuários em dois níveis

Quadro 2 – Privilégios das contas de usuários	
Nível de conta de usuário	Nível de relação/tabela
Cada conta ou usuário individual possui um tipo de privilégio específico, independentemente das relações/tabelas existentes no banco de dados	É possível definir para cada tabela do banco de dados um privilégio específico para acesso e manipulação dos dados

Fonte: Elaborado com base em Alves, 2014, p. 144.

Privilégios

- Para atribuir privilégios de inclusão: comando GRANT
- Para atribuir privilégio ao usuário criado: comando USERWPA

Figura 7 – Atribuição de privilégios

```
GRANT INSERT, DELETE ON
CLIENTES TO USERWPA;
```

Fonte: Alves, 2014, p. 144.

Privilégios

- Para remover/revogar os privilégios atribuídos: comando REVOKE
- Para remover privilégio atribuído ao usuário: comando USERWPA

Figura 8 – Revogar privilégios

```
REVOKE DELETE ON
CLIENTES FROM USERWPA;
```

Fonte: Alves, 2014, p. 145.

- Em sistemas padrão SQL, a segurança é baseada no conceito de direitos ou privilégios: os usuários têm ou não permissão para executar determinadas operações. Atualmente, os privilégios são assim definidos:

Quadro 2 – Privilégios das contas de usuários	
SELECT	Consulta/extração de dados
INSERT	Inclusão de novos registros
UPDATE	Atualização dos valores de campos
DELETE	Exclusão de registros

Fonte: Elaborado com base em Alves, 2014, p. 144.

Aspectos de administração dos SGDBs

- A segurança diz respeito a muitos aspectos da proteção de um sistema contra o uso não autorizado, incluindo autenticação de usuários, criptografia de informação, controle de acesso, políticas de *firewall* e detecção de intrusão
- A segurança de um sistema de banco de dados está relacionada diretamente à sua integridade e proteção das informações armazenadas nele

Quadro 4 – Questões de segurança	
Questões legais e éticas	Com relação ao direito de acessar certas informações, por exemplo: algumas informações podem ser consideradas particulares e não serem acessadas legalmente por organizações ou pessoas não autorizadas. Existem leis que controlam a privacidade da informação
Questões políticas em nível governamental institucional ou corporativo	Quanto aos tipos de informações que não devem ser públicas, por exemplo: as classificações de crédito e registros médicos pessoais
Questões relacionadas ao sistema	Como os níveis de sistema em que várias funções de segurança devem ser impostas. Por exemplo: se uma função de segurança deve ser tratada no nível de hardware físico, no nível do sistema operacional ou no nível do SGBD
Níveis de segurança e categorização dos dados	A necessidade de algumas organizações de identificar vários níveis de segurança e categorizar os dados e usuários com base nessas classificações. Por exemplo: altamente secreta, secreta, confidencial e não classificada

Fonte: Elaborado com base em Elmasrie; Navathe, 2011, p. 563.

Quadro 5 – Perda dos objetivos de segurança	
Perda da integridade	A integridade do banco de dados refere-se ao requisito de que a informação seja protegida contra modificação imprópria. A modificação de dados inclui criação, inserção, atualização, mudança do status dos dados e exclusão. A integridade é perdida se mudanças não autorizadas forem feitas nos dados por atos intencionais ou acidentais. Se a perda da integridade do sistema ou dos dados não for corrigida, o uso continuado do sistema contaminado ou de dados adulterados poderia resultar em decisões imprecisas, fraudulentas ou errôneas
Perda da disponibilidade	Quanto aos tipos de informações que não devem ser públicas, por exemplo: as classificações de crédito e registros médicos pessoais
Perda da confidencialidade	A confidencialidade do banco de dados refere-se à proteção dos dados contra exposição não autorizada. O impacto da exposição não autorizada de informações confidenciais pode variar desde a violação do Data Privacy Act até o comprometimento da segurança nacional. A exposição não autorizada, não antecipada ou não intencional poderia resultar em perda de confiança pública, constrangimento ou ação legal contra a organização

Fonte: Elaborado com base em Elmasrie; Navathe, 2011, p. 563.

- Um problema de segurança comum aos sistemas de computação é impedir que pessoas não autorizadas acessem o sistema, seja para obter informações, seja para fazer mudanças maliciosas em uma parte do BD
- Elmasri e Navathe (2011) destacam quatro medidas: controle de acesso, controle de inferência, controle de fluxo e criptografia de dados. O responsável por esses controles é o DBA

Aspectos de administração dos SGDBs

- Sensibilidade dos dados: a medida da importância atribuída aos dados por seu proprietário, com a finalidade de indicar sua necessidade de proteção
- Alguns BD contêm apenas dados confidenciais, enquanto outros podem não conter qualquer dado confidencial
- O tratamento do BD está relacionado ao controle de acesso

Quadro 6 – Fatores que classificam dados como confidenciais	
Inerentemente confidenciais	O valor dos próprios dados pode ser tão revelador ou confidencial que ele se torna sensível, por exemplo: o salário de uma pessoa ou o fato de um paciente ter HIV/ Aids
De uma fonte confidencial	A fonte dos dados pode indicar uma necessidade, por exemplo: um informante cuja identidade precisa ser mantida em segredo
Confidenciais declarados	O proprietário dos dados por tê-los declarados explicitamente como confidenciais
Um atributo ou registro confidencial	O atributo ou registro em particular pode ter sido declarado confidencial, por exemplo: o atributo de salário de um funcionário ou o registro do histórico de salários em um banco de dados pessoal
Confidencial em relação a dados previamente expostos	Alguns dados podem não ser confidenciais por si sós, mas assim se tornarão na presença de algum outro dado. Por exemplo: a informação exata de latitude e longitude para um local onde aconteceu algum evento previamente registrado, que mais tarde foi considerado confidencial

Fonte: Elaborado com base em Elmasri; Navathe, 2011, p. 566.

Quadro 7 – Ações de recuperação do BD	
Confinamento	Tomar ação imediata para eliminar o acesso do atacante ao sistema; isolar ou conter o problema para impedir que se espalhe mais
Avaliação de danos	Determina a extensão do problema incluindo funções que falharam e dados adulterados
Reconfiguração	Reconfigurar para permitir que a operação continue em um modo reduzido enquanto a recuperação prossegue
Reparo	Recuperar dados adulterados ou perdidos e reparar ou reinstalar funções do sistema que falharam para restabelecer o nível de operação normal
Tratamento de falha	Ao máximo possível, identificar os pontos fracos explorados no ataque; tomar medidas para impedir uma nova ocorrência

Fonte: Elaborado com base em Elmasri, 2011, p. 583.

Referências

- ALVES, W. P. Fundamentos de banco de dados. São Paulo: Érica, 2014.
- RAMAKRISHNAN, R.; GEHRKE, J. Sistemas de gerenciamento de bancos de dados. 3. ed. Porto Alegre: McGraw Hill, 2008.