Sistemas de Banco de Dados Projeto, implementação e gerenciamento

Capítulo 15

Administração e segurança de banco de dados

Objetivos

- **Neste capítulo, você aprenderá:**
  - Que os dados são um bem valioso de negócios, exigindo gerenciamento cuidadoso
  - Como o banco de dados executa um papel fundamental em uma organização
  - Que a introdução de um SGBD apresenta consequências tecnológicas, gerenciais e culturais importantes

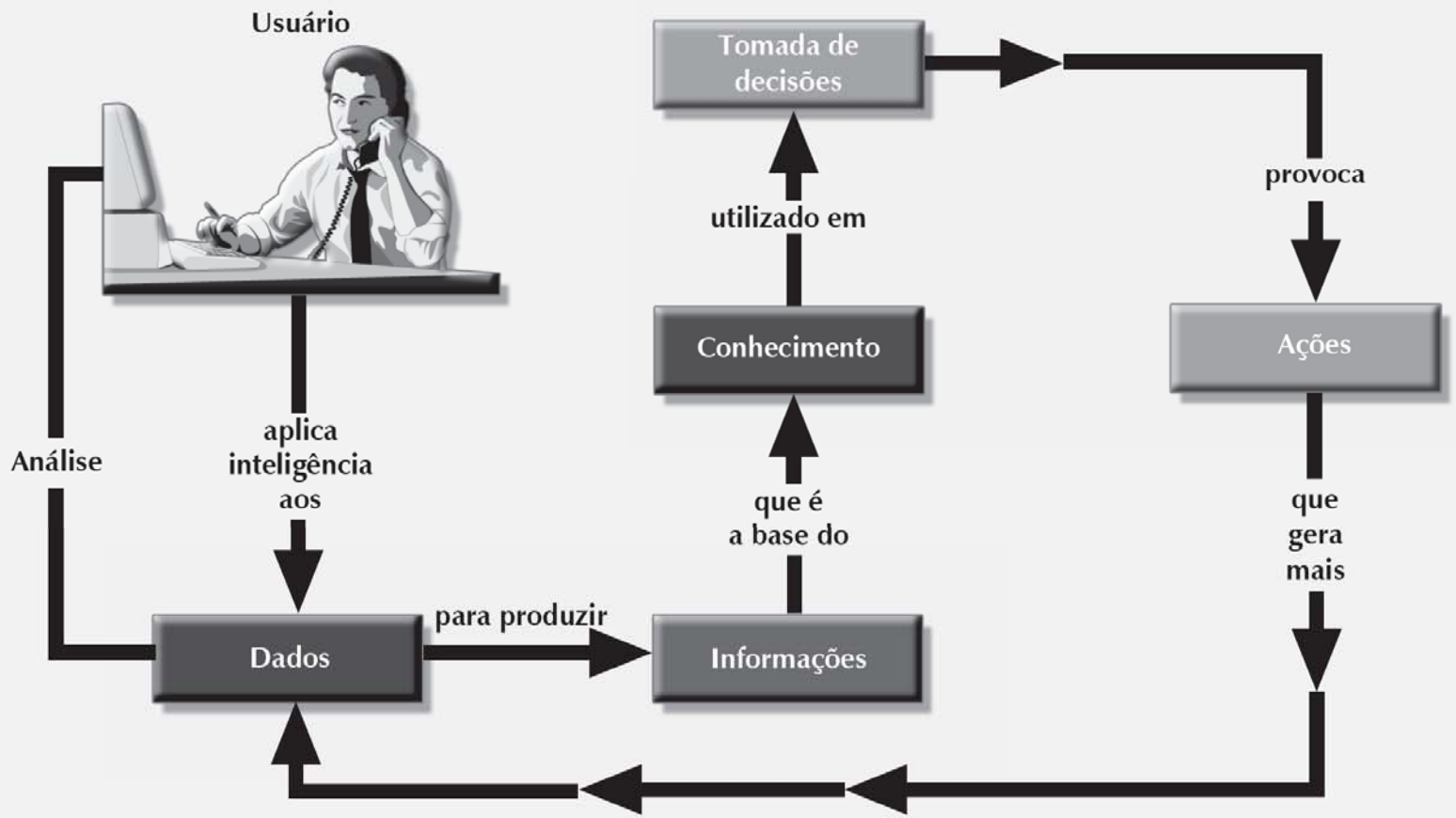
Objetivos (cont.)

- Quais são as funções gerenciais e técnicas do administrador de bancos de dados
- Sobre segurança de dados, segurança de bancos de dados e modelo de segurança de informações
- Sobre diversas ferramentas e estratégias de administração de bancos de dados
- Como diversas tarefas técnicas de administração de bancos de dados são executadas no Oracle

Dados Como um Bem Corporativo

- No ambiente atual os dados sejam um bem valioso que exija gerenciamento cuidadoso
- Os dados são um recurso valioso que pode ser traduzido em informações
- Se as informações forem precisas e oportunas, provavelmente provocarão ações que aprimorem a posição competitiva da empresa e gerem riqueza

FIGURA 15.1 Ciclo dados-informação-tomada de decisões



A Necessidade e a Função do Banco de Dados em uma Organização

- O papel predominante do banco de dados é dar suporte à tomada de decisões gerenciais em todos os níveis
- SGBDs facilitam:
  - A interpretação e a apresentação de dados
  - A distribuição de dados e informações
  - A preservação e o monitoramento dos dados
  - O controle da duplicação e da utilização de dados
- A estrutura gerencial de uma organização pode ser dividida em três níveis: alto, médio e operacional

Introdução de um Banco de Dados: considerações especiais

- A introdução de um SGBD representa um impacto profundo
  - Pode ser positivo ou negativo, dependendo de como for administrado
- Três aspectos importantes da introdução de um SGBD:
  - Tecnológico: Software e hardware do SGBD
  - Gerencial: Funções administrativas
  - Cultural: Resistência da corporação à mudança
- O departamento de administração de bancos de dados deve estar preparado para educar os usuários finais sobre os usos e benefícios do sistema

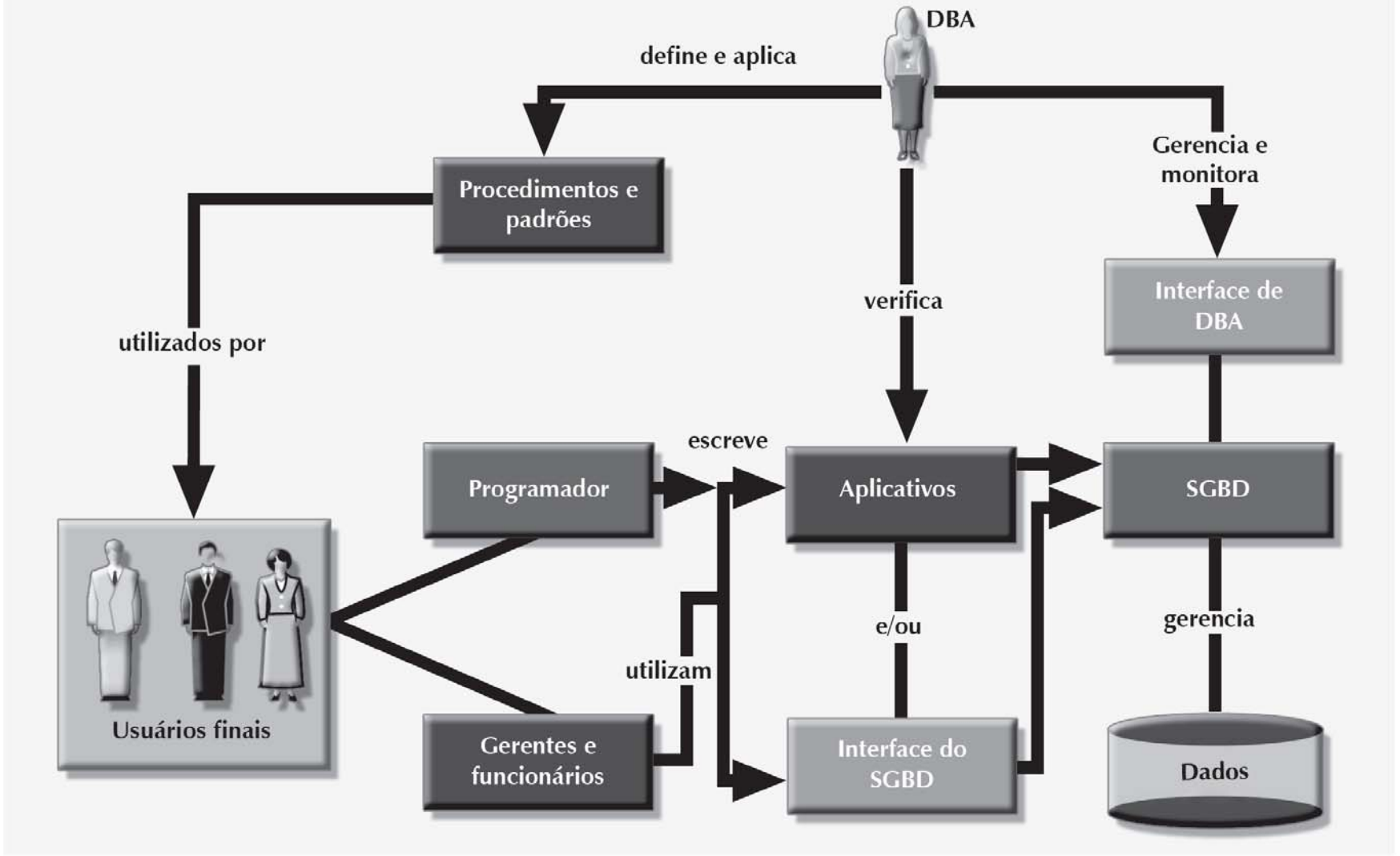
Evolução da Função de Administração de Banco de Dados

- A administração de dados tem suas raízes no antigo e descentralizado mundo dos sistemas de arquivos
- O surgimento do SGBD e de sua visão compartilhada dos dados produziu um novo nível de sofisticação
  - Evolução do departamento de PD para o **departamento de sistemas de informação** (**SI**)
- O gerenciamento de dados tornou-se um trabalho cada vez mais complexo
  - Desenvolvimento da função de administração de bancos de dados

Componente Humano do Ambiente do Banco de Dados

- Até os sistemas projetados com a mais cuidadosa destreza não podem ser operados sem o componente humano
- A administração eficiente de dados exige habilidades tanto técnicas como gerenciais
- O AD deve estabelecer metas de administração de dados
- O papel do DBA é o de mediador entre os dados e os usuários
- Necessidade de uma combinação diversificada de habilidades

FIGURA 15.6 Resumo das atividades do DBA



A Função Gerencial de DBA

- É responsável por:
  - Coordenar, monitorar e alocar os recursos de administração de bancos de dados:
    - As pessoas e os dados
  - Definir metas e formular planos estratégicos para a função de administração de bancos de dados
- Interage com o usuário final fornecendo serviços de suporte a dado
- Define **políticas**, **padrões** e **procedimentos**
- Gerencia a segurança a privacidade e a integridade de dados
- Garante o backup e a recuperação de dados
- Garante a distribuição e a utilização de dados

Função Técnica do DBA

- Avaliação, seleção e instalação do SGBD e utilitários relacionados
- Projeto e implementação de banco de dados e aplicações
- Teste e avaliação de banco de dados e aplicações
- Operação do SGBD, utilitários e aplicações
- Treinamento e suporte aos usuários
- Manutenção do SGBD, utilitários e aplicações

Segurança

- A **segurança** refere-se às atividades e medidas que garantem:
- **Confidencialidade**: dados protegidos contra acesso não autorizado
- **Integridade**: manutenção da consistência e da ausência de erros e anomalias
- **Disponibilidade**: possibilidade de acessar os dados sempre que solicitado por usuários autorizados para finalidades autorizadas

Políticas de Segurança

- As tarefas de segurança do sistema e de seu principal bem, os dados, são executadas pelo agente de segurança e pelo administrador
- **Política de segurança**: conjunto de padrões, políticas e procedimentos criados para garantir a segurança de um sistema, a auditoria e a conformidade
- O processo de auditoria de segurança começa pela identificação de vulnerabilidades da infraestrutura do sistema de informações
  - Desenvolve medidas para proteger o sistema e os dados desses pontos vulneráveis

Vulnerabilidades de Segurança

- **Vulnerabilidade de segurança**: ponto fraco em um componente do sistema
  - Pode ser explorado para permitir acesso não autorizado ou causar interrupções de serviço
- **Ameaça de segurança**: violação iminente que pode ocorrer a qualquer momento em razão de vulnerabilidades não verificadas de segurança
- **Falha de segurança**: ocorre quando uma ameaça de segurança é explorada para afetar negativamente a integridade, confidencialidade e disponibilidade do sistema
    - Preservada
    - Corrompido

TABELA 15.4 Exemplos de vulnerabilidades de segurança e medidas relacionadas

COMPONENTE DO SISTEMA	VULNERABILIDADE DE SEGURANÇA	MEDIDAS DE SEGURANÇA
Pessoas	• O usuário configura uma senha em branco. • A senha é curta ou inclui data de nascimento. • O usuário deixa a porta do escritório aberta o tempo todo. • O usuário deixa informações sobre folha de pagamento na tela por longos períodos de tempo.	• Aplicar políticas de senhas complexas. • Utilizar vários níveis de autenticação. • Utilizar telas de segurança e protetores de tela. • Instruir os usuários sobre dados sensíveis. • Instalar câmeras de segurança. • Utilizar travas automáticas nas portas.
Estações de trabalho e servidores	• O usuário copia dados para um pen drive. • A estação de trabalho é utilizada por diversos usuários. • Uma falta de energia quebra o computador. • Pessoal não autorizado pode utilizar o computador. • Dados sensíveis são armazenados em um laptop. • Dados são perdidos em consequência de roubo de disco rígido/laptop. • Desastre natural: terremoto, enchente etc.	• Utilizar políticas de grupo para restringir a utilização de pen drives. • Atribuir direitos de acesso a usuários de estações de trabalho. • Instalar fontes de energia não interrompíveis (UPS). • Adicionar dispositivos de bloqueio de segurança aos computadores. • Implementar um botão de emergência para o caso de roubos de laptop. • Criar e testar planos de backup e recuperação de dados. • Proteger o sistema contra desastres naturais; utilizar estratégias de várias localizações.

TABELA 15.4 Exemplos de vulnerabilidades de segurança e medidas relacionadas (continuação)

COMPONENTE DO SISTEMA	VULNERABILIDADE DE SEGURANÇA	MEDIDAS DE SEGURANÇA
Sistema operacional	• Ataques de sobrefluxo de buffer. • Ataques de vírus. • Ataques de root kits e worms. • Ataques de negação de serviço. • Cavalos de Troia. • Aplicações de spyware. • Identificadores (crackers) de senhas.	• Aplicar os patches e atualizações de segurança do SO. • Aplicar os patches do servidor de aplicações. • Instalar software antivírus e antispyware. • Aplicar trilhas de auditorias aos computadores. • Executar backups periódicos do sistema. • Instalar apenas aplicações autorizadas. • Utilizar políticas de grupo para evitar instalações não autorizadas.
Aplicações	• Bugs de aplicações – sobrefluxo de buffer • SQL Injection, invasão de sessão (session hijacking) etc. • Vulnerabilidades de aplicações; XSS (cross site scripting), entradas não validadas. • Ataques de e-mail: spam, phishing etc. • E-mails de engenharia social.	• Testar as aplicações exaustivamente. • Construir proteções no código. • Realizar testes exaustivos de vulnerabilidade nas aplicações. • Instalar filtro de spam/antivírus no sistema de e-mail. • Utilizar técnicas de codificação segura (veja *www.owasp.org*). • Instruir os usuários sobre ataques de engenharia social.
Rede	• IPs spoofing. • Sniffers de pacotes • Ataques de hackers. • Exclusão de senhas na rede.	• Instalar firewalls. • Redes virtuais privadas (VPN). • Sistemas de detecção de invasões (IDS). • Controle de acesso à rede (NAC). • Monitoramento de atividade da rede.
Dados	• Os compartilhamentos de dados estão abertos a todos os usuários; • Os dados podem ser acessados de modo remoto. • Os dados podem ser excluídos de recursos compartilhados.	• Implementar segurança de sistemas de arquivos. • Implementar segurança de acesso compartilhado. • Utilizar permissão de acesso. • Criptografar os dados no nível de sistema de arquivos ou banco de dados.

Segurança de Banco de Dados

- Rfere-se à utilização de recursos do SGBD e outras medidas relacionadas para atender às exigências de segurança
- O DBA deve proteger o SGBD do momento da instalação até a operação e a manutenção
- **Gerenciamento de autorizações**:
  - Gerenciamento de acesso de usuários
  - Definição de visualização
  - Controle de acesso ao SGBD
  - Monitoramento de utilização do SGBD

Ferramentas de Administração de Banco de Dados

- Existem dois tipos principais de dicionários de dados: *integrado* e *independente*
- **Dicionário de dados ativo** é atualizado automaticamente pelo SGBD em cada acesso ao banco de dados
- **Dicionário de dados passivo** não é atualizado automaticamente e costuma exigir a execução de um processo de batch
- A principal função do dicionário é armazenar a descrição de todos os objetos que interajam com o banco

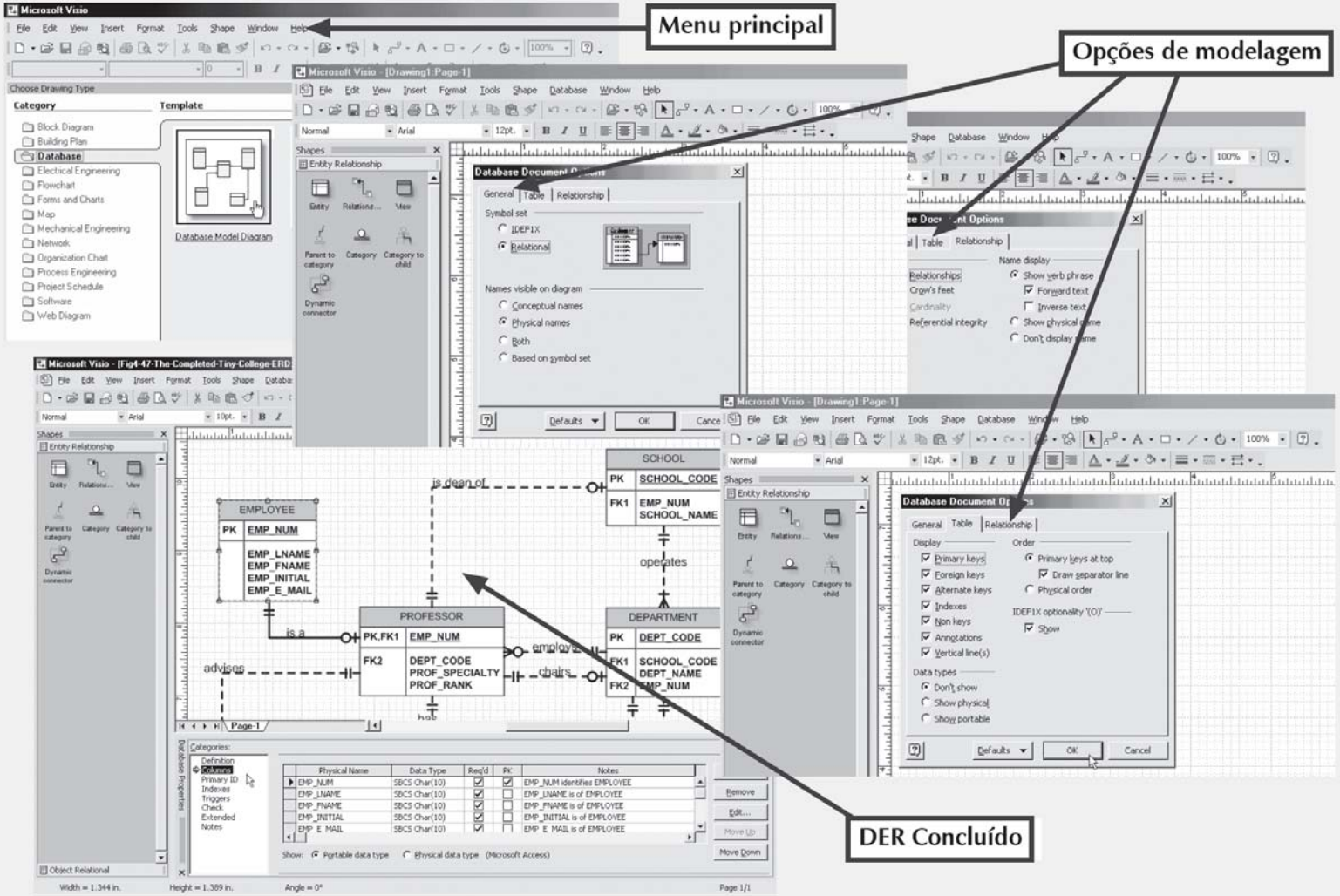
Ferramentas de Administração de Banco de Dados (cont.)

- Se o dicionário de dados incluir dados externos ao próprio SGBD, torna-se uma ferramenta particularmente flexível
  - Permite gerenciar a utilização e alocação de todas as informações da organização
- Os metadados armazenados no dicionário costumam ser a base do monitoramento da utilização do banco e da atribuição de direitos de acesso aos usuários
- O DBA pode utilizar o dicionário para dar suporte à análise e ao projeto de dados

Ferramentas CASE

- **CASE** é a sigla para *computer-aided software engineering* – **engenharia de software assistida por computador**
  - Automatizado para o CVDS (ciclo de vida de desenvolvimento de sistemas)
  - Utilizam metodologias estruturadas e poderosas interfaces gráficas
- **Ferramentas CASE front end** fornecem suporte às fases de planejamento, análise e projeto
- **Ferramentas CASE back end** dão suporte às fases de codificação e implementação
- Uma ferramenta CASE comum oferece cinco componentes

FIGURA 15.7 Exemplo de ferramenta CASE: Visio Professional



Desenvolvimento de Estratégia de Administração de Dados

- **Engenharia da informação** (**EI**) permite a tradução das metas estratégicas da empresa em dados e aplicações
- **Arquitetura de sistemas de informação (ASI)** serve como base para o planejamento, desenvolvimento e controle de futuros sistemas de informação
- A implementação de EI é um processo custoso
  - Fornece um modelo que inclui a utilização de ferramentas computadorizadas, automatizadas e integradas
- O sucesso da estratégia geral de sistemas de informação depende de vários fatores fundamentais
  - Gerenciais, tecnológicos e culturais da corporação

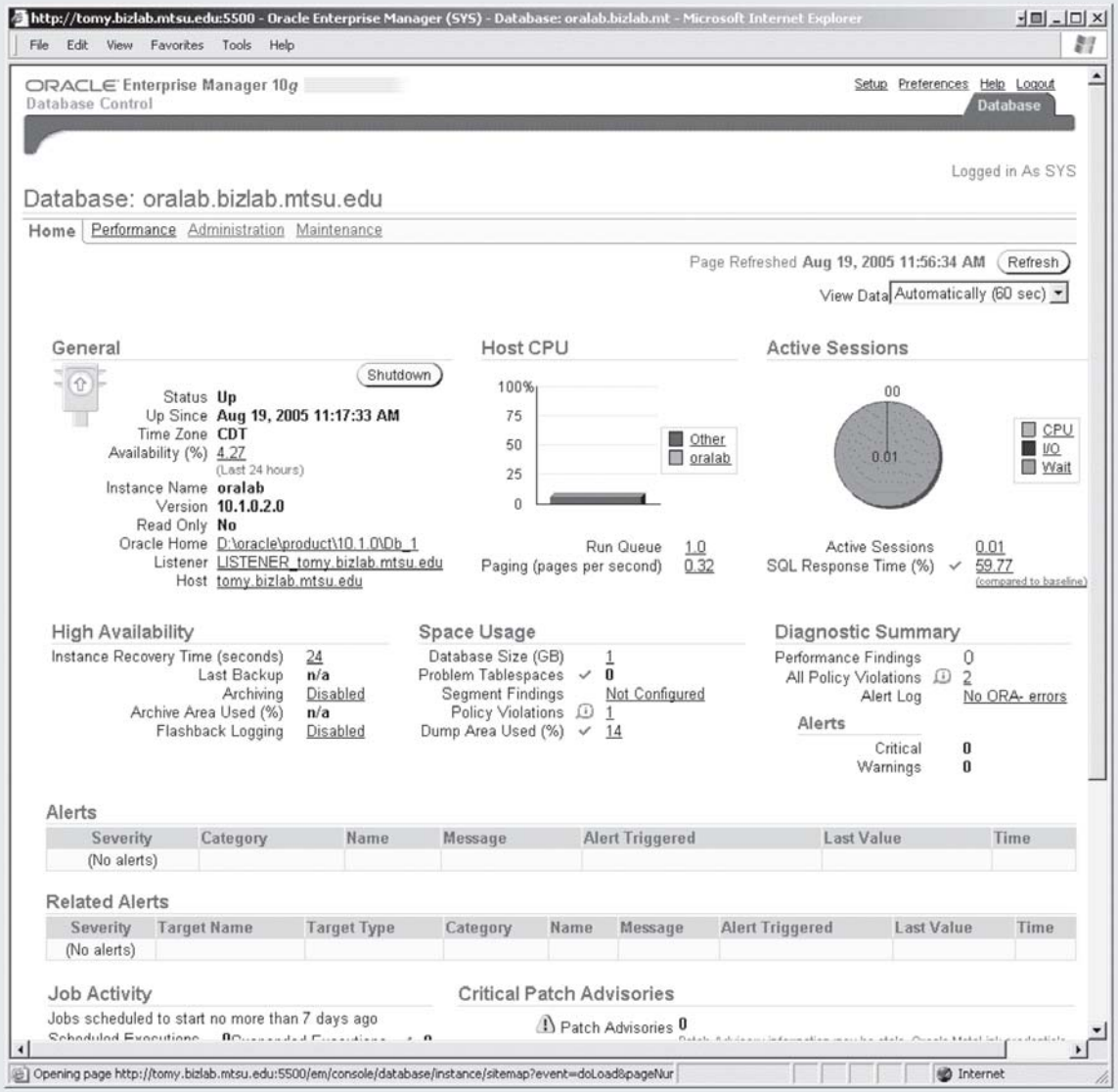
DBA em Ação: utilização de Oracle para a administração de banco de dados

- Tarefas técnicas de um SGBD específico:
  - Criação e expansão das estruturas de armazenamento do banco de dados
  - Gerenciamento de objetos de banco de dados
  - Gerenciamento do ambiente de banco de dados do usuário final
  - Personalização dos parâmetros de inicialização do banco de dados
- Todos os fornecedores disponibilizam um conjunto de programas que fazem interface com o banco de dados e executam uma ampla faixa de tarefas administrativas

Ferramentas de Administração de Banco de dados Oracle

- Todos os fornecedores de bancos de dados oferecem um conjunto de ferramentas de administração
- No Oracle, a maioria das tarefas de DBA é executada por meio da interface Oracle Enterprise Manager

FIGURA 15.9 Interface Oracle Enterprise Manager



Login Padrão

- Conectar-se ao banco de dados utilizando um nome de usuário com privilégios administrativos (DBA)
  - Usuários que possuem privilégios
- O Oracle cria automaticamente as IDs de usuário SYSTEM e SYS
- Define as credenciais preferidas para cada banco de dados clicando no link **Preferences** no topo da página e, em seguida, em **Preferred Credentials**
- Os nomes de usuário e senhas são específicos do banco de dados

Garantia de Inicialização Automática do SGBDR

- O DBA garante que o acesso ao banco de dados seja inicializado automaticamente ao ligar o computador
- *Serviço* é o nome do sistema Windows para um programa especial executado automaticamente como parte do sistema operacional
- **Instância de bancos de dados**: separada da memória, reservada para executar determinado banco de dados
  - É possível haver vários bancos em execução simultânea na memória

Criação de Tablespaces e Datafiles

- Um banco de dados é *logicamente* composto de uma ou mais tablespaces
- **Tablespace** é um espaço de armazenamento lógico
  - Agrupa dados logicamente relacionados
- **Datafile** armazena fisicamente os dados do banco
  - Cada datafile pode residir em um diretório diferente do disco rígido

Gerenciamento de Objetos de Banco de Dados: tabelas, visualizações, triggers e procedimentos

- **Objeto de banco de dados** é basicamente qualquer objeto criado por usuários finais
- O **esquema** do Oracle é uma seção lógica do banco de dados que pertence a determinado usuário
  - É identificado pelo nome de usuário
  - No interior do esquema, os usuários podem criar suas próprias tabelas e outros objetos
- Normalmente, os usuários são autorizados a acessar apenas os objetos que pertençam a seus próprios esquemas

Personalização dos Parâmetros de Inicialização do Banco de Dados

- A sintonização refinada exige a modificação de parâmetros de configuração
  - Alguns podem ser alterados em tempo real utilizando-se comandos de SQL
  - Outros exigem que o banco de dados seja fechado e reinicializado
  - Alguns parâmetros podem afetar o SGBDR em sua totalidade e todas as instâncias em execução
- Uma das funções importantes fornecidas pelos parâmetros de inicialização é reservar os recursos que devem ser utilizados pelo banco de dados durante a execução
- Uma vez modificados os parâmetros de inicialização, pode ser necessário reinicializar o banco de dados

Criação de um Novo Banco de Dados

- Embora o formato geral de criação de bancos de dados tenda a ser universal, sua execução costuma ser específica de cada SGBD
- Os líderes no fornecimento de SGBDR oferecem ao DBA a opção de criar bancos de dados manualmente, utilizando comandos de SQL ou processos com base em GUI
- Utilizando o assistente de configuração de bancos de dados do Oracle, é simples criar um banco de dados com a ajuda de um assistente

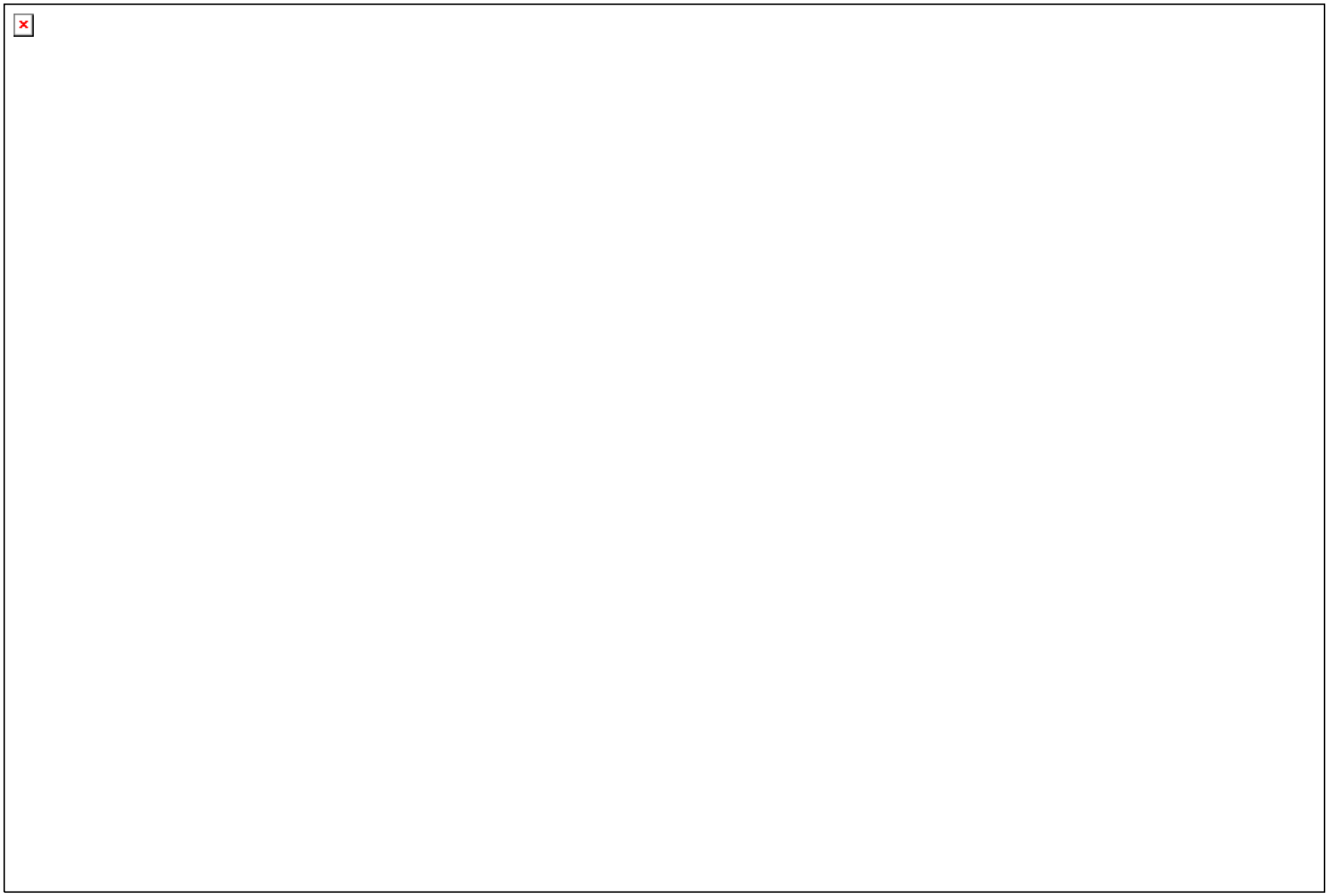


FIGURA 15.30 Progresso da criação do banco de dados

Resumo

- O gerenciamento de dados é uma atividade fundamental de qualquer organização
  - Os dados devem ser tratados como um bem corporativo
- O SGBD é a ferramenta eletrônica utilizada com mais frequência no gerenciamento de dados corporativos
- É necessário examinar cuidadosamente o impacto do SGBD sobre o modelo gerencial e cultural da organização
- O desenvolvimento da função de administração de banco de dados baseia-se na evolução do departamento de processamento de dados para um departamento de processamento eletrônico de dados

Resumo (cont.)

- O administrador de banco de dados (DBA) é responsável pelo gerenciamento de bancos de dados corporativos
- Essa atividade mais ampla de gerenciamento de dados é tratada pelo administrador de dados (AD)
- O AD é mais orientado para aspectos gerenciais e o DBA, para aspectos técnicos
  - A função de DBA é independente de SGBD
- Quando a estrutura da organização não inclui uma posição de AD, o DBA executa todas as suas funções

Resumo (cont.)

- Os serviços gerenciais da função de DBA incluem:
  - Suporte à comunidade de usuários finais
  - Definição e aplicação de políticas, procedimentos e padrões para a função de banco de dado
  - Garantia de segurança, privacidade e integridade de dados
  - Fornecimento de serviços de backup e recuperação de dados
  - Monitoramento da distribuição e utilização dos dados no banco

Resumo (cont.)

- O papel técnico exige que o DBA esteja envolvido, pelo menos, nas seguintes atividades:
  - Avaliação, seleção e instalação do SGBD
  - Projeto e implementação de banco de dados e aplicações
  - Teste e avaliação de bancos de dados e aplicações
  - Operação do SGBD, utilitários e aplicações
  - Treinamento e suporte aos usuários
  - Gerenciamento do SGBD, utilitários e aplicações

Resumo (cont.)

- A segurança refere-se às atividades e medidas que garantem a confidencialidade, integridade e disponibilidade de um sistema de informação e seus principais ativos, os dados
- A política de segurança é um conjunto de padrões, políticas e práticas
- A vulnerabilidade de segurança é um ponto fraco em um componente do sistema

Resumo (cont.)

- Para orientar o desenvolvimento desse plano geral, é necessária uma metodologia de integração
  - A metodologia de integração utilizada com mais frequência é conhecida como engenharia da informação (EI)
- Para ajudar a traduzir os planos estratégicos em planos operacionais, o DBA tem acesso a um arsenal de ferramentas de administração de banco de dados
  - Incluem o dicionário de dados e as ferramentas de engenharia de software assistida por computador (CASE)