CARLOS EDUARDO COSTA VANINI

UMA ABORDAGEM DE SEGURANÇA EM BANCO DE DADOS PARA SISTEMAS DE INFORMAÇÃO

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação.

UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS

Orientador: Eduardo Macedo Bhering
Co-orientador: Mestre Elio Lovisi Filho

BARBACENA
2003

CARLOS EDUARDO COSTA VANINI

UMA ABORDAGEM DE SEGURANÇA EM BANCO DE DADOS PARA SISTEMAS DE INFORMAÇÃO

Este trabalho de conclusão de curso foi julgado adequado à obtenção do grau de Licenciado em Ciência da Computação e aprovado em sua forma final pelo Curso de Ciência da Computação da Universidade Presidente Antônio Carlos.

Barbacena – MG, 09 de julho de 2003.

_____

Prof. Eduardo Macedo Bhering - Orientador do Trabalho

_____

Mestre Elio Lovisi Filho - Membro da Banca Examinadora

_____

Mestre Lorena Sophia C. de Oliveira- Membro da Banca Examinadora

AGRADECIMENTOS

Agradeço a Deus por ter me dado condições para realizar este trabalho, aos professores Élio, Eduardo pela colaboração e a todos que de alguma forma contribuíram para que eu pudesse realizar com sucesso este trabalho.

RESUMO

Com a crescente informatização das organizações, cresce cada vez mais a utilização de sistemas de informações nas empresas.

O componente do sistema de informação a ser abordado neste estudo é o componente banco de dados. Esse componente tem sido muito utilizado nas organizações pela necessidade de armazenamento dos dados da empresa. Juntamente com a crescente utilização de banco de dados, surge a preocupação com a questão de segurança já que vários usuários acessam os dados armazenados no banco.

Será apresentado um estudo de caso, utilizando o banco de dados existente na unidade CHPB, onde será abordado questões de segurança. Uma importante ferramenta para a garantia de segurança dos dados é o uso de visões.

SUMÁRIO

LISTAS

1 INTRODUÇÃO

1.1 MOTIVAÇÃO

Este trabalho foi motivado pelo fato de que cada vez mais, maior número de empresas estarem utilizando banco de dados, para armazenar suas informações.

Com essa crescente utilização de banco de dados, surge uma grande preocupação em relação a questões de segurança dos dados, já que pessoas não autorizadas podem por algum motivo ter acesso a esses dados, podendo causar algum dano à empresa.

Em se tratando de segurança existe um tópico muito interessante que é a questão de visões. Com visões podemos garantir que determinados usuários tenham acesso somente aos dados no quais tenham permissão para acessa-los.

1.2 OBJETIVO

Geral

O objetivo geral deste estudo é procurar garantir que usuários não acessem dados aos quais não tenham permissão.

Específico

Apresentar um estudo sobre segurança em banco de dados, mostrando através de visões uma forma garantir a segurança dos dados armazenados.

Com base nos conceitos de visões será feita a modelagem e a implementação de um sistema empresarial, a fim de exemplificar o uso dos conceitos estudados.

2 SISTEMA DE INFORMAÇÃO EM ORGANIZAÇÕES

Segundo [Laudon, 1999], um sistema de informação (SI) pode ser definido como um conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informação com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo discricionário em empresas e outras organizações.

2.1 ESTRUTURA DE UMA ORANIZAÇÃO

Segundo [Lima], a estrutura de uma organização é o conjunto de funções, cargos, relações e responsabilidades que constituem o desenho orgânico da empresa. A estrutura organizacional de uma empresa geralmente está demonstrada em organogramas, funcionogramas e fluxogramas de atividades.

A estrutura de uma organização representa, a medida exata daquilo que a sua direção idealiza como caminho para atingir os objetivos e a maneira como valoriza e distribui os seus módulos operativos dentro do contexto empresarial.

Uma estrutura organizacional pode ser representada da seguinte maneira:

- Funcional;

- Geográfico;
- Por processo;
- Por Produto;
- Por cliente;
- Da amplitude de controle

2.1.1 FUNCIONAL

A departamentalização funcional é aquela que leva em conta a especialização técnica dos ocupantes dos cargos e seus conhecimentos, conforme figura abaixo.

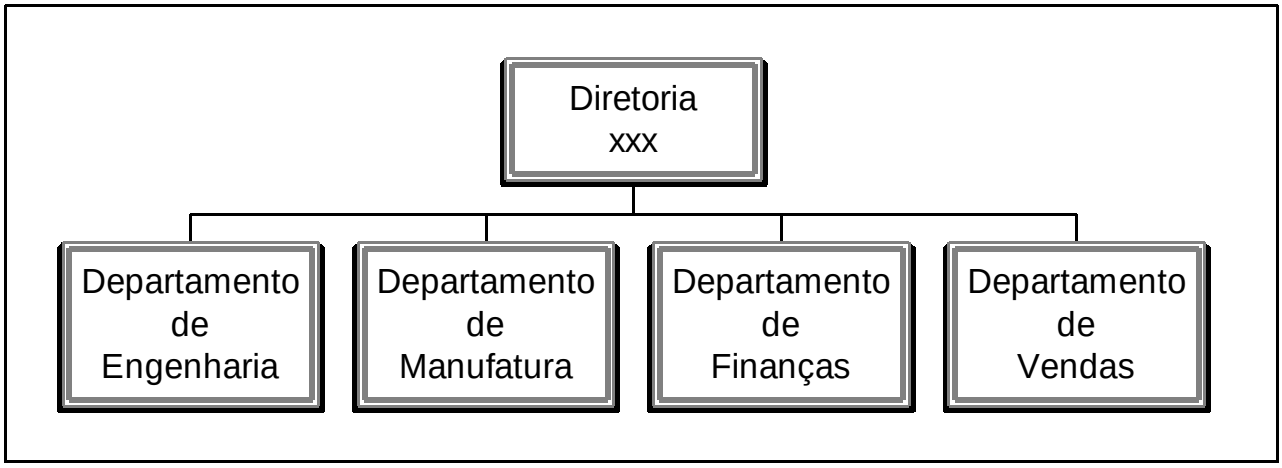


Figura 1: Departamentalização Funcional

2.1.2 GEOGRÁFICO

A departamentalização geográfica é

aquela que leva em conta onde se encontra a fábrica, empresa ou filial como critério de divisão interna, conforme figura abaixo.

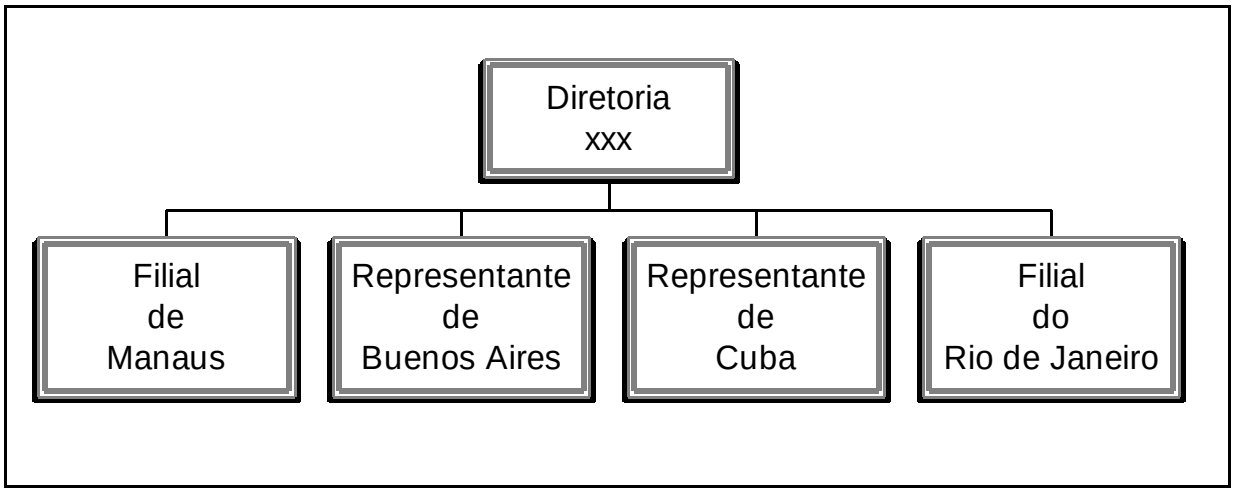


Figura 2: Departamentalização Geográfica

2.1.3 POR PROCESSO

Na departamentalização por processo, divide-se a estrutura em subsistemas que representam diferentes passos ou fases do todo, conforme figura abaixo.

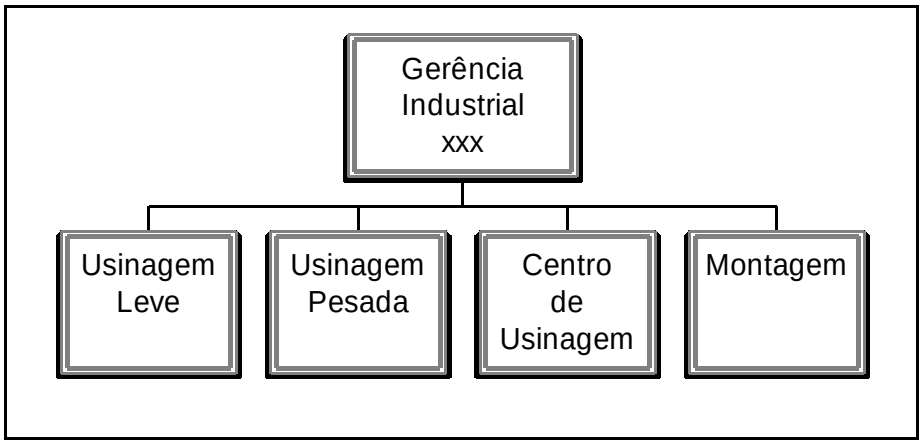


Figura 3: Departamentalização por Processo

2.1.4 POR PRODUTO

A departamentalização por produto ou serviço leva em consideração a subdivisão por produto ou serviço fabricados ou oferecidos, conforme figura abaixo.

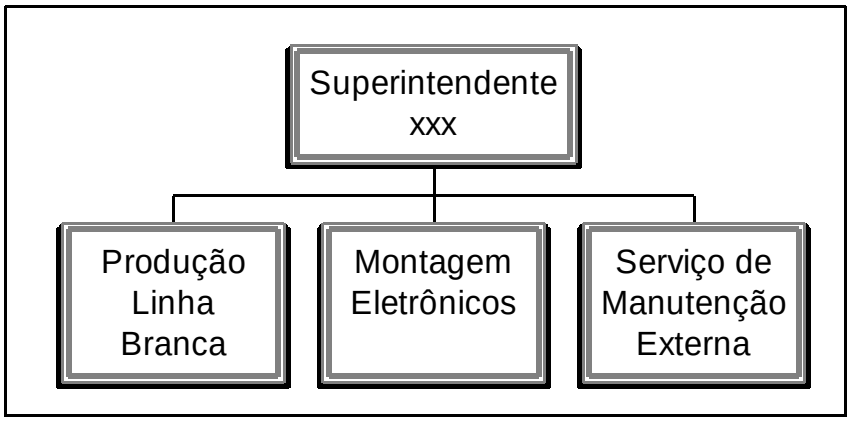


Figura 4: Departamentalização por Produto ou Serviço

2.1.5 POR CLIENTE

A departamentalização por cliente leva em consideração as especialidades dos clientes, agrupando-os em equipes de dedicação exclusiva, conforme figura abaixo.

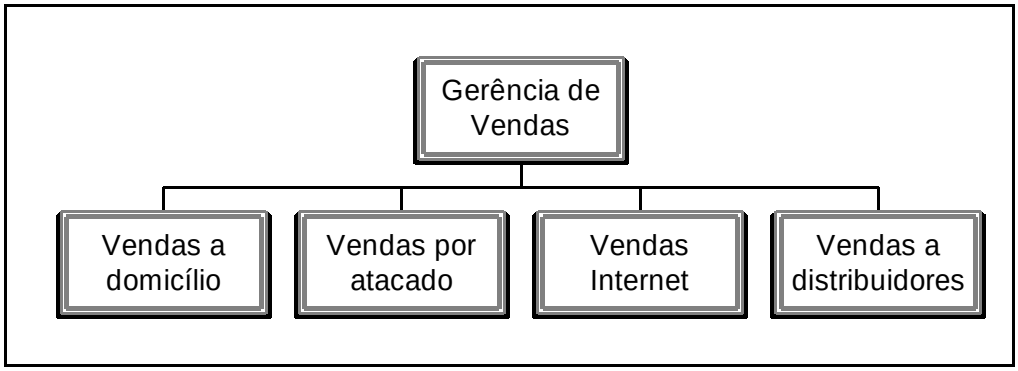


Figura 5: Departamentalização por Cliente

2.1.6 DA AMPLITUDE DE CONTROLE

A departamentalização pela amplitude de controle leva em consideração o tamanho da equipe que está sob o comando de um gerente, conforme figura abaixo.

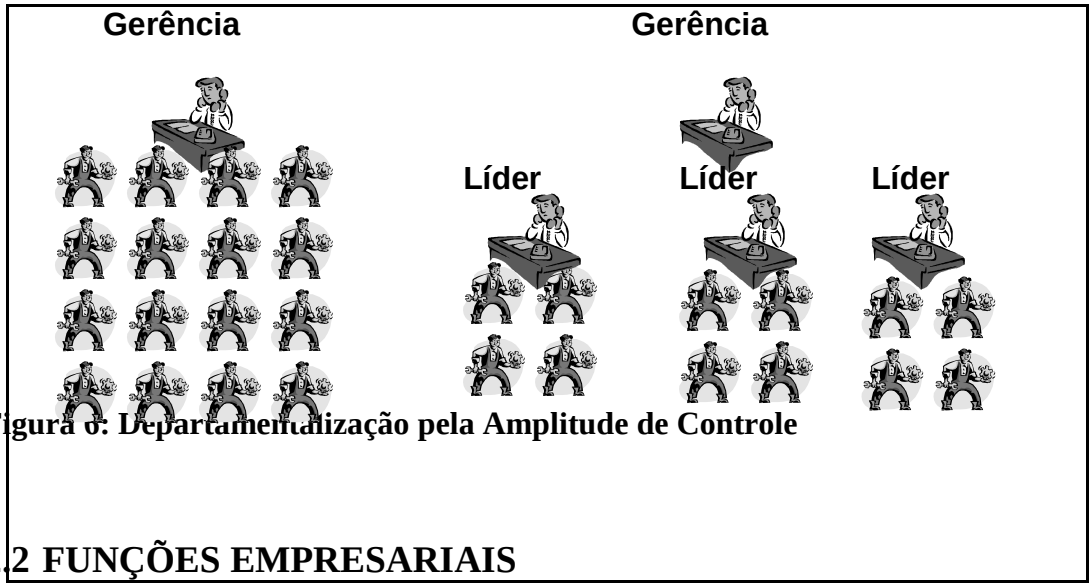


Figura 6: Departamentalização pela Amplitude de Controle

2.2 FUNÇÕES EMPRESARIAIS

Abaixo são citadas as funções empresariais:

- Produção: gerar o produto ou serviço.
    - Arranjo de pessoas, máquinas e procedimentos.
- Vendas e Marketing: vender o produto ou serviço.
- Recursos Humanos: selecionar, treinar, contratar e motivar o pessoal da empresa (colaboradores).
    - Controle de funcionários.
- Finanças e Contabilidade: Controlar a parte financeira da organização.

2.3 NÍVEIS DE UMA EMPRESA

Uma empresa está dividida em níveis, como os citados abaixo:

- Gerência Sênior: tomada de decisões a longo prazo sobre os produtos ou serviços fornecidos pela empresa.
- Gerência Média: executa os programas da gerência sênior, supervisionando empregados.
- Trabalhadores do Conhecimento: desenvolvem o produto ou serviço (como os engenheiros) e administram os documentos associados à empresa (como os funcionários de escritório).
- Funcionários de Produção (ou serviços): produzem efetivamente os produtos ou serviços da firma.

Uma organização difere da outra quanto à autoridade concentrada em cada camada, não existe organização onde a autoridade é concentrada no topo, em algumas existe um número pequeno de gerentes seniores, uma camada de gerência média seguida imediatamente pelos funcionários de produção, já em organizações mais burocráticas existem várias camadas de gerência.

2.4 SISTEMAS EMPRESARIAIS: FUNÇÕES E PROCESSOS

Os sistemas empresariais são classificados de acordo com o tipo de problema organizacional que resolvem.

- Estratégico: envolvem objetivos da organização e sobrevivência a longo prazo. Ex.: Sistemas para auxiliar na decisão sobre novos produtos.

- Tático: envolvem como atingir os objetivos. Ex.: Acompanhamento de vendas (metas).
- Conhecimento: envolvem a criação, a distribuição e o uso das informações. Ex.: Sistemas de escritório.
- Operacionais: envolvem a solução de problemas relativos à produção. Ex.: Controle de maquinário.

2.5 COMPONENTES DE SISTEMAS DE INFORMAÇÃO

2.5.1 SOFTWARE

Segundo [Laudon, 1999], o software de computador consiste em instruções pré-programadas que coordenam o trabalho dos componentes do hardware para que executem os processos exigidos por cada sistema de informação. Sem o software, o computador não saberia o que fazer e como e quando fazê-lo. O software consiste em programas que se relacionam, e cada um deles é um grupo de instruções para executar tarefas específicas de processamento.

2.5.2 HARDWARE

Segundo [Laudon, 1999], o hardware em um sistema de informação é o equipamento físico usado para as tarefas de entrada, processamento e saída do sistema. O hardware consiste na unidade de processamento do computador e nos vários dispositivos de entrada, saída e armazenamento, além dos meios físicos que interligam esses dispositivos.

O hardware de entrada é responsável por coletar os dados e os converter em uma forma em que o computador possa processar. O hardware de processamento transforma entrada em saída com base em instruções fornecidas ao computador através de software.

O hardware de saída entrega a saída de um sistema de informação ao seu usuário, e em geral consiste em impressoras e terminais de vídeo.

Um componente de hardware muito importante é a tecnologia de armazenamento, que é utilizada para organizar e armazenar os dados utilizados por uma empresa. A tecnologia de armazenamento inclui meios físicos para armazenar dados, como discos magnéticos, óticos ou fitas, assim como o software que rege a organização de dados nesses meios físicos.

2.5.3 TELECOMUNICAÇÕES

Segundo [Laudon, 1999], telecomunicações são usadas para conectar partes diferentes do hardware e para transferir dados de um ponto a outro via redes. Uma rede liga dois ou mais computadores entre si para transmitir dados, voz, imagens, sons e vídeo ou para compartilhar recursos como, por exemplo, uma impressora.

2.5.4 BANCO DE DADOS

2.5.4.1 Definição de Banco de Dados

Segundo [Date, 2000] um banco de dados é uma coleção de dados persistentes utilizada pelos sistemas de aplicação de determinada empresa.

Um dado é dito persistente, pois ao ser inserido na base de dados ele fica armazenado até que através de uma operação de exclusão do SGBD, que após ser executada o dado será excluído.

Segundo [Date, 2000] o termo “empresa” é apenas um termo genérico conveniente para qualquer organização comercial, científica, técnica ou outra organização razoavelmente autônoma. Uma empresa poderia ser desde um único individuo até uma grande empresa.

A vantagem de utilizar banco de dados é torná-los independentes da aplicação. As aplicações, que antes acessavam os dados diretamente, com banco de dados passaram a se comunicar com o SGBD, enviando apenas as requisições necessárias para obter os resultados desejados.

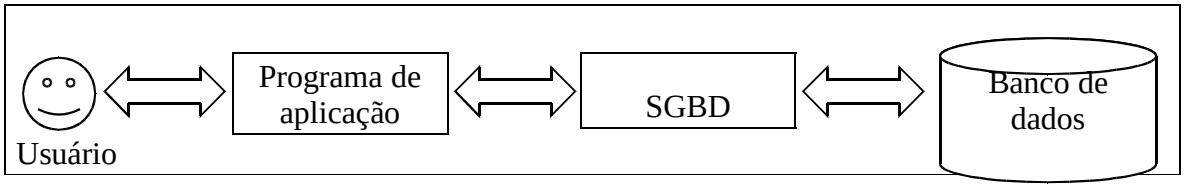


Figura 7: Representação de um banco de dados.

2.5.4.2 Sistema de banco de dados

Segundo [Date, 2000] um sistema de banco de dados consiste no armazenamento computadorizado de informações, permitindo ao usuário buscar e atualizar estas informações quando necessário.

Um sistema de banco de dados possui quatro componentes principais: dados, hardware, software e usuários.

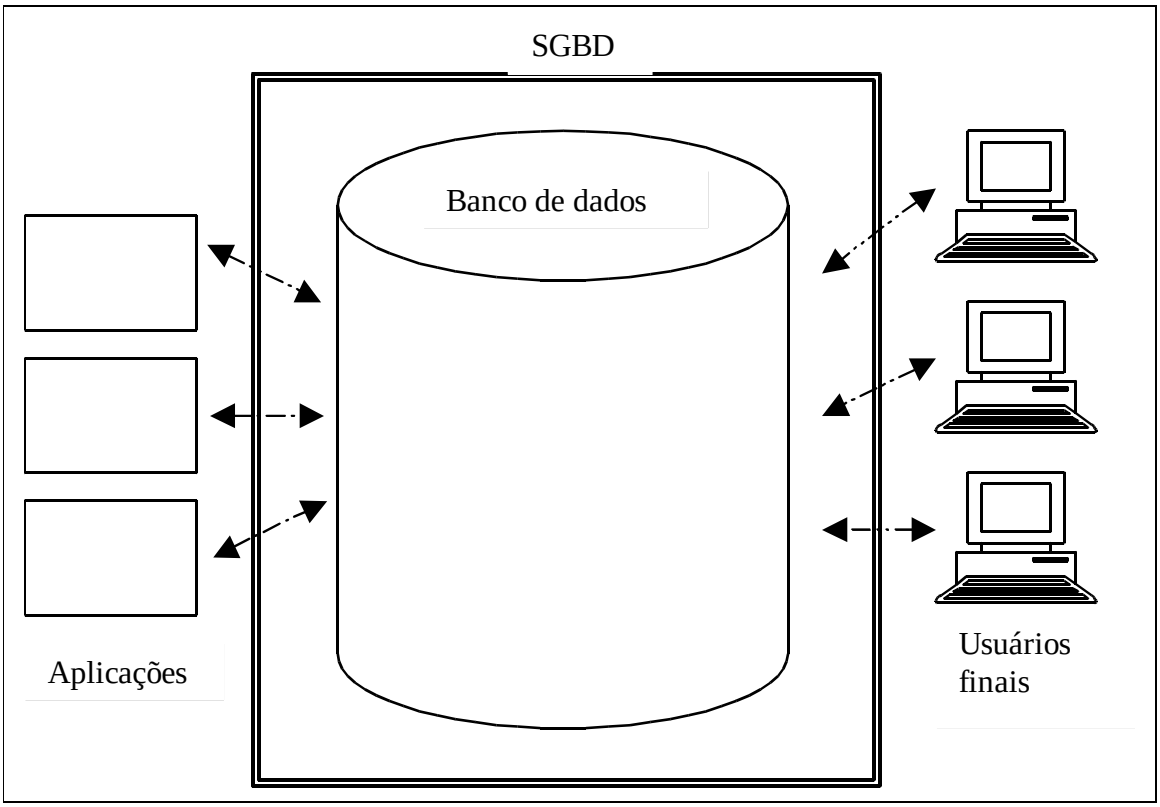


Figura 8: Representação simplificada de um sistema de banco de dados.

2.5.4.2.1 Software

O software é uma camada que está localizada entre os dados armazenados e os usuários. Esta camada é conhecida por gerenciador do banco de dados, servidor de banco de dados ou sistema gerenciador de banco de dados (SGBD). O SGBD trata todas as solicitações de acesso ao banco de dados, além de operações básicas em um sistema de banco de dados como: inserir, buscar, alterar, eliminar dados.

2.5.4.2.2 Hardware

Os componentes de hardware de um sistema de banco de dados consistem em:

- Volumes de armazenamento secundário: principalmente discos magnéticos – usados para guardar os dados armazenados.
- Processador(es) e memória principal: usados para fornecer suporte à execução do software do sistema de banco de dados.

2.5.4.2.3 Dados

Um sistema de banco de dados pode ser de duas formas: monousuários, multiusuários. Um sistema monousuário é um sistema em que apenas um usuário pode ter acesso ao banco de dados num dado instante, já um sistema multiusuários, é um sistema que permite que vários usuários tenham acesso ao banco de dados ao mesmo tempo.

Os dados do banco de dados estarão de certa forma integrados e compartilhados, ou seja, um banco de dados é dito integrado quando unifica vários arquivos de dados distintos; e quando se diz compartilhado é devido ao fato de que partes isoladas de dados do

banco de dados podem ser compartilhadas entre diferentes usuários, de forma que cada um dos usuários poderá ter acesso à mesma porção de dados.

2.5.4.2.4 Usuários

Existem três classes de usuários:

- Programadores de aplicações: são responsáveis pela elaboração de programas aplicativos de banco de dados em uma linguagem de programação. Os programas têm a função de permitir que o usuário tenha acesso ao banco de dados através de uma estação de trabalho ou de um terminal on-line.

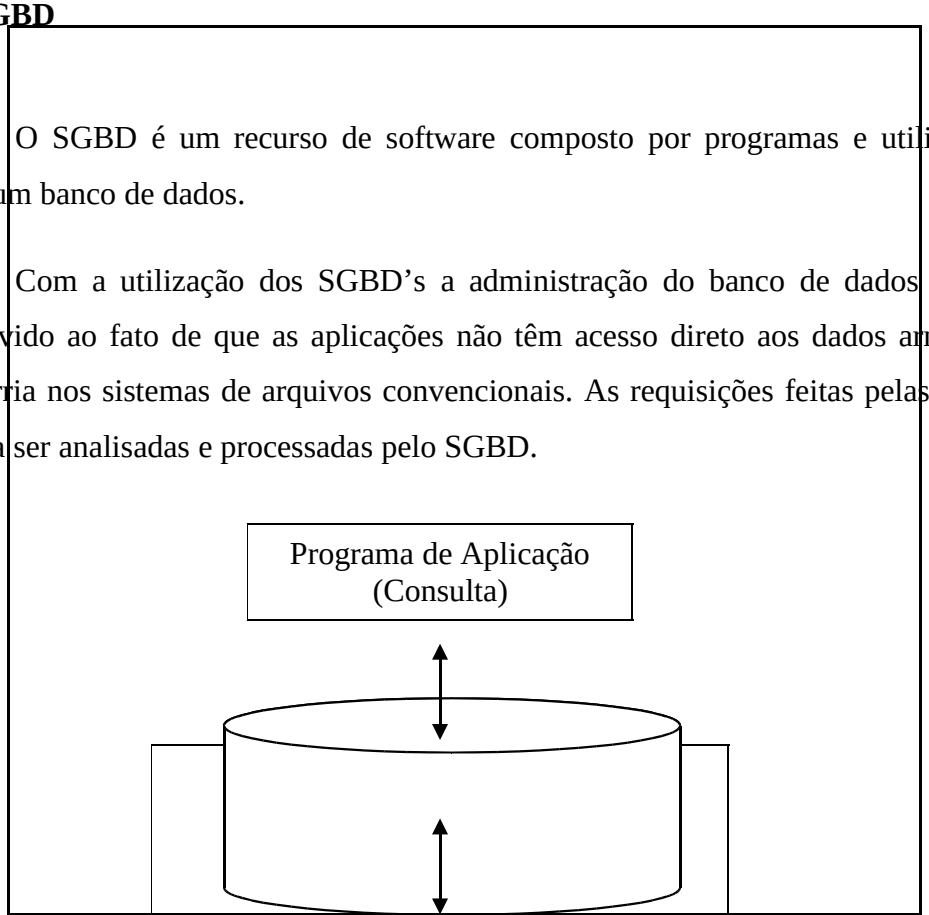
- Usuários finais: são usuários que têm acesso ao banco de dados através de terminais ou estações de trabalho on-line.

- Administrador de banco de dados (DBA): é o responsável em decidir que dados devem ser armazenados no banco de dados, estabelecer normas para manter e tratar os dados armazenados. O trabalho do DBA é criar o banco de dados, colocar em práticas as normas estabelecidas, além de assegurar que o sistema tenha um desempenho adequado.

2.5.4.3 SGBD

O SGBD é um recurso de software composto por programas e utilitários para gerenciar um banco de dados.

Com a utilização dos SGBD's a administração do banco de dados ficou mais segura, devido ao fato de que as aplicações não têm acesso direto aos dados armazenados, como ocorria nos sistemas de arquivos convencionais. As requisições feitas pelas aplicações passaram a ser analisadas e processadas pelo SGBD.



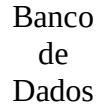


Figura 9: Estrutura de um SGBD.

2.5.4.4 Diferenças entre um banco de dados e um sistema tradicional de arquivos

Em um sistema tradicional de arquivos, é implementado um ou mais arquivos para a necessidade de cada usuário, já em um banco de dados existe um único repositório de dados, donde todos usuários acessaram os dados que lhes convém. Abaixo estão listadas algumas características que diferem um banco de dados de um sistema tradicional de arquivos:

- Existência um dicionário de dados: fundamental característica de um banco de dados é dizer que o SGBD não contém apenas a base de dados, existe também o armazenamento da descrição da estrutura dos dados armazenados. Este armazenamento pode ser definido como um sistema de dicionário de dados. Nele estão contidas informações, como a estrutura de cada arquivo, o tipo e o formato de cada dado armazenado. As

informações armazenadas neste dicionário são chamadas **metadados**. Em um sistema tradicional de arquivos a definição dos dados é feita na própria implementação dos programas de aplicação. Conseqüentemente estes programas são desenvolvidos para trabalhar com uma base de dados específica, enquanto em um SGBD é possível acessar diversas bases de dados.

- Independência entre programa-dado e programa-operação: Em um sistema tradicional de arquivos devido ao fato da estrutura dos dados estarem embutidas nos programas de aplicação, uma mudança na estrutura de um arquivo implicaria na mudança do programa de aplicação, já em um SGBD essa mudança na estrutura de um dado não necessariamente implicaria em mudanças no programa de aplicação, mesmo que houvesse tal necessidade as mudanças seriam mais fáceis de serem aplicadas. A independência entre programa-dado é permitida graças à implementação do dicionário de dados. O mesmo acontece na implementação ou alteração das operações, em que usando um SGBD as inclusões ou alterações poderiam ser realizadas sem afetar o programa de aplicação. Essa independência é conhecida como independência lógica.

- Abstração de dados: O SGBD permite abstração de dados, através da qual é conseguido a independência entre programa-dado e programa-operação, essa abstração significa esconder do usuário detalhes de como os dados são armazenados ou como as operações básicas são implementadas.

- Suporte a múltiplas visões de dados: O SGBD através do suporte a múltiplas visões de dados permite que usuários diferentes tenham acesso à mesma base de dados, porém cada usuário visualiza os dados de modos diferentes, chamados visões.

- Compartilhamento de dados entre múltiplas transações: Um SGBD com tal característica é dito multiusuários, ou seja, vários usuários acessam a base de dados ao mesmo tempo.

2.5.4.5 Vantagens em utilizar um SGBD

Será mostrado algumas vantagens de se utilizar um sistema de controle de dados centralizados, ou seja, as vantagens da utilização de um banco de dados, e o que um bom SGBD deve oferecer.

- Compartilhamento de dados: Compartilhar dados significa que as várias aplicações existentes podem compartilhar o banco de dados, outra vantagem do compartilhamento de dados é que novas aplicações podem ser desenvolvidas e acessar os mesmos dados antes acessados pelas outras aplicações sem a necessidade do acréscimo de novos dados ao banco de dados.

- Controle de redundância: Em um sistema de arquivos tradicional cada grupo de aplicações mantém seus próprios arquivos, que serão controlados pelas aplicações de sistema. A redundância pode gerar o desperdício do espaço de armazenamento, alem da inconsistência dos dados (que será tratado em seguida). A redundância consiste no armazenamento de forma desnecessária dos dados várias vezes. Um SGBD é um banco de dados distribuído, onde cada parte do banco pode estar em locais diferentes, porém são centralizados pelo SGBD. É importante lembrar que um SGBD não visa eliminar a redundância dos dados, mas sim fazer um cuidadoso controle, já que em alguns casos a redundância se torna essencial (por razões comerciais ou técnicas).

- Inconsistência de dados: A inconsistência de dados está intimamente ligada à redundância. A inconsistência pode ocorrer também quando uma

regra de integridade ou restrição é violada Suponhamos um fato do mundo real – um empregado E1 trabalha no departamento D5 – seja representado por duas entradas diferentes no banco de dados (porém o SGBD não tem conhecimento dessa redundância). Poderá haver em determinada ocasião em que as duas entradas não concordaram, ou seja, quando uma das entradas tiver sido atualizada e a outra não. Ocorrendo tal situação é dito que o banco de dados se encontra em um estado inconsistente (ou incoerente). Quando um banco de dados encontra-se em um estado inconsistente possivelmente fornecerá ao usuário informações incorretas ou contraditórias. Se houver uma redundância controlada (conhecida pelo SGBD), o SGBD poderá garantir ao usuário que o banco de dados nunca estará inconsistente, utilizando para isso o que chamamos de propagação de atualizações, ou seja, ao efetuar qualquer mudança em uma entrada o SGBD aplicará as mudanças nas demais entradas.

- Suporte a transações: Segundo [Date, 2000] uma transação é uma unidade lógica de trabalho, em geral envolvendo diversas operações de banco de dados (em particular, várias operações de atualização). Um exemplo clássico de transação é o seguinte: suponhamos que determinado usuário deseja retirar dinheiro da conta A e depositar na conta B. Considerando que será feito duas atualizações o sistema deve garantir que as duas atualizações sejam realizadas ou que nenhuma delas seja efetivada (por exemplo, uma queda de energia em meio à transação).

- Integridade dos dados: A integridade dos dados significa que os dados devam estar corretos no banco de dados. Um exemplo de falta de integridade seria um empregado ter trabalhado 40 horas na semana e o sistema estar mostrando 400 horas. Para evitar que aconteça isto é necessária a implementação de restrições de integridade (conhecidas também como regras de negócio), que são verificadas sempre que acontece alguma operação de atualização.

- Restrição de acessos não autorizados: Devido ao fato de vários usuários compartilharem os dados de um mesmo banco de dados, pode ocorrer que pessoas não autorizadas tenham acesso aos dados, ou efetuem operações que não lhes são permitidas. Para evitar o acesso não autorizado o SGBD deve fornecer um sub-sistema de segurança e autorização, ficando a cargo do DBA criar grupos de usuários e especificar as restrições de cada grupo.

- Sistema de Backup e Restauração de Backup: O SGBD deve disponibilizar recursos para a realização de backup e restauração do mesmo. Por exemplo, quando um usuário estiver realizando uma operação e por algum motivo ocorrer uma falha, o SGBD deve permitir que o usuário volte o banco de dados ao estado anterior à falha, garantindo assim ao usuário a integridade dos dados.

2.5.4.6 Modelo de Representação de Dados

O modelo de representação de dados está ligado à forma que os dados serão modelados do mundo real para uma aplicação de banco de dados, definindo a maneira como os dados serão acessados e manipulados pelos usuários.

Atualmente existem várias áreas que utilizam banco de dados, para armazenar e manipular seus dados.

Ao contrário do que muitos pensam, não existem somente aplicações com banco de dados tradicionais, onde a maioria das informações são textuais e numéricas, existem outros tipos como:

- Banco de dados multimídia: armazenam imagens, vídeo clips e sons.

- Sistemas de informação geográfica (SIG’s): armazenam e analisam mapas, dados sobre o tempo e imagens de satélites.

- Data warehouses e processamento analítico on-line (OLAP) : são sistemas utilizados em companhias com o objetivo de extrair e analisar informações de grandes bases de dados.

- Tempo real: é usado para controlar o processo de fabricação em industrias, controle de tráfego aéreo.

Atualmente o modelo relacional é o mais utilizado, porém com a necessidade de utilizar sistemas capazes de gerenciar dados complexos, houve a necessidade de criar novos modelos de tratamento de dados.

Abaixo segue uma descrição sobre os principais modelos de dados existentes:

- **Modelo Relacional**

Criado em 1970 por Codd, com o intuito de tornar mais fácil a modelagem de um problema do mundo real para um sistema de banco de dados, além de permitir aos SGBD's processar os dados de maneira mais eficiente. Neste modelo os dados são representados em forma de tabelas, existindo entre as tabelas um relacionamento a fim de garantir a integridade dos dados.

- **Modelo Orientado a Objetos**

Segundo [Silva, 2001], com o surgimento de novas aplicações, surge então novos tipos dados aos quais temos que tratar. O fato da necessidade de estruturar e trabalhar com os novos tipos de dados não convencionais foi necessária a criação de um novo modelo intitulado de modelo orientado a objetos.

O modelo orientado a objetos utiliza-se de conceitos de orientação a objetos já utilizados em linguagens de programação orientada a objetos como, por exemplo, SmallTalk e C++.

O principal objetivo do modelo Orientado a Objetos é tratar os tipos de dados complexos como tipos abstratos de dados, ou seja, como objetos.

Uma das vantagens de um SGBD Orientado a Objetos é a capacidade de integração com linguagens OO, permitindo assim usar de recursos de uma linguagem OO.

O modelo Orientado a Objetos permite que os usuários definam tipos de dados que serão gerenciados pelo SGBD. Neste modelo não existe dependência de relacionamentos.

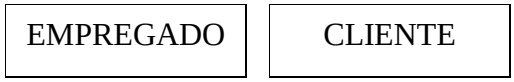
O padrão usado no desenvolvimento de um banco de dados orientado a objetos é o SQL3, proposto pelos comitês ISO e ANSI, que na verdade é uma extensão do SQL 92, usada nos modelos relacionais.

A figura abaixo ilustra o uso do modelo orientado a objetos, onde existem três classes, onde as classes empregado e cliente são uma herança da classe pessoa.

Este modelo é usado com mais freqüência para a construção de banco de dados orientados a objetos de áreas complexas como:

- **Modelo Objeto-Relacional**

Recentemente, surgiram os SGBD's objeto-relacionais [Stonebraker, M. Moore, D. 1996], estes SGBD's dão suporte a um modelo relacional estendido com certos aspectos de orientação a objetos.



Segundo [Silberschatz e Korth, 1999] "Os sistemas de bancos de dados objeto-relacionais fornecem um conveniente caminho de migração para usuários de bancos de dados relacionais que desejam usar características orientadas a objetos".

3 SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

3.1 CONCEITOS BÁSICOS

- **Segurança** - pode ser definido como o estado daquele indivíduo (ou sistema) que se encontra seguro, imune a acidentes ou ataques que possam lhe causar danos físicos e/ou econômicos. A segurança de um sistema de informação (SI) refere-se a normas, procedimentos, ferramentas e técnicas para garantir que os SI’s não tenham perdas físicas e lógicas.

- **Segurança na Área de Informática**

A segurança na área de informática está relacionada a dois pontos importantes, safety e security. Ao estabelecer uma boa política de segurança esses dois pontos devem ser levados consideração.

- **Safety** - Segurança relacionada a suporte de acontecimentos casuais do sistema, ou seja, o sistema deve tolerar ações inadvertidas. Mais aplicável em Sistemas de controle.
- **Security** - Segurança relacionada com proteção do sistema a ações maliciosas (intencionais).

3.2 SEGURANÇA FÍSICA

A segurança física de um sistema de informação está relacionada com a garantia do estado seguro dos equipamentos.

Abaixo são apresentadas algumas medidas que são usadas para garantir a proteção física dos recursos contra ameaças voluntárias (roubos, invasões) e involuntárias (incêndio, acidentes):

- Controle de acesso aos componentes do sistema;
- Formas de Prevenção e controle de incêndios;
- Dispositivos para Backup;
- Controle de Queda de Energia.

Existem medidas que devem ser tomadas desde a montagem de um sistema de informação até seu funcionamento:

- Observadas desde a montagem do Sistema:
  - Prevenção a Danos causados pela água (telhados, subsolo);
  - Prevenção a Incêndios (detecção, alarme e combate);
  - Climatização do ambiente;
  - Dimensionamento e qualidade do sistema elétrico
    - Pára-raios;
    - No-Breaks;
    - Qualidade dos cabos, transformadores e estabilizadores.
  - Controle de Acesso;
  - Qualidade da Equipe (treinamento);
  - Dispositivos de Armazenamento de Dados;
- Observados durante o todo o período de funcionamento:
  - Controle de Acesso;
  - Acesso aos Equipamentos;
  - Sistema de Imagens (circuito interno);
  - Detecção Prevenção e Combate de Incêndios;
  - Infra-Estrutura para Redundância;
  - Armazenamento de Dados;

- Procedimentos e Rotinas com Funcionários;
- Plano de Contingência

•

3.3 SEGURANÇA LÓGICA

A segurança lógica baseia-se em mecanismos que permitem aos gerentes controlar o acesso e o uso das informações pertencentes ao sistema. Devido ao fato de que várias pessoas usam um determinado sistema é necessário o tratamento de acessos não autorizados aos sistemas, partindo de outros computadores, cuidando do acesso a arquivos.

3.3.1 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação engloba os seguintes atributos:

1. **Disponibilidade**

   A Informação deve estar disponível sempre que necessária.

2. **Sigilo**

   Informação inteligível somente para usuários autorizados.

3. **Autenticidade**

Informação não foi alterada.

4. **Integridade**

Identificação correta da origem da informação e dos participantes.

A questão de integridade pode ser aplicada a todo um fluxo de mensagens de uma conexão, a uma única mensagem ou a determinados campos desta mensagem. Uma conexão que tenha este princípio implantado garante que as mensagens serão recebidas como foram enviadas, sem duplicação, inserção indevida, modificações, sem reordenação ou repetições.

5. **Controle de Acesso**

Somente pessoas autorizadas podem acessar determinado tipo de informação.

Habilidade de limitar ou controlar o acesso aos computadores através do controle de acesso físico ou aplicações através de senhas, por exemplo. Para tal, cada entidade que precisa obter acesso ao recurso, deve primeiramente ser identificada, ou autenticada e de forma a que os direitos e permissões de acesso sejam atribuídos ao usuário em questão.

6. **Não Repúdio**

Participantes não podem negar ação anterior, ou seja, previne tanto o emissor quanto o receptor, contra a negação de uma mensagem transmitida. Desta forma, quando uma mensagem é enviada, o receptor pode provar que de fato a mensagem foi enviada pelo emissor em questão. De forma similar, quando uma mensagem é recebida, o emissor pode provar que a mensagem foi realmente recebida pelo receptor em questão.

4 SEGURANÇA EM BANCO DE DADOS

4.1 INTRODUÇÃO

Segundo [Date, 2000], segurança de banco de dados se refere à proteção de dados contra revelação, alteração ou destruição não autorizadas.

Em se tratando de segurança em banco de dados, atualmente existem duas abordagens conhecidas como controle discricionário e mandatário. Os aspectos de cada abordagem são indicados a seguir:

- No controle discricionário, um usuário terá direitos de acesso (privilégios) diferentes sobre dados diferentes, incluindo a capacidade de acessar arquivos específicos de

dados, campos específicos de uma tabela ou mesmo poder utilizar determinadas operações sobre a base de dados (ler, inserir, excluir, alterar, atualizar). O controle discricionário é muito flexível, pois, por exemplo, um usuário U1 pode acessar a tabela T1, mas não pode ter acesso a T2, já o usuário U2 pode acessar as tabelas T1 e T2.

- No controle mandatário, os usuários e os dados são classificados em vários níveis de segurança, de acordo com a política de segurança da empresa. Um determinado usuário somente terá acesso aos dados que estiverem no mesmo nível de segurança ao qual lhe foi concebido. Por exemplo, imaginamos a seguinte situação: se um determinado usuário U1 possui nível de segurança N1 e o usuário U2 possui nível N2, sendo que os dados D1 e D3 possui nível N1 e os dados D2 e D4 possui nível N2. Com base no exemplo acima o usuário U1 terá acesso aos dados D1 e D3, enquanto o usuário U2 terá acesso somente aos dados D2 e D4.

4.1.1 SEGURANÇA DE DADOS

Sabendo que o administrador de banco de dados (DBA) é a autoridade central no sentido de gerenciar o banco de dados, é de sua responsabilidade conceder aos usuários privilégios para que possam manipular o banco de dados e classificar os dados de acordo com a política da empresa. O DBA possui uma conta chamada “ conta administrador” na qual permite direitos ao DBA que uma conta de um usuário normal não possui. O DBA conta com direitos tais como conceber e revogar privilégios a usuários, a grupos de usuários e realizar as ações a seguir:

1. Criação de contas: criação de novas contas e senhas para um usuário ou grupo de usuários, a fim de permitir o acesso ao banco de dados.

2. Atribuição de privilégios: permite ao DBA a atribuição de privilégios a determinadas contas.

3. Revogação de privilégios: permite que o DBA revogue (cancele) certos privilégios previamente concebidos a determinadas contas.

4. Atribuição de níveis de segurança: esta ação consiste no poder do DBA em atribuir às contas de usuários níveis de segurança.

A segurança do sistema de banco de dados é de responsabilidade do DBA. Na lista acima o item 1 refere-se ao controle de acesso ao banco de dados, os itens 2 e 3 referem-se ao controle discricionário enquanto o item 4 refere-se ao controle mandatário.

4.1.1.1 Autorização de Acesso

A função das autorizações de acesso é permitir que apenas agentes autorizados, sejam usuários ou aplicações, realizem certas operações sobre certos dados. Para tanto, faz-se necessário manter uma matriz de autorização, que especifica, para cada agente e cada dado, a(s) operação(ões) autorizadas. Por dado entende-se alguma porção do BD, como um ou mais registros, um arquivo completo ou vários, alguns campos de um registro, etc. O mecanismo de visões permite especificar a porção do BD que um agente tem direito de acesso.

4.1.2 PROTEÇÃO DE ACESSO, CONTAS DE USUÁRIOS E AUDITORIA DE BANCO DE DADOS

Quando um usuário ou grupo de usuários precisam acessar um banco de dados, precisam ter uma conta de usuário. A criação desta conta é de responsabilidade do DBA, que juntamente com a criação da nova conta irá também atribuir a esta conta uma senha, para que o usuário possa ser reconhecido pelo sistema de banco de dados. Para que o usuário faça o “log in” do banco de dados é necessário que entre com a sua conta e senha. Caso a conta e senha fornecidas pelo usuário sejam válidas, o usuário está autorizado a ter acesso ao banco de dados, caso contrário o acesso será bloqueado até o fornecimento de uma conta e senha válidas.

Outro importante mecanismo na proteção dos dados seria a criação de logs, que a partir do momento em que o usuário faça o “log in” no sistema todas as suas ações são registradas até que o usuário faça o “log off”.

A auditoria de dados consiste em examinar os logs gerados pelo SGBD, com o propósito de rastrear as operações feitas em determinado período de tempo. Caso o DBA descubra que houve uma operação ilegal ou não autorizada, através do log é possível localizar qual usuário efetuou determinada ação.

4.2 CONTROLE DISCRICIONÁRIO

O controle discricionário de um banco de dados é baseado na atribuição e revogação de privilégios de acesso.

4.2.1 TIPOS DE PRIVILÉGIOS

O SGBD deve fornecer acesso seletivo às informações armazenadas, baseado em contas especificas. Podem também ser atribuídos privilégios em relação às operações.

Existem dois níveis para atribuir privilégios a usuários de um sistema de banco de dados.

1. Nível de conta: o DBA especifica os privilégios específicos que cada usuário possui, independente das relações no banco de dados.

2. Nível de relação (ou tabela): é controlado o acesso a cada relação ou visão individual no banco de dados.

Privilégios do nível de conta não estão definidos como parte do SQL2, estes devem ser definidos pelos implementadores do SGDB.

Privilégios do nível de relação já estão definidos pela SQL2. A concessão e revogação de privilégios utilizam-se de um modelo chamado modelo de matriz de acesso, onde as linhas da matriz M representam sujeitos (usuários, contas e programas) e as colunas representam objetos (relações, visões, colunas, operações). Cada posição M(i, j) na matriz

representa os tipos de privilégios (ler, gravar, atualizar) que o sujeito i possui em relação ao objeto j.

Para controlar a concessão e revogação de privilégios de relações, é designada a cada relação R em um banco de dados uma conta do proprietário (owner), onde geralmente a conta do proprietário é a conta que foi utilizada quando a relação foi criada.

Os seguintes tipos de privilégios podem ser concebidos na SQL em relação a cada relação individual R.

- Privilégio SELECT (recuperação ou leitura) na relação R: dá à conta o privilégio de ser recuperada.
- Privilégio MODIFY na relação R: dá à conta a capacidade de modificar tuplas de R.
- Privilégio REFERENCES na relação R: dá à conta a capacidade de referenciar a relação R ao especificar restrições de integridade. Esse privilégio também pode ser restrito a atributos específicos de R.

4.2.2 ESPECIFICAÇÃO DE PRIVILÉGIOS UTILIZANDO VISÕES

Visões são utilizadas como importante mecanismo para a concessão de autorização. Por exemplo, se um proprietário (owner) A de uma relação R deseja que uma conta B seja capaz de recuperar somente alguns campos de R, então A pode criar uma visão V de R, onde serão incluídos somente os atributos que B pode visualizar.

4.3 VISÕES

4.3.1 INTRODUÇÃO

Segundo [Date, 2000], uma visão é essencialmente uma expressão nomeada da álgebra relacional (ou algo equivalente à álgebra relacional). Por exemplo:

```
VAR BOM_FORNECEDOR VIEW
      (F WHERE STATUS > 15)  {F#, STATUS, CIDADE}
```

Quando essa instrução é executada, a expressão não é avaliada, mas apenas "lembrada" pelo sistema – na verdade cria-se um catálogo nomeado BOM_FORNECEDOR. Para o usuário é como se houvesse uma variável de relação chamada BOM_FORNECEDOR no banco de dados, contendo tuplas e atributos, ou seja, o nome BOM_FORNECEDOR é uma variável de relação derivada (virtual), cujo valor em qualquer instante é a relação que resultaria se a expressão de definição da visão fosse de fato avaliada no instante.

A figura abaixo é resultado do uso da visão Bom_Fornecedor, esta visão foi aplicada na tabela, deixando visível para o usuário apenas as partes que não estão sombreadas.

F#	FNOME	STATUS	CIDADE
F1	Carlos	20	Barbacena
F2	João	10	Rio de Janeiro
F3	Umberto	30	Belo Horizonte
F4	Tom	20	Barbacena
F5	Maria	30	Juiz de Fora

Figura 10: BOM_FORNECEDOR como visão da variável de relação básica F (partes não sombreadas).

O usuário poderá visualizar os dados que não estão sombreados.

4.3.2 PARA QUE SERVEM AS VISÕES

Algumas razões para a utilização de visões:

4.3.2.1 As visões fornecem segurança automática para dados ocultos

A expressão “dados ocultos” se refere aos dados não visíveis através de uma determinada visão (por exemplo, nomes de fornecedores, no caso da visão BOM_FORNECEDOR). Esses dados estão realmente seguros quanto ao acesso (pelo menos ao acesso de busca) através dessa visão particular. O uso de visões para o acesso de um banco de dados é um mecanismo simples, mas eficiente em se tratando de segurança.

4.3.2.2 As visões permitem que os mesmos dados sejam vistos por usuários diferentes de modos diferentes ao mesmo tempo

As visões permitem que os usuários tenham acesso somente a uma parte do banco de dados que lhes interessa e ignorem o restante. Essa consideração é importante quando há muitos usuários diferentes, com muitas exigências diferentes, todos interagindo ao mesmo tempo com um único banco de dados integrado, ou até mesmo por questões de segurança, ou seja, um determinado usuário não pode acessar determinados dados, somente parte deles.

Uma visão pode esconder dados do usuário que ele não precisa (ou não pode) ver. Com o uso de visões será um meio para que o administrador possa projetar um banco de dados personalizado, geralmente definindo níveis de usuários:

Exemplo:

- Administrador do Banco de Dados (DBA);
- Gerente;
- Programador;

- Pessoal de apoio.

4.3.3 VISÕES EM SQL

4.3.3.1 Conceito de Visões em SQL

Uma visão em SQL é uma tabela derivada de outras tabelas. Estas outras tabelas podem ser tabelas do próprio banco de dados, ou visões previamente definidas. Uma visão não necessariamente precisa existir fisicamente, ou seja, uma visão é considerada uma tabela virtual, diferentemente das tabelas do banco de dados, nas quais as tuplas estão armazenadas no banco de dados.

4.3.3.2 Especificando Visões em SQL

Em SQL, o comando usado para a criação de visões é o CREATE VIEW. A visões possui um nome, uma lista de atributos, e uma consulta para especificar o conteúdo da visão. Abaixo segue o exemplo da criação de duas visões:

EMPLOYEE

FNAME	MINIT	LNAME	SSN	BDATE	ADDRESS	SEX	SALARY	SUPERSSN	DNO

DEPARTMENT

DNAME	DNUMBER	MGRSSN	MGRSTARTDATE

DEPT_LOCATIONS

DNUMBER	DLOCATION

PROJECT

PNAME	PNUMBER	PLOCATION	DNUM

WORKS_ON

ESSN	PNO	HOURS

DEPENDENT

```
V1:   CREATE VIEW    WORKS_ON1
      AS    SELECT   FNAME, LNAME, PNAME, HOURS
            FROM     EMPLOYEE, PROJECT, WORKS_ON
            WHERE    SSN=ESSN AND PNO=PNUMBER;

V2:   CREATE VIEW    DEPT_INFO (DEPT_NAME, NO_OF_EMPS, TOTAL_SAL)
      AS    SELECT   DNAME, COUNT(*), SUM(SALARY)
            FROM     DEPARTMENT, EMPLOYEE
            WHERE    DNUMBER=DNO
            GROUPBY  DNAME;
```

WORKS_ON1

FNAME	LNAME	PNAME	HOURS

DEPT_INFO

DEPT_NAME	NO_OF_EMPS	TOTAL_SAL

Figura 11: V1 e V2, especificadas no esquema acima.

5 APLICAÇÃO DE VISÕES – ESTUDO DE CASO

5.1 INTRODUÇÃO

Abaixo será apresentado alguns conceitos relacionados à utilização de um banco de dados em empresas:

- **O que é uma empresa?**

Segundo [Hackathorn, 1993] uma empresa é um grupo de pessoas que estão motivadas por objetivos comuns e utilizam recursos comuns para atingir estes objetivos.

- **O que é uma aplicação empresarial?**

Segundo [Hackathorn, 1993] uma aplicação é um conjunto de programas que suportam funções especificas do negocio.

- **O que é um banco de dados empresarial?**

Segundo [Hackathorn, 1993] um banco de dados empresarial é composto dos dados formais da empresa que residem em um sistema de gerenciamento de banco de dados, em alguma plataforma no interior do sistema de informação.

5.2 A EMPRESA

A rede FHEMIG está a 25 anos oferecendo serviços especializados nas áreas de urgência e emergência, psiquiatria, reabilitação física, toxicomania, doenças infecto-parasitárias, entre outras, e suas unidades são referência no Estado de Minas Gerais em diversos tipos de atendimento, como o de trauma e queimados. Tem 2.798 leitos operacionais, 110 de CTI.

Durante seus 25 anos, a Rede FHEMIG vem investindo no servidor, em projetos para todas as áreas e, principalmente, no atendimento ao usuário. O número de consultas médicas é da ordem de 1,2 milhões ao ano; os exames passaram de 125 mil para mais de 2,5 milhões e o número de cirurgias, que era de cerca de 2.600 ao ano, chegou a 25 mil. A Fundação já realizou cerca de 14 milhões de consultas médicas, mais de 19 milhões de exames, aproximadamente 308 mil cirurgias e mais de um milhão de internações.

5.3 UNIDADES

A rede FHEMIG conta com 22 unidades, sendo 14 em Belo Horizonte, e oito no interior do estado, contando com sedes em Juiz de Fora, Patos de Minas, Ubá, Barbacena, Betim, Sabará, Três corações e Bambuí.

5.3.1 CENTRO HOSPITALAR PSIQUIÁTRICO DE BARBACENA (CHPB)

Após um longo período de barbaridades e violências no tratamento dos “loucos”, CHPB passou por um profundo processo de humanização e ostenta hoje a classificação de Psiquiatria IV, o maior grau em saúde mental, do Ministério da Saúde. Hoje os pacientes do CHPB conta com modernos e humanos métodos e terapias de dignidade. Os internos produzem arte como terapia ocupacional e não existem mais internações definitivas.

5.3.1.1 Estrutura

O CHPB conta com uma área construída de 35 mil metros quadrados, contando com 494 leitos, sendo 426 asiliares, 32 agudos e 36 de enfermaria de intercorrências clínicas. A estrutura do CHPB se compara à de pequenas cidades do interior. O serviço de nutrição e dietética ocupa uma área de 800 m², produzindo diariamente duas mil refeições, com distribuição de mais de três mil pães e cerca de 400 litros de leite. Tem também uma marcenaria e serralheria que fabricam portas, marcos, janelas e mobiliário em geral. Com material moderno e sistema especial de desinfecção, a lavanderia lava e passa, por dia, mais de uma tonelada de roupas de cama, mesa e uso pessoal.

Os usuários participam de diversas atividades, onde a arte, a cultura e o relacionamento interpessoal são os principais instrumentos terapêuticos.

É no cenário desta empresa que o projeto de implementação de Visões em Banco de Dados será desenvolvido. As informações serão colhidas in loco e junto ao Serviço de Apuração de Custos da Rede FHEMIG, para serem inseridas no banco de dados proposto.

5.4 MODELAGEM DO SISTEMA

O cenário onde será aplicado o estudo de caso existe um sistema de estatística que utiliza as informações oriundas das bases transacionais de atendimentos aos clientes onde são feitas as entradas de dados a partir das tabelas:

Tabela	Descrição
ATENDIMENTO	Atendimentos prestados aos clientes, incluindo ambulatoriais e internações
INTERNAÇÃO	Especialização de Atendimentos
LEITO	Leitos do hospital
CENTRO DE CUSTO	Setores ou unidades de atendimento do hospital
CONVÊNIO	Planos de saúde de clientes
ESTATÍSTICA	Tabela principal da estatística

Tabela 1 Tabelas do sistema de estatística hospitalar.

No sistema de estatística, existe uma tabela de lançamentos de internações, transferências e altas de pacientes, de acordo com informações provenientes da base de dados de internações. Esta tabela está relacionada com os convênios (planos de saúde) e leitos que estão localizados nas unidades de internação, pode-se associar este modelo ao esquema estrela, onde há uma tabela de fatos com as dimensões de convênio, leito, unidade de internação.

A cada mês são emitidos os relatórios da estatística hospitalar, os quais contêm os dados relativos às internações realizadas naquele período. O sistema constrói uma grade que contém nas linhas os convênios e nas colunas o número total de internações, o número de pacientes-dia, o percentual de ocupação e o coeficiente de mortalidade.

Esta grade é baseada nas centenas de registros que são transferidos ao final do mês para esta base de dados e que são posteriormente sumarizados por convênio e unidade de internação.

A variável paciente-dia indica o número de dias em que os leitos estiveram ocupados por pacientes. Outra variável utilizada na estatística é chamada leito-dia, a qual indica o número de leitos disponíveis para internação durante um período determinado.

Em anexo B – Modelo entidades-relacionamentos da base de dados do CHPB Para melhor entendimento das tabelas e relacionamentos existentes no banco de dados existente na unidade CHPB,

5.5 IDENTIFICANDO AS ORIGENS DOS DADOS

O sistema transacional que está em uso no hospital foi desenvolvido em Data Flex para Unix, mais precisamente em um ambiente AIX versão 4. Neste sistema existe diversas tabelas relacionadas entre si e que servem basicamente para armazenar os dados relativos às internações dos pacientes nos leitos, solicitadas pelos médicos ao hospital. Quando um paciente é internado, o sistema gera um atendimento no dia e na hora do cadastro, sendo que o paciente pode estar cadastrado em um plano de saúde ou não possuir nenhum plano, passando a ser considerado como paciente particular. A diferença básica entre os convênios é que o hospital irá cobrar as despesas do plano de saúde a que pertence o cliente ou irá cobrar os valores diretamente do paciente considerado particular.

No caso do sistema transacional utilizado neste estudo de caso, os gastos dos pacientes estão divididos em dois grandes grupos: o grupo dos serviços e o grupo dos produtos, incluindo estes últimos os materiais e os medicamentos.

No grupo dos serviços estão incluídas as taxas, como as diárias, e os honorários dos profissionais que trabalham no hospital.

No grupo dos produtos estão os materiais: as seringas, as agulhas, as gazes, os esparadrapos, entre outros, além dos medicamentos, como os comprimidos, os ampolados, etc.

Cada paciente internado possui uma conta onde são debitados os gastos relativos aos cuidados que recebe dentro do hospital. A qualquer momento pode-se emitir um extrato de débitos chamado "nota de gastos", o qual contém todos os valores devidos pelo paciente ao hospital, separados por unidade de internação (centros de custo) e por grupo.

A divisão por grupos possui seguintes itens:

Grupo	Descrição resumida
DIÁRIAS	Corresponde ao número de dias em que o paciente esteve internado no hospital multiplicado pelo valor da diária pago pelo plano de saúde ou pelo próprio paciente
MEDICAMENTOS	Gastos com medicamentos em geral
MATERIAIS	Gastos com materiais utilizados para aplicar os medicamentos
EXAMES	Gastos com exames radiológicos, laboratoriais e outros
OUTROS SERVIÇOS	Serviços extraordinários..

Tabela 2: Grupos de gastos de pacientes.

5.6 DEFININDO O NÍVEL DE DETALHE (GRANULARIDADE) DA BASE DE DADOS

Se a granularidade for muito alta, a performance do sistema pode cair a níveis inaceitáveis por possuir um número muito grande de registros armazenados. Pelo contrário, caso a granularidade seja muito baixa os dados estarão muito resumidos que praticamente não restará nada para o usuário fazer em termos agregações, por exemplo.

Neste estudo de caso, a granularidade ao nível de lançamentos de gastos nas contas dos pacientes, os lançamentos de gastos foram agrupados por atendimento.

A seguir serão expostas três alternativas de granularidade possíveis para estudo:

5.6.1 GRANULARIDADE A NÍVEL DE LANÇAMENTOS DOS GASTOS

Cada paciente possui uma conta onde são gravados os seus gastos, conforme foi descrito anteriormente, e para que isto seja possível são necessárias algumas tabelas relacionadas representadas na figura abaixo:

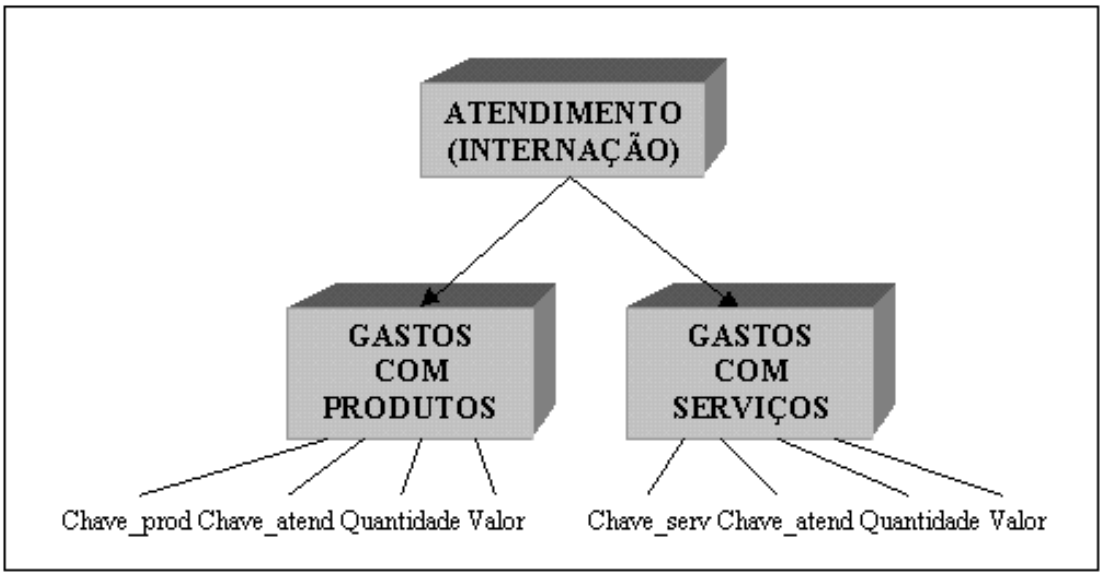


Figura 12: Granularidade a nível de lançamentos dos gastos.

Como se pode notar, existem dois tipos de gastos: com produtos e com serviços. Embora exista a distinção entre produtos e serviços, no modelo ER os gastos do paciente não importa, sendo utilizado apenas o código de relacionamento com a tabela correspondente, a quantidade e o valor unitário deste serviço.

O agrupamento pode ser feito de acordo com abaixo:

Campo	Descrição

Chave_prod	Relacionamento com a tabela de produtos
Chave_atend	Relacionamento com a tabela de atendimentos a pacientes
Chave_serv	Relacionamento com a tabela de serviços
Quantidade	Quantidade de produtos ou número de diárias ou de incidências de serviços realizados
Valor	Valor unitário do produto ou do serviço

Tabela 3: Campos utilizados no modelo estrela.

5.6.2 GRANULARIDADE A NÍVEL DE LANÇAMENTOS AGRUPADOS POR CÓDIGO CONTÁBIL

Um determinado grupo de serviços pode ser representado pelo seu código contábil, o qual representa uma conta do Plano de Contas do setor financeiro. Com isto definido, podemos representar os gastos dos pacientes por estes códigos, o que reduz sensivelmente o número de lançamentos, na proporção de até cinco para um, ou mais, em alguns casos. Caso fosse feito um agrupamento por código contábil, a estrutura ficaria da seguinte forma para os gastos de clientes:

Antes				**Depois**		
Serviço	Quantidade	Valor Total		Código Contábil	Quantidade	Valor Total
15483	5	R$ 250,00		848	15	R$ 1.065,10
9872	6	R$ 800,00				
92873	4	R$ 15,10				

Tabela 4: Antes e depois do agrupamento por código contábil.

Desta maneira, os gastos que antes seriam lançados um a um seriam agrupados por seus respectivos códigos contábeis, caso todos os gastos de serviços da tabela da esquerda fossem do mesmo código contábil.

5.6.3 GRANULARIDADE A NÍVEL DE ATENDIMENTOS

Esta foi a opção escolhida neste estudo de caso, sendo que a tabela 5 ficaria ainda mais reduzida, uma vez que um mesmo atendimento do paciente pode ser resumido em apenas duas medidas, o total de produtos e o total de serviços, expressos em reais.

5.7 IDENTIFICANDO AS DIMENSÕES

Existem oito dimensões definidas (médico, leito, funcionário, convênio, cidade-do-cliente, sexo-do-cliente, estado-civil-do-cliente e tempo).

As dimensões que foram criadas a partir das tabelas físicas originais são: clicidades, clisexo e cliestadocivil. Na verdade foram feitas configurações na tabela de dimensão de cliente para que fosse possível visualizar os dados de forma a se ter agregações por cidade, sexo e estado civil.

5.8 DEFININDO OS NÍVEIS DE AGREGAÇÃO DAS DIMENSÕES

Algumas tabelas são constituídas de níveis de agregação, ou hierarquias de atributos que estão relacionados com a tabela de fatos na forma de muitos-para-um.

Na figura 10, está um exemplo da tabela de dimensão de tempo que possui algum nível de agregação.O tempo foi dividido inicialmente em anos, os anos em trimestres, os trimestres em meses e finalmente os meses em datas, ou seja, em dias. Desta maneira existe a possibilidade de se realizar operações de "*drill-down*", ou seja, detalhar os dados até que

sejam mostrados os dias, bem como realizar operações de "*roll-up*", que significa sumarizar os dados de um ano inteiro numa grade.

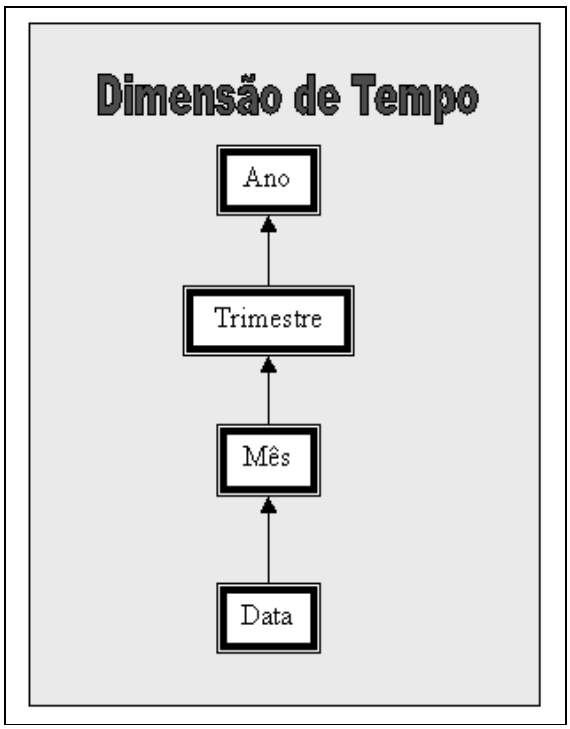


Figura 13: Níveis de agregação da dimensão de tempo.

Neste estudo de caso foram feitas diversas agregações em dimensões, como segue:

Dimensão	*Campos*
Médico	Especialidade æ Nome do Médico
Leitos	Centro de Custo (Unidade ou Setor) æ Número do Leito

Funcionário	Centro de Custo (Unidade ou Setor) æ Nome do Funcionário
Convênios	Categoria æ Descrição do Convênio
Clientes – Cidades	Estado (Unidade da Federação) æ Cidade æ Nome do Cliente
Clientes – Sexo	Sexo (M=Masculino ou F=Feminino) æ Nome do Cliente
Clientes – Estado Civil	Estado Civil (S=Solteiro,C=Casado,D=Divorc.,V=Viúvo,O=Outros) æ Nome do Cliente
Tempo	Ano (Número com quatro dígitos) æ Trimestre do Ano (de 1 a 4) æ Mês do Ano (de 1 a 12) æ Data (Dia no formato dd/mm/aaaa)

Tabela 5: Agregações utilizadas no estudo de caso.

5.9 DEFININDO AS MEDIDAS NUMÉRICAS

As medidas numéricas são definidas em função dos valores que se deseja exibir, compondo normalmente a parte interna da tabela que é dividida em linhas e colunas. No estudo em questão foram definidas diversas medidas, como segue:

- Tot dias – número total de dias em que o paciente permaneceu internado durante todo o atendimento, sendo que nenhum paciente pode ficar menos de um dia internado;

- Tot serv – valor total dos gastos com serviços, entre diárias e serviços prestados pelos funcionários do hospital, expresso em reais;
- Tot prod - valor total dos gastos com produtos, medicamentos e materiais, expresso em reais;
- Tot nfisc – valor total da nota fiscal emitida pela conta do paciente ao final da internação, expresso em reais, sendo que a nota de gastos pode ter um valor superior ao da nota fiscal, em virtude da concessão de descontos;
- Tot grat – valor total recebido pelo paciente em gratuidades, ou seja, valores que não são pagos pelo paciente ao hospital, expresso em reais;
- Tot desc – valor total recebido pelo paciente a respeito de descontos de valores, expresso em reais;
- Tot nota – valor total da nota de gastos do paciente, sendo igual ao valor de serviços acrescido do valor de produtos, expresso em reais. Nem sempre o valor da nota de gastos será totalmente cobrado do paciente, ficando a cardo dos funcionários responsáveis pela negociação a concessão ou não de descontos.

5.10 DEFININDO OS MEMBROS CALCULADOS

Os membros calculados possuem características semelhantes às das medidas, uma vez que são derivados destas medidas, como segue:

- Valor Arrecadado Diário – é executada a fórmula valor total da nota dividido pelo número total de dias de internação, expresso em reais;
- Valor Arrecadado com Serviços Diário – é executada a fórmula valor total do atendimento gasto com serviços dividido pelo número total de dias de internação, expresso em reais;

- Valor Arrecadado com Produtos Diário – é executada a fórmula valor total do atendimento gasto com produtos dividido pelo número total de dias de internação, expresso em reais;
- Média Diária da Nota Fiscal – é executada a fórmula valor total da nota fiscal dividido pelo número total de dias da internação;
- Média Diária de Gastos com Produtos – é executada a fórmula valor total de gastos com produtos dividido pelo número total de dias da internação;
- Média Diária de Gastos com Serviços – é executada a fórmula valor total de gastos com serviços dividido pelo número total de dias da internação.

5.11 ESTRUTURA OAGANIZACIONAL DA EMPRESA

A figura abaixo mostra a estrutura organizacional da unidade CHPB, sendo exibido os níveis hierárquicos existentes.

Em Anexo A: Organograma (CHPB) utilizado no estudo de caso segue um organograma da unidade CHPB, localizado na cidade de Barbacena, alguns setores que não foram citados serão citados abaixo na hierarquia que será apresentada.

Hierarquia:

GOVERNO DO ESTADO

SECRETARIA ESTADUAL DE SAÚDE

FHEMIG

UNIDADES

CHPB, HPS, SSFÉ, HRJP, E OUTRAS

DIRETOR

CHEFE DE DIVISÃO ASSISTENCIAL GERÊNCIA ADMINISTRATIVA

Ligados ao Chefe de Divisão Assistencial

- Unidades Clínicas
- Unidades Psiquiátricas
- Bloco Cirúrgico
- Laboratório
- CCIH (Comissão de Controle de Infecção Hospitalar)
- Farmácia
- Central de Esterilização
- CAPS
- Ambulatório
- Porta de Entrada

Ligados à Gerência Administrativa

- Serviço de Nutrição e Dietética
- Lavanderia
- Caldeira
- Refeitórios A e B
- Manutenção
- Creche

- SPP
- Museu
- Canteiro de Obras
- Serviço de Ponto
- Portaria
- Vigilância
- Telefonia
- Serviço de Expediente
- Serviço de Compras
- Serviço de Almoxarifado
- CPL
- Serviço de Finanças
- Planejamento
- Biblioteca
- Serviço de Patrimônio

OBS: O serviço de custos está ligado ao Chefe de Divisão Assistencial e à gerencia administrativa, fornecendo relatórios para ambos.

5.12 SEGURANÇA DO SGBD

O sistema gerenciador de banco de dados utilizado pela unidade CHPB é o Microsoft Access, e serão mostradas aqui maneiras de garantir a segurança dos dados. Em anexo D – Telas, estão telas usadas, para a atribuição de questões de segurança ao banco de dados, as telas exibidas são encontradas no menu Ferramentas > Segurança.

5.12.1 O QUE É UM GRUPO DE TRABALHO DO MICROSOFT ACCESS?

Um grupo de trabalho do Microsoft Access é um grupo de usuários que compartilham dados em um ambiente multiusuários. Quando a segurança em nível de usuário está definida, os membros de um grupo de trabalho estão registrados em contas de usuário e grupo armazenadas em um arquivo de informação do grupo de trabalho do Microsoft Access. As senhas dos usuários também são armazenadas no arquivo de informação do grupo de trabalho. Essas contas de segurança podem ter, então, permissões para bancos de dados e suas tabelas, consultas, formulários, relatórios e macros. As permissões propriamente são armazenadas no banco de dados protegido.

5.12.2 CONTAS DE SEGURANÇA

A tabela abaixo apresenta as contas predefinidas:

Conta	Função
Administrador	A conta de usuário padrão. Essa conta é exatamente a mesma para todas as cópias do Microsoft Access e outros aplicativos que possam utilizar o mecanismo do banco de dados Microsoft Jet, tal como o Microsoft Visual Basic for Applications e o Microsoft Excel.
Administradores	A conta de grupo do administrador. Essa conta é exclusiva para cada

	arquivo de informação do grupo de trabalho. Por padrão, o usuário Administrador está no grupo Administradores. Deve haver pelo menos um usuário no grupo Administradores a qualquer momento.
Usuários	A conta de grupo que abrange todas as contas de usuário. O Microsoft Access adiciona automaticamente contas de usuário ao grupo Usuários quando um membro do grupo Administradores as cria. Essa conta é a mesma para qualquer arquivo de informação do grupo de trabalho, mas contém somente contas de usuário criadas por membros do grupo Administradores desse grupo de trabalho. Por padrão, essa conta possui permissões totais sobre todos os objetos recém-criados. A única maneira de remover uma conta de usuário do grupo Usuários é pela exclusão desse usuário realizada por um membro do grupo Administradores.

Tabela 6: Contas predefinidas

Administradores e proprietários são importantes porque têm permissões que não podem ser retiradas:

- Administradores (membros do grupo Administradores) sempre podem obter permissões totais para objetos criados no grupo de trabalho.
- Uma conta que tem uma tabela, uma consulta, um formulário, um relatório ou uma macro sempre pode conseguir permissões totais para esse objeto.
- Uma conta que tem um banco de dados sempre pode abrir esse banco de dados.

Como a conta de usuário Administrador é exatamente a mesma para todas as cópias do Microsoft Access, os primeiros passos para proteger o banco de dados são definir as contas de usuário do administrador e do proprietário (ou utilizar uma única conta de usuário como conta de administrador e proprietário) e, em seguida, remover a conta de usuário Administrador do grupo Administradores.

5.12.3 PERMISSÕES

5.12.3.1 Tipos de permissões

A tabela a seguir resume as permissões que podem ser atribuídas:

Permissão	Permite ao usuário	Aplica-se a
Abrir/Executar	Abrir um banco de dados, formulário ou relatório, ou executar uma macro.	Bancos de dados, formulários, relatórios e macros
Abrir Exclusivo	Abrir um banco de dados com acesso exclusivo.	Bancos de dados
Ler Estrutura	Visualizar objetos no Modo estrutura	Tabelas, consultas, formulários, relatórios e macros
Modificar Estrutura	Visualizar e alterar a estrutura de objetos ou excluí-los.	Tabelas, consultas, formulários, relatórios e macros
Administrador	Para banco de dados, definir senhas de banco de dados, replicar um banco de dados e alterar propriedades de inicialização. Para tabelas, consultas, formulários, relatórios e macros, ter pleno acesso a esses objetos e dados, incluindo a possibilidade de atribuir permissões.	Bancos de dados, tabelas, consultas, formulários, relatórios e macros
Ler Dados	Visualizar dados.	Tabelas e consultas
Atualizar Dados	Visualizar e modificar mas não inserir ou excluir dados.	Tabelas e consultas
Inserir Dados	Visualizar e inserir mas não modificar ou excluir dados.	Tabelas e consultas
Excluir Dados	Visualizar e excluir mas não modificar ou inserir dados.	Tabelas e consultas

Tabela 7: Permissões que podem ser atribuídas

5.12.3.2 Funcionamento e atribuição das permissões

Há dois tipos de permissões: explícitas e implícitas. Permissões explícitas são aquelas concedidas diretamente a uma conta de usuário; nenhum outro usuário é afetado.

Permissões implícitas são aquelas concedidas a uma conta de grupo. Adicionar um usuário ao grupo concede a esse usuário as permissões do grupo; sua remoção retira as permissões de grupo desse usuário.

Quando um usuário tenta efetuar uma operação em um objeto de banco de dados protegido, o conjunto de permissões desse usuário é baseado na interseção das suas permissões explícitas e implícitas. O nível de segurança de um usuário é sempre a menos restritiva das permissões explícitas desse usuário e das permissões de todo e qualquer grupo ao qual o usuário pertença. Por essa razão, a maneira mais fácil de administrar um grupo de trabalho é criar novos grupos e atribuir permissões a eles, e não a usuários individualmente. Se for preciso conceder novas permissões, estas podem ser concedidas para todos os membros de um grupo em uma única operação.

Permissões para um objeto de banco de dados podem ser alteradas por:

- Membros do grupo Administradores.
- O proprietário do objeto.
- Qualquer usuário que possuir permissão de Administrador para o objeto.

O usuário que cria uma tabela, uma consulta, um formulário, um relatório ou uma macro é o proprietário desse objeto. O mesmo grupo de usuários que pode alterar permissões, também pode alterar a posse desses objetos utilizando o comando Permissões para usuário e grupo, no submenu Segurança (menu Ferramentas), ou pode recriar esses objetos.

5.12.4 PROTEGENDO UM ARQUIVO DE BANCO DE DADOS DO MICROSOFT ACCESS

O método mais simples de proteção é definir uma senha para abrir um banco de dados do Microsoft Access (.mdb). Uma vez definida uma senha, uma caixa de diálogo solicitando a senha será exibida sempre que o banco de dados for aberto. Somente os usuários que digitarem a senha correta poderão abrir o banco de dados. Esse método é seguro, porém

só se aplica à abertura de um banco de dados. Uma vez aberto o banco de dados, todos os seus objetos estarão disponíveis para o usuário (a menos que outros tipos de segurança já tenham sido definidas).

5.12.5 PROTEGENDO OBJETOS DE BANCO DE DADOS COM SEGURANÇA EM NÍVEL DE USUÁRIO

O método mais flexível e completo de proteger um banco de dados é denominado segurança em nível de usuário. Essa forma de segurança é semelhante aos métodos utilizados na maioria dos sistemas de rede. As duas principais razões para usar a segurança em nível de usuário são:

- Impedir que os usuários interrompam inadvertidamente um aplicativo alterando tabelas, consultas, formulários, relatórios e macros dos quais o aplicativo dependa.

- Proteger dados sigilosos do banco de dados.

Na segurança em nível de usuário, os usuários têm que se identificar através de uma chave e digitar uma senha quando iniciar o Microsoft Access. Dentro do arquivo de informação do grupo de trabalho, eles são identificados como membros de um grupo. O Microsoft Access fornece dois grupos padrão: administradores (chamado de grupo Administradores) e usuários (chamado de grupo Usuários), mas podem ser definidos grupos adicionais.

Após executar o Assistente de segurança em nível de usuário, pode ser atribuído ou removido permissões para contas de usuários e de grupos em seu grupo de trabalho para um banco de dados e suas tabelas, formulários, relatórios e macros existentes.

São concedidas permissões a grupos e a usuários para regular o modo pelo qual eles poderão trabalhar com cada tabela, consulta, formulário, relatório e macro em um banco de dados. Por exemplo, os membros do grupo Usuários podem ter permissão para visualizar, inserir ou modificar dados em uma tabela Clientes, mas não para alterar a estrutura dessa

tabela. Embora o grupo Usuários possa ter permissão somente para visualizar dados em uma tabela que contenha dados de pedidos, pode não ter qualquer acesso a uma tabela Folha de Pagamento. Os membros do grupo Administradores têm permissões totais sobre todas as tabelas, consultas, formulários, relatórios e macros de um banco de dados.

As permissões típicas do grupo Usuários podem incluir Ler dados e Atualizar dados em tabelas e consultas e Abrir/executar para formulários e relatórios.

Se houver a necessidade de um controle mais rígido de diferentes grupos de usuários, podem ser criados grupos próprios, atribuindo diferentes conjuntos de permissões para esses grupos e adicionar usuários aos grupos apropriados.

5.12.6 SEGURANÇA EM UM AMBIENTE MULTIUSUÁRIO

Em muitas situações, é necessário impedir que os usuários façam replicação do banco de dados. Replicar um banco de dados permite que um usuário faça uma cópia de um banco de dados compartilhado e também adicione campos e faça outras alterações no banco de dados atual. Deve ser impedido também que os usuários definam uma senha para o banco de dados. Se um usuário definir uma senha de banco de dados para um banco de dados compartilhado, nenhum outro usuário poderá abrir o banco de dados sem fornecer a senha. Se um banco de dados compartilhado não possuir segurança em nível de usuário definida, não será possível impedir que um usuário faça tais alterações. Executar o Assistente de segurança em nível de usuário em um banco de dados define a segurança em nível de usuário, a qual permite o controle de acesso a certos recursos e determinar como os objetos de banco de dados poderão ser usados. Quando a segurança em nível de usuário está definida, um usuário ou grupo deve possuir permissão de administrador no banco de dados para replicá-lo, definir uma senha de banco de dados ou alterar as propriedades de inicialização. Após executar o Assistente de segurança em nível de usuário, somente membros do grupo Administradores do grupo de trabalho atual têm permissão de administrador.

Se a segurança em nível de usuário já estiver definida e um usuário ou grupo possuir permissão de administrador em um banco de dados, remover essa permissão impedirá que o usuário ou grupo faça tais alterações.

5.12.7 UTILIZANDO INSTRUÇÕES SQL

A maneira mais fácil de se construir uma instrução SQL é criar uma consulta na grade de estrutura da consulta, alternar para o modo SQL e copiar e colar a instrução SQL correspondente no seu código.

O exemplo a seguir mostra como criar um objeto QueryDef com uma instrução SQL simples. Esta consulta retorna todos os pedidos de uma tabela Pedidos que foram feitos após 31-3-96:

```
Dim dbs As Database, qdf As QueryDef, strSQL As String

Set dbs = CurrentDb

strSQL = "SELECT * FROM Pedidos WHERE DataDoPedido >#3-31-96#;"

Set qdf = dbs.CreateQueryDef("SegundoTrimestre", strSQL)
```

5.13 PROTÓTIPO E O USO DE QUESTÕES DE SEGURANÇA NO ESTUDO DE CASO

Em toda organização existem níveis hierárquicos, como o citado na seção 5.11, o uso de visões está presente justamente para cuidar dos dados que cada nível terá acesso, por

exemplo, o Chefe de divisão assistencial pode ter acesso aos dados do laboratório e da farmácia, dentre outros e o pessoal da gerência administrativa tem acesso aos dados do Serviço de Nutrição e Dietética, Lavanderia dentre outros.

Em Anexo C seguem alguns documentos (relatórios), fornecidos pela funcionária dos setor de custos do CHPB Suzana de Oliveira Nunes. A lista de produtos refere-se a todos os processos existentes no CHPB, e para ilustrar o uso de visões foi solicitado à funcionária um relatório que seria encaminhado para o chefe de divisão assistencial e outro para o pessoal da gerência administrativa. A funcionária do setor de custos é responsável por fornecer aos setores citados acima relatórios, porém cada setor tem seus relatórios específicos.

No caso exposto, a funcionária do setor de custos tem acesso à lista de produtos, a gerência administrativa solicitou um relatório que somente este setor tem acesso, que é o relatório Custo Global dos Produtos por Atividades, que está em Anexo C.Já o chefe de divisão assistencial, tem acesso ao relatório Produtos por Atividades, que no caso exposto é um relatório do custo para realizar determinado exame, que está em Anexo C, onde neste relatório consta todo o processo para realizar tal exame, desde o RH (recurso humano) usado, mensuração de material e equipamentos, estes dados são de interesse somente do chefe da divisão assistencial, não importando para o pessoal da gerência administrativa. Com este exemplo fica claro a utilidade de fazer uso de visões.

Um exemplo da aplicação de visões no sistema utilizado pela unidade CHPB é aa tela abaixo, mostrando todas as consultas disponíveis para a funcionária do setor de custos, que ao fornecer sua identificação e senha o sistema a reconhece e restringe algumas telas e funções do banco.

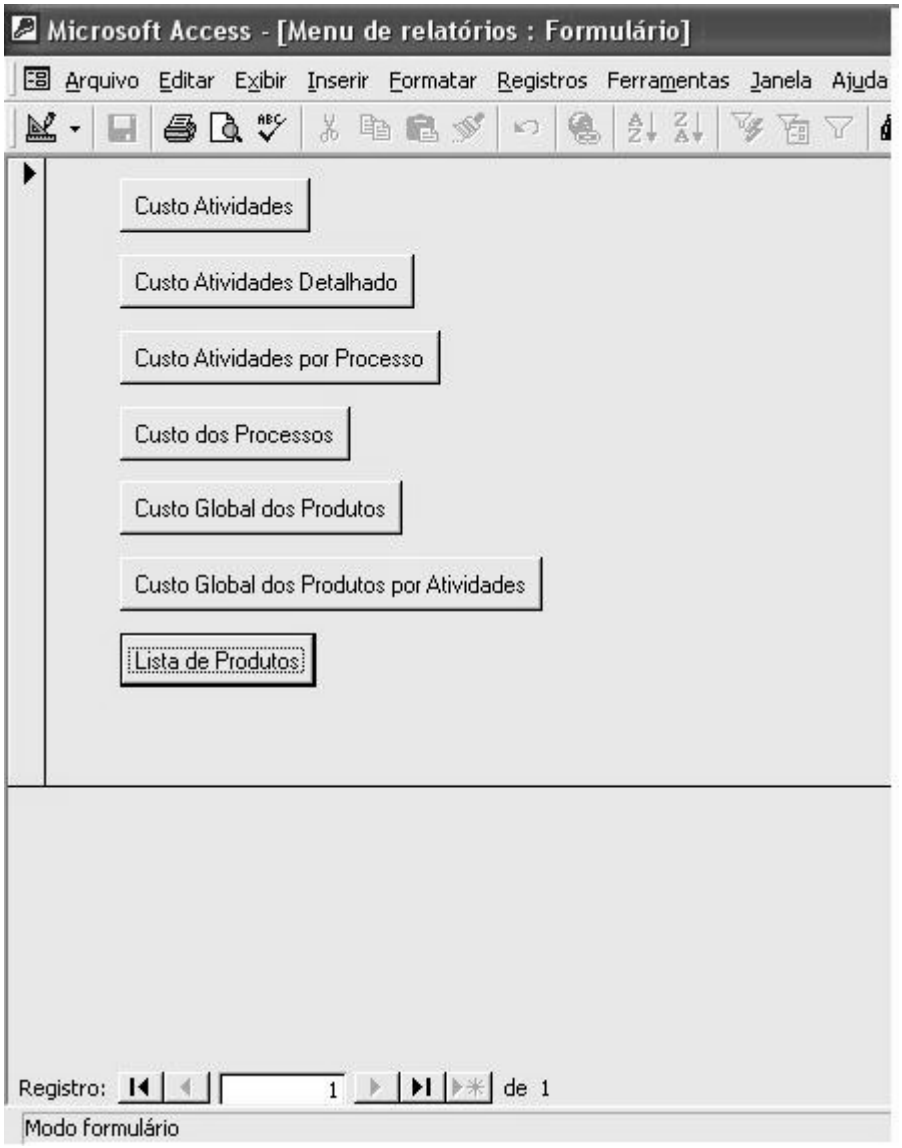


Figura 14: Opções disponíveis para a funcionária do setor de custos

A tela abaixo fornece as opções permitidas ao gerente administrativo.

As figuras 14 e 15 implicam as opções necessárias a dois funcionários da unidade do CHPB, onde cada um desses funcionários têm uma senha e uma identificação, após serem identificados pelo sistema, a funcionária do setor de custos pode usar as funções disponíveis

na figura 14 e o gerente administrativo apenas as funções disponíveis na figura 15, isto é conseguido, pois foi criado uma conta para cada funcionário e cada um deles devem exercer funções diferentes.

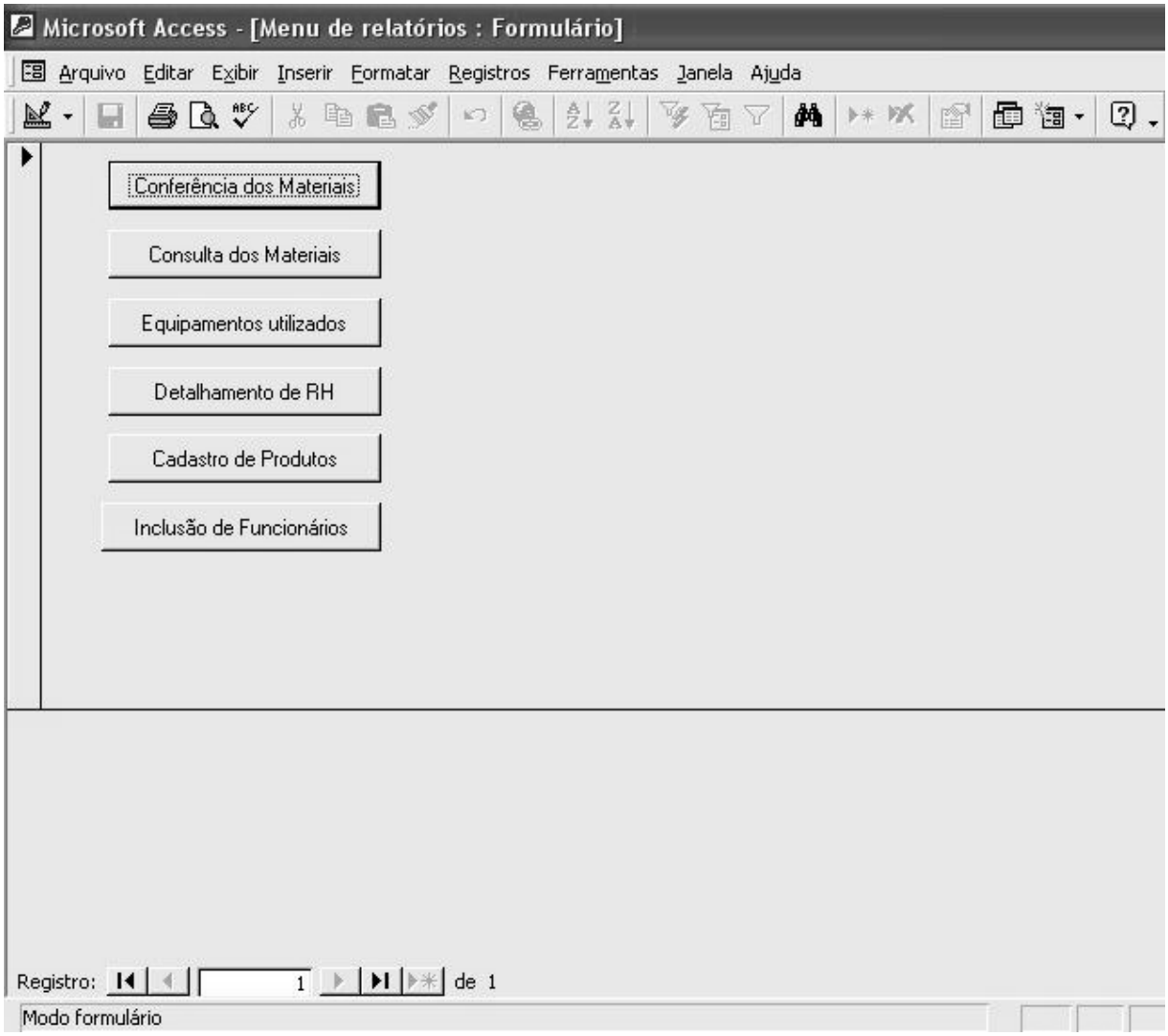


Figura 15: Opções disponíveis para gerente administrativo

A figura abaixo mostra, a solicitação de senha para que o usuário possa abrir o arquivo do banco de dados do Microsoft Access, abordado no tópico 5.12.4, onde é requisitada apenas uma senha, esta estando correta o usuário está permitido a usar o banco de dados.

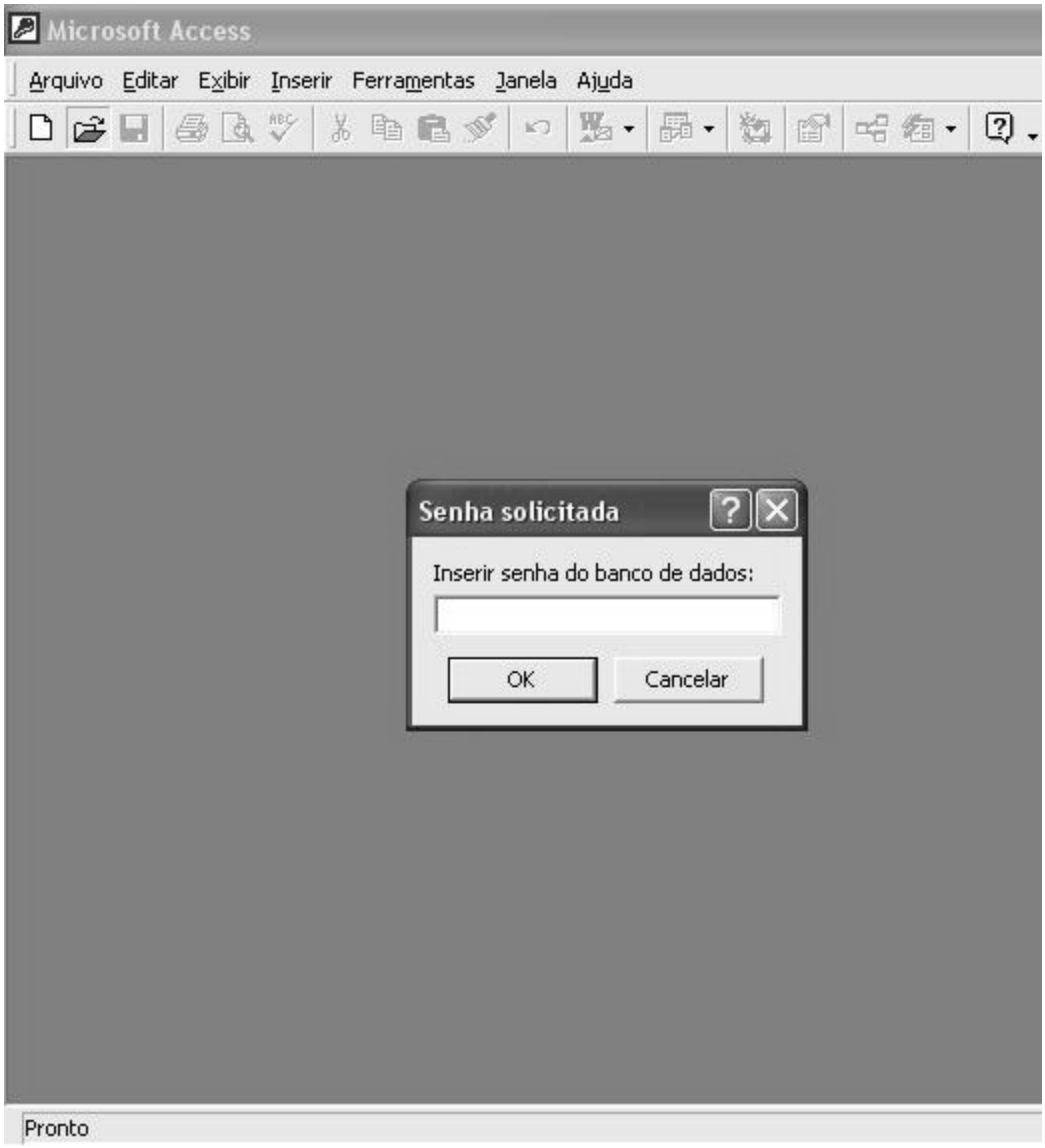


Figura 16: Tela de solicitação de senha para a abertura do arquivo do banco de dados

6 CONCLUSÃO

Atualmente devido ao grande número de informações nas empresas, elas têm utilizado sistemas de informação (SI's). SI pode ser definido como um conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar,

armazenar e distribuir informação com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo discricionário em empresas e outras organizações. Estes SI's são compostos por hardware, software, telecomunicações e banco de dados.

Este estudo deu ênfase no componente banco de dados, mais especificamente na questão de segurança de banco de dados. Como é sabido banco de dados é uma coleção de dados persistentes utilizada pelos sistemas de aplicação de determinada empresa. Segurança de banco de dados se refere à proteção de dados contra revelação, alteração ou destruição não autorizadas. Devido ao fato do sistema de banco de dados, estar disponível para que muitas pessoas tenham acesso, surgiu a preocupação da segurança dos dados, ou seja, pessoas não autorizadas poderiam acessar dados que não lhes interessavam, ou que não podiam ser acessados. Com isso surgiu a idéia de criação de contas e atribuição de privilégios, onde o DBA atribui a cada usuário um nível, nível esse que irá liberar ou bloquear o acesso a determinados dados. Juntamente com essa idéia surge também o uso de visões, a fim de garantir segurança aos dados, ou seja, as visões permitem que os usuários tenham acesso somente a uma parte do banco de dados. Essa consideração é importante quando há muitos usuários diferentes, com muitas exigências diferentes, todos interagindo ao mesmo tempo com um único banco de dados integrado, ou até mesmo por questões de segurança, ou seja, um determinado usuário não pode acessar determinados dados, somente parte deles.

Uma visão pode esconder dados do usuário que ele não precisa (ou não pode) ver. O uso de visões é um meio em que o administrador pode projetar um banco de dados personalizado, geralmente definindo níveis de usuários.

Com este estudo, fica claro a necessidade em se preocupar com a segurança dos dados, devido ao fato de que muitas empresas possuem seus movimentos em um sistema de banco de dados, podendo ter prejuízos incalculáveis se determinada pessoa, apagar ou mesmo alterar os dados. Porém a preocupação com a segurança não deve ser somente na parte lógica, mas também na parte física. A segurança física envolve medidas usadas para garantir a proteção física dos recursos contra ameaças voluntárias (roubos, invasões) e involuntárias (incêndio, acidentes).

Com o sistema já utilizado pela unidade CHPB fica claro a validade do uso de visões em um banco de dados, pois em uma organização nem todos necessitam ou podem ter acesso aos mesmos dados, um bom exemplo é a questão de que um médico da empresa utilizada no estudo, FHEMIG, não tem a necessidade de saber quantas seringas foram usadas no hospital durante o mês, para ele basta saber a ficha dos pacientes, já para o pessoal que responsável pela compra de materiais, não têm a necessidade de conhecer a ficha de cada paciente, para eles bastam apenas saber a quantidade de produtos gastos, para que possam efetuar a compra. Com este exemplo fica claro como as visões seriam úteis no bloqueio de algumas informações. Outra questão de segurança vista no estudo foi a de atribuição de contas aos usuários para que eles tenham disponíveis apenas as funções necessárias para a função exercida.

REFERÊNCIAS BIBLIOGRÁFICAS

DATE, C. J. **Introdução a Sistemas de Banco de Dados**; tradução[da 7. ed. Americana]. Rio de Janeiro: Campus, 2000.

LAUDON, Kenneth C.e LAUDON, Jane Price. **Sistemas de Informação**; Rio de Janeiro, RJ, 1999.

NAVATHE, Shamkant B. e ELMASRI, Ramez. **Fundamentals of Database Systems**; 3rd ed.; Vancouver, Canadá, 2000.

HACKATHORN, Richard D. **Conectividade de banco de dados empresariais**; Rio de Janeiro, RJ, 1993.

BERNSTEIN, T. et al. **Segurança na Internet**. Rio de Janeiro: Campus, 1997. 461 p.

GIL, A. L. **Auditoria de Computadores**. 4ª ed. São Paulo: Atlas Ltda, 1999

CARUSO, C.A.A. & STEFFEN, F. D. **Segurança em Informática e de Informações**. Ed. SENAC São Paulo, 1999.

MARÂNDOLA, Cristina. **FHEMIG, 25 anos de história**. Belo Horizonte: Gráfica FHEMIG, 2002.

OLIVEIRA, Suzana Azevedo de. **O Sistema de Custeio na Rede FHEMIG**. Belo Horizonte: Gráfica FHEMIG, 2003.

SILVA, Enio K. O. **Um Estudo Sobre Sistemas De Banco De Dados Cliente/Servidor** : Monografia, 2001 - Faculdade Paraibana de Processamento de Dados João Pessoa - PB.

NUNES, Suzana de Oliveira. **Modelagem de um Data Warehouse para uma Aplicação Hospitalar** : Monografia, 2003 - Faculdade Presidente Antônio Carlos (UNIPAC) Barbacena - MG.

TELECOMUNICAÇÕES. Disponível na URL: http://www.lsi.usp.br/~telemat/aprenda/telecom/index.htm

http://www.redegoverno.gov.br/eventos/arquivos/Mod_Seg_Inf.pdf

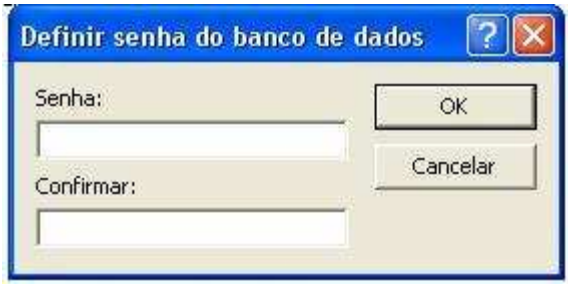
http://www.unir.br/~rissino/db1/cap678.pdf

ANEXO A – ORGANOGRAMA

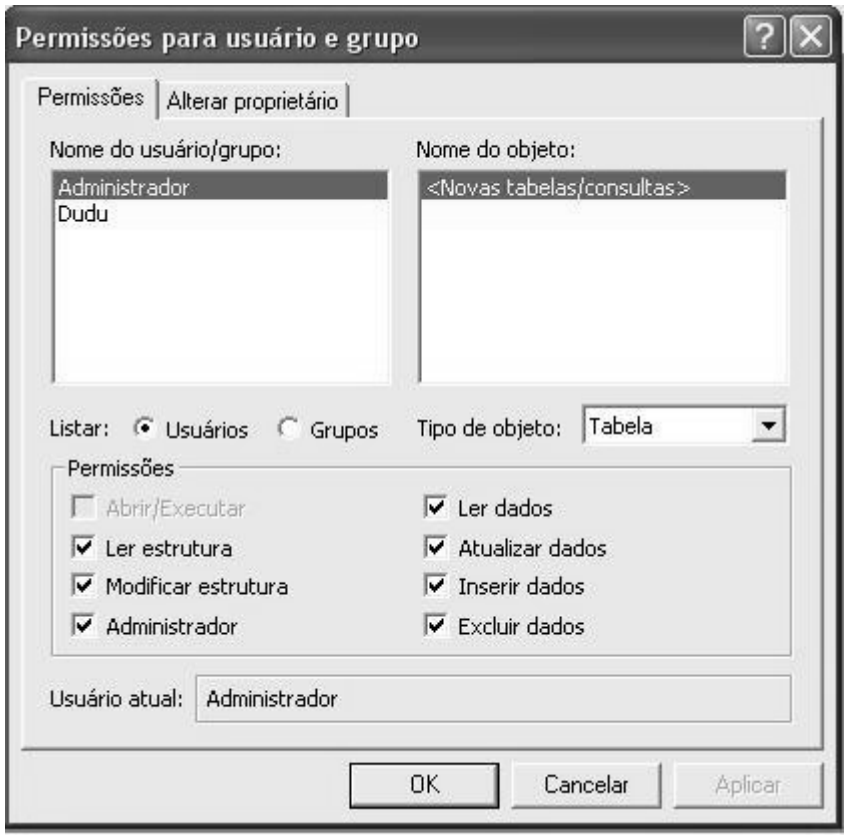
ANEXO B – MODELO ENTIDADES-RELACIONAMENTOS DA DASE DE DADOS DO CHPB

ANEXO C - DOCUMENTOS

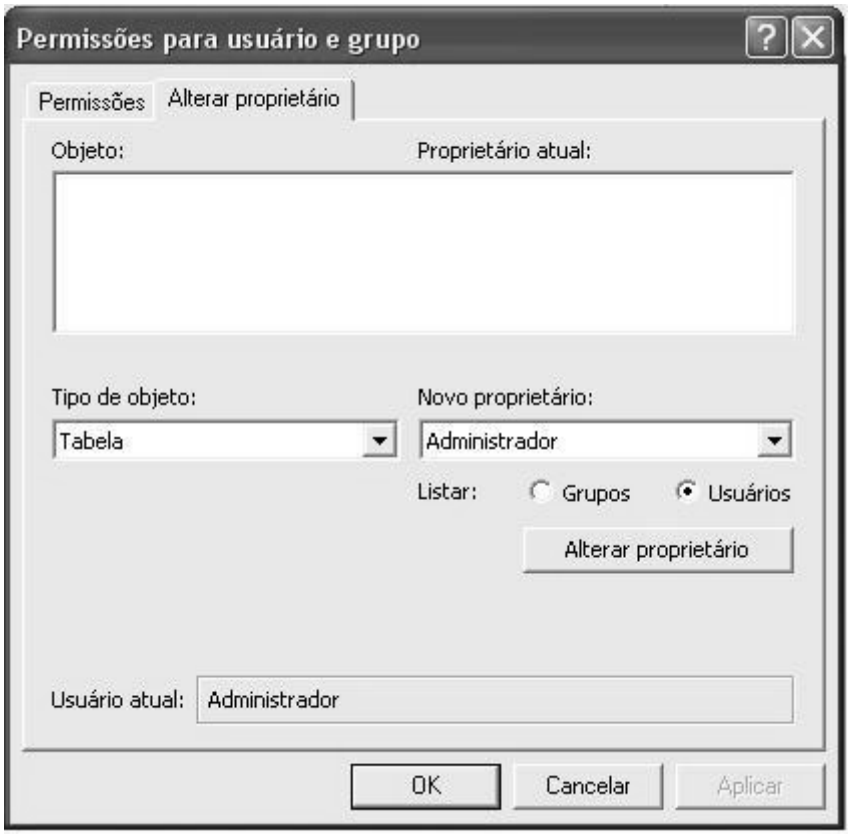
ANEXO D – TELAS



Tela para a definição de senha ao banco de dados



Tela para o controle de permissões a usuários e grupos



Tela para alterar o proprietário de um objeto

Tela para o controle de usuários do banco de dados

Tela para o controle dos grupos do banco de dados

Tela para o controle da senha de logon