SISTEMA GERENCIADOR DE BANCO DE DADOS

AULA 2

Profª Vívian Ariane Barausse de Moura

CONVERSA INICIAL

O objetivo desta aula é introduzir os principais conceitos e temas sobre as noções básicas de administração de banco de dados. Abordaremos assuntos pertinentes às tarefas administrativas de um Database Administrator (DBA), como criação de usuários e definições de papéis, e como são concedidas as permissões de autenticação e as permissões de autorização. Também abordaremos os aspectos da administração dos sistemas gerenciadores de banco de dados, que englobam questões de segurança, ameaça, confidencialidade, disponibilidade, integridade, auditoria e as recuperações de dados.

TEMA 1 – VISÃO GERAL DE UM BANCO DE DADOS

De acordo com Ramakrishnan e Gehrke (2008, p. 541), o desempenho de um SGBD (Sistema de Gestão de Base de Dados) em consultas feitas comumente e 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 identificando gargalos e ajustando alguns parâmetros do SGBD, como por exemplo o tamanho do pool de buffers ou a frequência dos pontos de verificação, ou adicionando hardware para eliminar tais gargalos. Entretanto, os autores ressaltam que o primeiro passo para se obter um bom desempenho é fazer boas escolhas para o projeto do banco de dados.

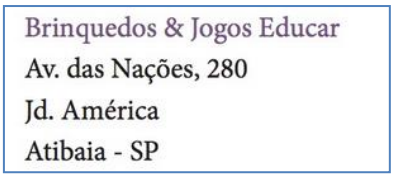
Assim como todos os outros aspectos do projeto de banco de dados, conforme defendem Ramakrishnan e Gehrke (2008, pág. 542), o projeto físico deve ser guiado pela natureza dos dados e seu uso pretendido. Em particular, é importante entender a carga de trabalho típica que o banco de dados deve suportar; a carga de trabalho consiste em uma mistura de consultas e atualizações. Para criar um bom projeto físico de banco de dados e sintonizar o desempenho do sistema, em resposta à evolução dos requisitos do usuário, um projetista deve entender o funcionamento de um SGBD, especialmente as técnicas de indexação e de processamento de consultas suportadas. Se o banco de dados será acessado concorrentemente por muitos usuários, ou seja, se for um banco de dados distribuído, a tarefa se torna mais complicada e outros recursos de um SGBD são utilizados.

Os bancos de dados possuem seu próprio vocabulário de termos técnicos. Alves (2014, p. 33) apresenta as seguintes 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. Isso significa que os dados armazenados são separados em pequenos fragmentos. Cada campo somente pode conter um tipo de dado (Alves, 2014, p. 34).

Acompanhe o exemplo apresentado na figura.

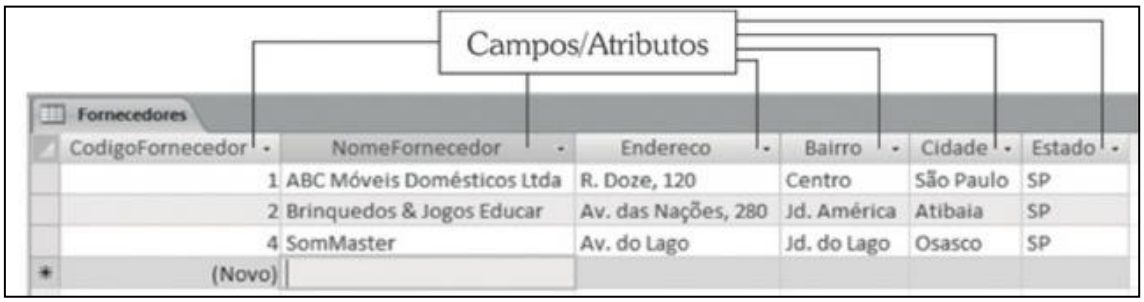
Figura 1 – Exemplo de dados



Fonte: Alves, 2014, p. 34.

O exemplo apresentado na imagem não faz sentido, pois Alves (2014, p. 34) defende que, “para ser armazenado num banco de dados é preciso separá-lo em diversas partes, assume-se que cada linha é uma fração da informação como um todo. Imagine-a distribuída numa folha quadriculada em que cada item/linha ocupa uma coluna, como nas planilhas eletrônicas”. Seguindo essa visualização, a representação teria o formato da Figura 2.

Figura 2 – Campos/atributos de uma tabela de banco de dados



CodigoFornecedor	NomeFornecedor	Endereco	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
4	SomMaster	Av. do Lago	Jd. do Lago	Osasco	SP
(Novo)					

Fonte: Alves, 2014, p. 34.

Durante e estruturação do banco de dados, uma das principais tarefas do projetista do sistema é definir quais campos irão compor as tabelas. Cada campo recebe um nome de identificação, a especificação do tipo de dado que será capaz de armazenar e o tamanho para armazenamento, entre outras informações (Alves, 2014).

Alves (2014, p. 34) define os tipos de dados básicos que podem ser atribuídos aos campos:

> caractere, numérico (com ou sem casas decimais), data, hora e lógico (valores do tipo verdadeiro ou falso). Nem todos os sistemas de banco de dados suportam o tipo de dado lógico e alguns possuem um tipo especial denominado autoincremento. Há sistemas de banco de dados, como é o caso de alguns servidores SQL, que permitem a criação de campos calculados. Esse tipo de campo é formado por uma expressão matemática, que envolve outros campos da própria tabela ou mesmo constantes numéricas. Seu valor é o resultado obtido por meio dessa expressão.

O autor exemplifica a partir da Figura 3: “suponha que haja uma tabela de pedidos de clientes e nela constem campos para entrada da quantidade do produto e o preço unitário. O preço total do item poderia simplesmente ser obtido multiplicando o valor do campo de quantidade pelo valor do campo de preço unitário”. Alves (2014, p. 34). Em termos simples, a especificação do campo seria parecida com a seguinte instrução fictícia.

Figura 3 – Exemplo da utilização de expressão matemática

```
DEFINIR "VALORTOTAL" COMO CÁLCULO ("QUANTIDADE" * "PRECOUNITARIO")
```

Fonte: Alves, 2014, p. 34.

Em alguns sistemas, também é possível, segundo Alves (2014, p. 35)

> definir um valor padrão para o campo, o que significa que se o usuário não fornecer um valor, será assumido o padrão. Os sistemas mais recentes incluem um novo tipo de dado chamado BLOB (*Binary Large Objects* - Objetos Binários Grandes) e permitem o armazenamento de dados não estruturados, como imagens, sons, vídeos etc. Diversos sistemas permitem que campos do tipo caractere sejam definidos com tamanho fixo ou variável. A definição de nome e atributos (tipos de dados e tamanhos) dos campos constitui o formato do registro.

Um registro (ou linhas) é definido por Alves (2014, p. 35) como

> o conjunto de campos valorizados (ou seja, que possuem valores) de uma tabela. É a unidade básica para o armazenamento e recuperação de dados e que identifica a entrada de um único item de informação em particular numa tabela do banco de dados”. São também chamados de “**tuplas** ou **n-uplas**. Numa tabela cujos registros são formados por cinco campos, cada registro é denominado de **5-upla** (ou quíntupla).

Os registros de uma tabela de dados

> são do mesmo tipo, ou seja, permitem o armazenamento dos mesmos tipos de dados, seus campos podem ser de tipos e tamanhos diferentes. Quando o registro possui campos do tipo caractere de tamanho variável, o tamanho do próprio registro pode também variar conforme os dados que se encontram armazenados nele, é durante a

> estruturação das tabelas do banco de dados que se define o formato (ou layout) dos registros. Por exemplo, numa tabela de cadastro de produtos, os registros são utilizados para guardar os dados referentes a produtos, não sendo possível armazenar qualquer outro tipo de dado (como de clientes ou de funcionários) (Alves, 2014, p. 35).

A partir da Figura 4, "é possível visualizar que cada linha da tabela representa um registro, neste sentido a tabela como um todo se resume a um agrupamento de linhas (registros) que são divididas em colunas (campos)" (Alves, 2014, p. 35).

Figura 4 – Registros de uma tabela de banco de dados

Fonte: Alves, 2014, p. 35.

A tabela de dados é definida por Alves (2014, p. 41) como "um conjunto ordenado de registros/linhas. Cada registro possui o mesmo número de colunas (campos)". O autor exemplifica:

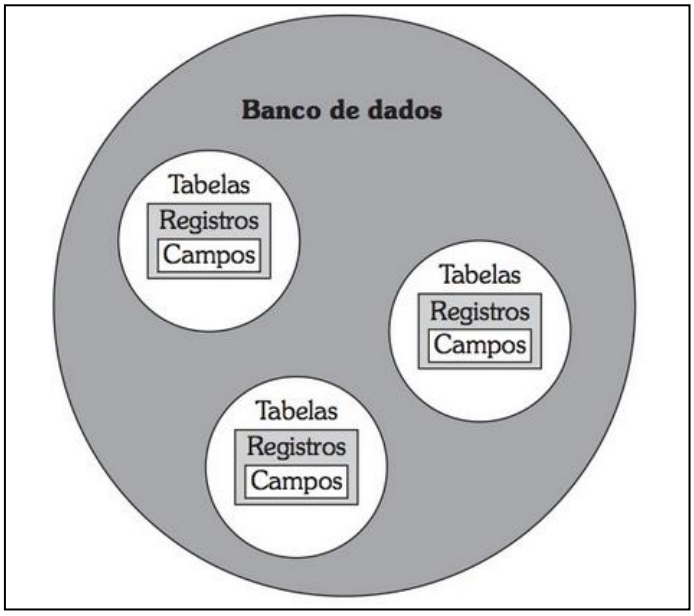
> um banco de dados pode ser formado por uma ou mais tabelas, e cada uma deve ser definida de tal forma que somente possa conter um tipo de informação. Por exemplo, uma tabela para armazenar dados dos clientes, uma para os fornecedores, uma para os produtos etc. Falando em termos de modelagem de dados, elas representam as entidades do modelo conceitual (Alves, 2014, p. 41).

Ainda segundo Alves (2014, p. 41),

> cada tabela deve ser identificada por um nome único dentro do banco de dados. São as tabelas que possuem toda a estrutura/composição dos registros, como nomes, tipos de dados e tamanhos. Uma aplicação de banco de dados somente pode acessar um determinado registro se referenciar a tabela na qual ele está definido. Na linguagem SQL também é necessário especificar o nome da tabela a ser utilizada num comando de consulta ou atualização de dados.

O autor apresenta um gráfico da hierarquia de tabelas, registros e campos (Figura 5).

Figura 5 – Gráfico da hierarquia de tabelas, registros e campos



Fonte: Alves, 2014, p. 36.

Alves (2014) apresenta um exemplo de comando em linguagem SQL para a definição de uma tabela de dados (Figura 6).

Figura 6 – Exemplo definição 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 varchar(80) default NULL,
  Site varchar(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: Alves, 2014, p. 36.

O autor defende que “as aplicações normalmente utilizam várias tabelas do banco de dados para consolidar e retornar informações nas quais o usuário tem interesse. Exemplo: na geração de um relatório de vendas no mês ou o boletim escolar dos alunos” (Alves, 2014, p. 41).

TEMA 2 – DBA: USUÁRIO ADMINISTRADOR

A atuação de um administrador de banco de dados relaciona-se ao trabalho de administrar, que implica supervisão e gerenciamento dos recursos de qualquer organização em que existam pessoas que utilizem tais recursos. Os autores defendem que, em um BD, o recurso principal é o próprio banco de dados; o recurso secundário é o SGBD e softwares relacionados. A administração desses recursos é responsabilidade do administrador de banco de dados (DBA – Database Administrator). De acordo com Elsmari e Navathe (2011, pág. 11), “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”. Além disso, questões quanto à utilização do sistema, como segurança e tempo de resposta, também são essenciais. A depender do tamanho do banco de dados e da organização, o DBA é auxiliado por uma equipe.

Ramakrishnan e Gehrke (2008) realizam um comparativo entre um banco de dados pessoal e um banco de dados organizacional, visto que o banco de dados pessoal é mantido tipicamente pelo indivíduo que o possui e o utiliza, enquanto os bancos de dados corporativos normalmente são importantes e complexos o suficiente para que a tarefa de projetar e manter o banco de dados seja confiada a um profissional, o DBA. Ele é responsável por realizar várias tarefas, conforme vemos no Quadro 1.

Quadro 1 – Tarefas realizadas pelo DBA

Projeto dos esquemas conceitual e físico	O DBA é responsável por interagir com os usuários do sistema para compreender quais dados devem ser armazenados no SGBD e como eles serão mais provavelmente utilizados. Baseado nesse conhecimento, o DBA deve projetar o esquema conceitual (decidir quais relações armazenar) e o esquema físico (decidir como armazená-las). O DBA também pode projetar partes extensamente utilizadas do esquema externo, embora os usuários provavelmente estendam esse esquema criando visões adicionais.

(continua)

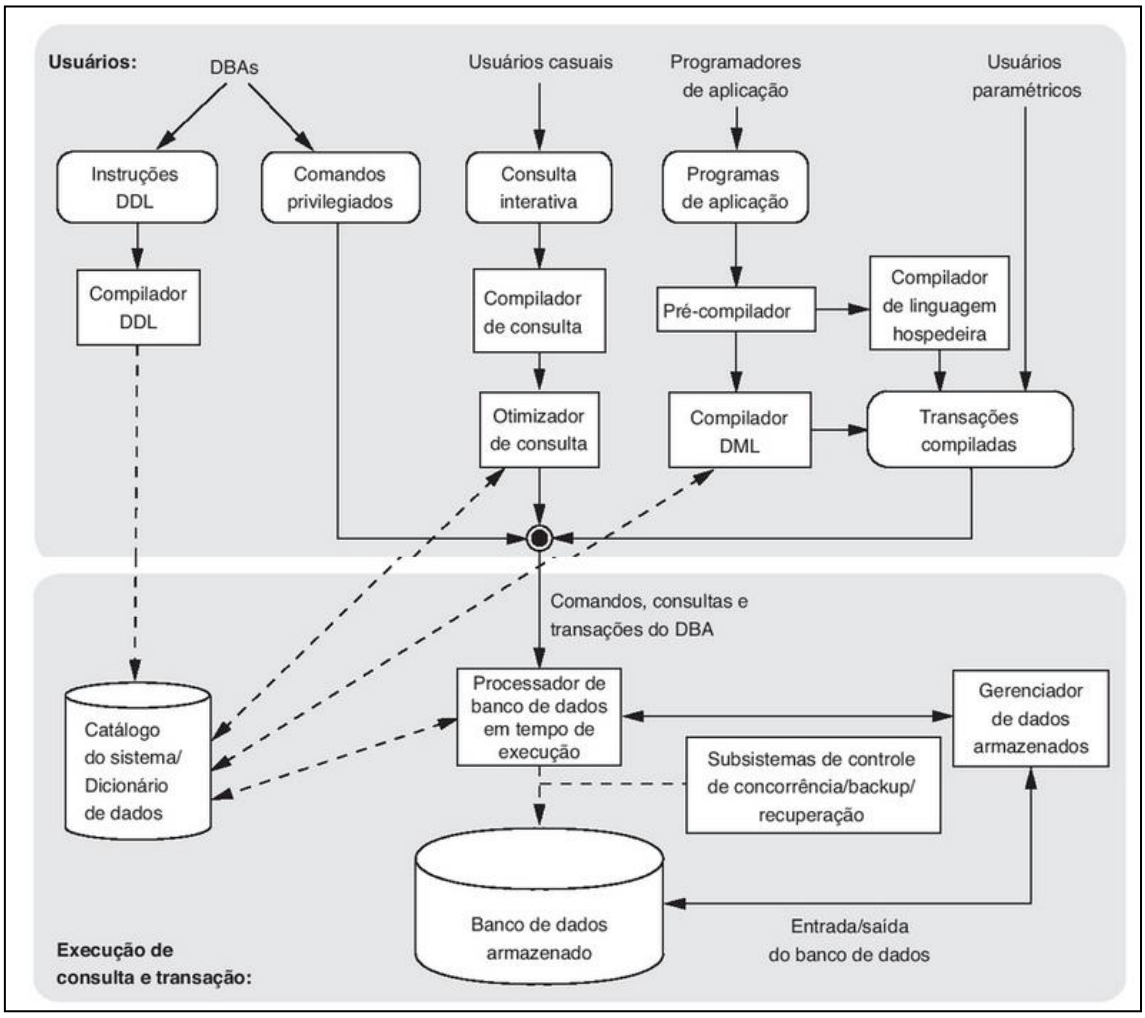
(continuação do Quadro 1)

Segurança e autorização	O DBA é responsável por assegurar que o acesso não autorizado aos dados não seja permitido. Em geral, nem todos devem ser capazes de acessar todos os dados. Em um SGBD relacional, os usuários podem ganhar permissão de acesso apenas a determinadas visões e relações. Por exemplo, embora se possa permitir que os alunos localizem as matrículas do curso e quem ministra determinado curso, não é desejável que os alunos vejam os salários dos professores ou as informações de notas dos demais alunos. O DBA pode forçar essa política concedendo permissão de apenas leitura para a visão InfoCurso (informações sobre o curso).
Disponibilidade de dados e recuperação de falhas	O DBA deve tomar medidas para assegurar que, caso o sistema falhe, os usuários possam continuar a acessar o máximo possível dos dados não corrompidos. O DBA também deve restaurar os dados a um estado consistente. O SGBD fornece suporte de software para essas funções, mas o DBA é responsável por implementar os procedimentos para realizar o backup dos dados periodicamente e manter os logs da atividade do sistema (para facilitar a recuperação de uma falha).
Sintonização de banco de dados	É bem provável que as necessidades dos usuários evoluam ao longo do tempo. O DBA é responsável por modificar o banco de dados, em particular os esquemas conceituais e físicos, para assegurar desempenho adequado conforme os requisitos sofrem alterações.

Fonte: Elaborado com base em Ramakrishnan; Gehrke, 2008, p. 18.

A maioria dos sistemas de banco de dados contém comandos privilegiados que podem ser usados apenas pelos DBAs. Estes incluem comandos para criar contas, definir parâmetros do sistema, conceder autorização de conta, alterar um esquema e reorganizar as estruturas de armazenamento de um banco de dados (Elsmari; Navathe, 2011). A Figura 7 representa de forma simplificada os componentes do SGBD.

Figura 7 – Módulos componentes de um SGBD e suas interações



Fonte: Elsmari; Navathe, 2011, p. 27

A parte superior refere-se aos vários usuários do ambiente de dados e suas interfaces relacionadas. Ela apresenta as interfaces para DBA, usuários casuais que trabalham com interfaces interativas para formular consultas, programadores de aplicação que criam programas usando algumas linguagens de programação hospedeira, e usuários paramétricos que realizam a entrada dos dados fornecendo parâmetros para transações predefinidas. Os DBA definem o banco de dados e realizam ajustes, alterando sua definição por meio da DDL e outros comandos privilegiados. A parte inferior mostra os detalhes internos do SGBD, responsáveis por armazenamento de dados e processamento de transações. (Elsmari; Navathe, 2011).

Nesse sentido, de acordo com Elsmari e Navathe (2011), o DBA é autoridade central para gerenciar um sistema de banco de dados. Suas responsabilidades incluem a concessão de privilégios aos usuários que precisam

usar o sistema e a classificação dos usuários de acordo com a política da organização.

Para realizar essas atividades, Elsmari e Navathe (2011) indicam que, no SGBD, o DBA tem uma conta de DBA, também conhecida como *conta do sistema*, ou *conta de superusuário*, que oferece capacidades poderosas que não estão disponíveis às contas e usuários comuns do banco de dados. Os comandos privilegiados do DBA incluem concessão e revogação de privilégios a contas, usuários ou grupos de usuários individuais, conforme vemos no quadro abaixo.

Quadro 2 – Ações do DBA

Criação de conta	Essa ação cria uma 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

TEMA 3 – DBA: CRIAÇÃO DE USUÁRIOS E DEFINIÇÕES DE PAPÉIS, PERMISSÃO DE AUTENTICAÇÃO E AUTORIZAÇÃO

A expansão e as alterações quanto às regras de negócios levaram A atualizações no sistema de um modo geral. Alves (2014) defende que, atualmente, todos os SGBDs relacionais apresentam um subsistema de controle de acesso que é responsável pelo gerenciamento de usuários, pela definição de níveis de acesso e pela seleção das operações que podem ser executadas por cada um deles.

Outra função muito importante é a criptografia dos dados armazenados no banco (Alves, 2014), cujo objetivo é protegê-los, por serem sigilosos – como, por exemplo, números de cartões de crédito. O autor defende que cabe ao DBA a responsabilidade por definir privilégios aos usuários de acordo com as políticas de segurança da organização.

O DBA realiza essa atividade com a sua conta de usuário especial, a partir da identificação de usuário e senha de acesso, por meio dos quais o usuário efetua o *log-in* no sistema toda vez que precisar utilizar a aplicação que acessa

o banco de dados. 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. (Alves, 2014).

Os bancos de dados relacionais permitem o gerenciamento de privilégios dos usuários em dois níveis, de acordo com o quadro abaixo.

Quadro 3 – 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.

Elsmari e Navathe (2011) afirmam que, quando vários usuários compartilham um grande banco de dados, é provável que a maioria deles não esteja autorizada a acessar todas as informações nele contidas – por exemplo, dados que são considerados confidenciais, como dados financeiros que somente pessoas com autorização têm a permissão de acessar. Além disso, alguns usuários só podem ter permissão para recuperar dados, enquanto outros podem recuperar e atualizar, o que implica que operações de acesso, recuperação ou atualização também devam ser controladas.

De um modo geral, os usuários e grupos de usuários recebem números de conta protegidas por senhas, que podem usar para acessar o banco de dados. Um SGBD deve oferecer um subsistema de segurança e autorização, que o DBA utiliza para criar contas e especificar restrições (Eslmari; Navathe, 2011).

Para que seja possível conceder privilégios a um usuário, é preciso que ele esteja previamente criado. Isso pode ser feito com o comando *create user*.

Figura 8 – Criação de um novo usuário

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

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

A partir da sua criação, o novo usuário não tem permissão para fazer nada na sua base de dados, sendo necessário inserir privilégios. Na linguagem SQL, existem dois comandos para o gerenciamento de privilégios de usuários: *grant* para garantir um determinado privilégio e *revoke* para revogar (remover) um privilégio anteriormente estabelecido (Alves, 2014).

Vamos imaginar um banco de dados com uma tabela de cadastro de clientes denominada *clientes*. Para atribuir privilégios de inclusão e exclusão ao usuário criado e identificado como USERWPA, o comando SQL seria o seguinte.

Figura 9 – Atribuição de privilégios

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

Fonte: Alves, 2014, p. 144.

Se houvesse a necessidade de revogar o privilégio de exclusão, o comando seria como o da figura abaixo.

Figura 10 – Revogar privilégios

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

Fonte: Alves, 2014, p. 145.

Existem diversas ferramentas gráficas que permitem a manipulação dos bancos de dados SQL de uma maneira fácil e intuitiva. Entre as operações possíveis, estão o gerenciamento de contas, usuários e privilégios. Alves (2014) define que em sistemas padrão SQL a segurança é baseada no conceito de direitos ou privilégios, por meio dos quais os usuários têm ou não permissão para executar determinadas operações. Atualmente, o padrão ANSI/ISO define quatro privilégios, conforme o Quadro 4.

Quadro 4 – Privilégios padrão ANSI/ISO

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.

Se um usuário com privilégio somente de consulta SELECT tentar incluir um registro utilizando o comando INSERT INTO, sem especificar, Alves (2014) indica que o servidor SQL vai informar uma mensagem de erro.

Quadro 5 – Comandos de definição de dados (DDL)

Comando	Função
CREATE DATABASE	Criar uma base de dados totalmente vazia.
ALTER DATABASE	Permitir alterações em algumas caraterísticas da base de dados.
DROP DATABASE	Apagar um banco de dados existente (deve ser utilizado com muito cuidado).
CREATE TABLE	Criar uma tabela de dados (também há necessidade de cuidado na utilização).
ALTER TABLE	Permitir alterações na estrutura de uma tabela existente.
DROP TABLE	Apagar uma tabela de dados existente.
CREATE INDEX	Criar índices secundários para uma tabela.
DROP INDEX	Apagar um índice existente.
CREATE DOMAIN	Criar um domínio para campos das tabelas.
DROP DOMAIN	Apagar um domínio existente.
CREATE VIEW	Criar uma visão com base em uma ou mais tabelas.
DROP VIEW	Apagar uma visão existente.

Fonte: Alves, 2014, p. 124.

TEMA 4 – ASPECTOS DE ADMINISTRAÇÃO DOS SGBDs

A segurança na TI, de acordo com Elmasri e Navathe (2011, p. 566), "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". O propósito desse estudo é o tratamento da segurança quanto a conceitos associados à forma que um sistema de banco de dados pode proteger o acesso de suas informações.

De acordo com Alves (2014, pág. 143) “a segurança de um sistema de banco de dados está relacionada diretamente com sua integridade e proteção das informações armazenadas nele”. Ao trabalhar com segurança, é importante levar em consideração algumas questões – as principais estão discriminadas no Quadro 6.

Quadro 6 – Questões de Segurança

Questões legais e éticas	Com relação ao direito de acessar certas informações, como 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, como 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. Como 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, em 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. A política de segurança da organização com relação a permitir o acesso a várias classificações dos dados deve ser imposta.

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

Alves (2014, p. 144) destaca que, em aplicações do tipo *monousuário*, como um aplicativo doméstico para controle de contas a pagar e a receber, a segurança não precisa necessariamente ser um item que mereça tanta atenção – o que não ocorre quando se trata de sistemas multiusuários, pois é imprescindível a existência de técnicas que controlem o acesso por parte de grupos de usuários, fornecendo acesso apenas a partes específicas do banco de dados.

Elmasri e Navathe (2011) definem que as ameaças ao banco de dados podem resultar na perda ou degradação de alguns ou de todos os objetivos de segurança comumente aceitos: integridade, disponibilidade e confidencialidade. As perdas desses objetivos resultam em vários problemas, apresentados no Quadro 7.

Quadro 7 – 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, uso continuado do sistema contaminado ou de dados adulterados poderia resultar em decisões imprecisas, fraudulentas ou errôneas.
Perda da disponibilidade	A disponibilidade do banco de dados refere-se a tornar os objetos disponíveis a um usuário humano ou a um programa ao qual eles têm um direito legítimo.
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 Elmasri; 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 ou para fazer mudanças maliciosas em uma parte do banco de dados. Neste sentido, Elmasri e Navathe (2011, p. 564) destacam quatro medidas de controle principais que são usadas para fornecer segurança nos bancos de dados: controle de acesso, controle de inferência, controle de fluxo e criptografia de dados. O responsável por realizar esses controles é o DBA, a partir da conta DBA no SGBD, também conhecida como *conta do sistema* ou *conta de superusuário*, que oferece capacidades já vistas nos temas anteriores, como: criação de conta, concessão de privilégio, revogação de privilégio e atribuição de nível de segurança.

TEMA 5 – DEMAIS ASPECTOS DE ADMINISTRAÇÃO DOS SGBDs

Outra questão destacada por Elmasri e Navathe (2011, p. 565) é a sensibilidade dos dados, que segundo os autores é a medida da importância atribuída aos dados por seu proprietário, com a finalidade de indicar a necessidade de proteção. Alguns bancos de dados contêm apenas dados confidenciais, enquanto outros podem não conter qualquer dado confidencial. O tratamento de banco de dados nesses dois extremos está relacionado ao controle de acesso. Porém, a situação torna-se mais complicada quando alguns

dos dados são confidenciais, enquanto outros não o são. Diversos fatores podem fazer com que os dados sejam classificados como confidenciais conforme apresentado indica o quadro abaixo.

Quadro 8 – 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 pode 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 o confidencial.

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

Elmasri e Navathe (2011) atribuem também a responsabilidade da segurança ao administrador da segurança, pois junto com o DBA, devem estabelecer coletivamente as políticas de segurança da organização. Isso indica que o acesso a certo atributo do banco de dados deve ser permitido (também conhecido como *coluna da tabela* ou *elemento de dados*), ou não, para usuários individuais ou para categorias de usuários. Vários fatores precisam ser considerados antes de decidir se é seguro revelar os dados. Elmasri e Navathe (2011) indicam os três fatores no Quadro 9.

Quadro 9 – Fatores de segurança

Disponibilidade de dados	Se um usuário estiver atualizando um campo, então esse campo torna-se inacessível e outros usuários não devem visualizar esses dados. Esse bloqueio é temporário apenas para garantir que nenhum usuário veja quaisquer dados imprecisos.
Aceitabilidade de acesso	Os dados devem ser revelados a usuários autorizados. Um administrador de banco de dados também pode negar acesso a uma solicitação do usuário, mesmo que esta não acesse diretamente um item de dados confidencial, com base no fato de os dados solicitados poderem revelar informações sobre os dados confidenciais que usuário não está autorizado a ter.

(continua)

(continuação do Quadro 9)

Garantia de autenticidade	Antes de conceder acesso, certas características externas sobre o usuário também podem ser consideradas. Por exemplo, o usuário só pode ter acesso permitido durante as horas de trabalho. O sistema pode rastrear consultas anteriores para garantir que uma combinação de consultas não revele dados confidenciais.

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

Se houver suspeita de qualquer adulteração no banco de dados, é realizada uma auditoria. Ela consiste, de acordo com Elmasri e Navathe (2011, p. 583), em rever o log para examinar todos os acessos de operações aplicadas ao banco de dados durante certo período. Quando uma operação ilegal ou não autorizada é encontrada, o DBA pode determinar o número de conta usado para realizar a operação. As auditorias são particularmente importantes para banco de dados confidenciais, que são atualizados por muitas transações e usuários, como no caso de bancos que os atualizam por meio de seus diversos caixas. Um log de banco de dados, utilizado principalmente para fins de segurança, às vezes é chamado de *trilha de auditoria*.

Porém, mesmo que ocorram violações no BD, é necessário garantir a sobrevivência do banco de dados. Pois, segundo Elmasri e Navathe (2011, p. 583), os sistemas de banco de dados precisam operar e continuar suas funções, mesmo com capacidades reduzidas, apesar de ventos destruidores, como ataques de busca de vantagem competitiva. Um SGBD, além de realizar todos os esforços para impedir um ataque e detectar quando um caso problemático ocorreu, deve ser capaz de realizar as ações do quadro abaixo.

Quadro 10 – 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	Determinar 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 e tomar medidas para impedir uma nova ocorrência.

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

Alves (2014, p. 148) aponta outro aspecto de segurança que deve ser abordado, que está relacionado com a forma de preservação e de recuperação

de informações ou do banco de dados inteiro. Isso significa que o administrador deve fazer uso de recursos oferecidos pelo próprio servidor de banco de dados ou utilizar outro meio que possibilite ter cópias do banco de dados. A maneira mais óbvia é fazer backups (cópias de segurança) periódicos. Alguns sistemas operacionais e servidores oferecem ferramentas para essa tarefa; no entanto, no caso de não estarem disponíveis, podem ser utilizados aplicativos utilitários disponíveis no mercado, alguns até gratuitos.

É importante ressaltar que um ataque ao sistema pode ter vários objetivos, como buscar uma vantagem competitiva ou prejudicar a organização. Embora alguns ataques paralisem totalmente o sistema, eles também devem ser bem temporizados para diminuir o alcance do objetivo do atacante, com a finalidade de retornar o sistema à sua condição operacional, diagnosticando como ocorreu o ataque e tomando medidas preventivas.

As questões relacionadas à sobrevivência do banco de dados ainda não foram suficientemente investigadas. É necessário que se realizem mais pesquisa sobre técnicas e metodologias que possam garantir a sobrevivência do sistema de banco de dados.

FINALIZANDO

Nesta aula, aprendemos os conceitos pertinentes às noções básicas da administração de banco de dados, tarefa de um *database administrator*, DBA, ou administrador de bancos de dados. Suas funções vão desde a avaliação do hardware e do servidor até o monitoramento do desempenho do banco de dados. Ele é responsável por criar objetos referentes a dados, estruturas físicas e lógicas do banco de dados. Além de iniciar o serviço pertinente ao funcionamento do banco de dados, também é responsável pela execução dos backups. Também aprendemos alguns conceitos de segurança e a importância da sua adoção em sistemas de bancos de dados, como o controle de usuários e suas permissões de acesso ao sistema, além de questões pertinentes à recuperação dos dados, o que garante a continuidade do funcionamento dos sistemas.

REFERÊNCIAS

ALVES, W. P. **Banco de dados**. São José dos Campos, SP: Érica, 2014.

ELMASRI, R.; NAVATHE, S. B. **Sistema de banco de dados**. 6. ed. São Paulo: Pearson Education do Brasil, 2011.

RAMAKRISHNAN, R.; GEHRKE, J. **Sistemas de gerenciamento de bancos de dados**. 3. ed. Porto Alegre: McGraw Hill, 2008.