



**Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"**

Danilo Cavassini Matioli

Importância da segurança em banco de dados

Assis
2010

Danilo Cavassini Matioli

Segurança em banco de dados

Trabalho de Conclusão de
Curso Apresentado ao Instituto
Municipal de Ensino Superior
de
Assis, com requisito do curso
de graduação.

Orientador: Domingos de Carvalho Villela Junior
Área de Concentração: Banco de Dados

Assis
2010

FICHA CATALOGRÁFICA

Cavassini Matioli, Danilo

Importância da segurança em banco de dados - Autor: Danilo
Cavassini Matioli

FEMA - Fundação Educacional do Município de Assis, Cândido
Mota - 2010

Orientador: Domingos de Carvalho Villela Junior

Trabalho de Conclusão de Curso - Instituto Municipal de Ensino
Superior de Assis

1 Banco de dados 2 Segurança em Banco de Dados

CDD: 001.61
Biblioteca da Fema

Importância da segurança em Banco de Dados

Danilo Cavassini Matioli

Trabalho de Conclusão de Curso Apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do curso de graduação analisado pela seguinte comissão examinadora:

Orientador: Domingos de Carvalho Villela Junior

Analisador Fábio Eder Cardoso

DEDICATÓRIA

Dedico este trabalho aos meus pais Antonio Mauricio Matioli e Isabel Cristina Cavassini Matioli, a meus amigos e aos professores da FEMA que me ajudaram a realizar este sonho.

AGRADECIMENTOS

Ao professor Domingos de Carvalho Villela Junior pela orientação e pelo constante estímulo transmitido durante o trabalho.

Aos amigos Rafael Ispier, Gabriel de Cleve, Rodrigo Peres, Paulo Vitor, Fábio Desiró e a todos que colaboraram direta ou indiretamente na execução deste trabalho.

Aos Familiares Antonio Mauricio, Izabel Cavassini, Ângela Cavassini e Luzia Lourenço Matioli.

“A amizade é um amor que nunca morre.”
Mário Quintana

RESUMO

Este trabalho demonstra a importância na segurança de banco de dados, sua importância para a empresa e prova com políticas simples que sua segurança será garantida a todo o tempo. O objetivo é verificar os problemas na segurança dos dados e através de políticas evitar ou mostrar soluções para que não ocorra a perda de dados.

Palavras Chave: Banco de Dados, Segurança, Tecnologia, Backup em Banco

ABSTRACT

This study demonstrates the importance of safety database, its importance to the company with policies and simple proof that its security will be guaranteed at all times. The goal is to identify problems and data security through policy solutions to prevent or show that no data loss occurs.

Keywords: Database, Security, Technology, Backup Database

LISTA DE ILUSTRAÇÕES

Figura 1 - Banco de dados.

Figura 2 – Tela Exemplo de lançamentos que o usuário pode fazer no sistema

Figura 3 - Imagem de um SGBD. Ele fica entre o banco de dados e os usuários.

Figura 4 – Tela de login no servidor de backup.

Figura 5 – Área de trabalho servidor de backup.

Figura 6 - Tela de Restore Objects

Figura 7 – Tela de Restore Sessions

Figura 8 – Fita do servidor de backup cheia

Figura 9 – Fita do servidor de backup vazia

Figura 10 - Representação de um sistema de banco de dados

LISTAS DE ABREVIATURAS E SIGLAS

SGBD – Sistema Gerenciador de Banco de Dados
DBA – Administrador de banco de dados
TB – Tera Byte

SUMÁRIO

1	INTRODUÇÃO	14
1.1	Justificativas/Motivações	15
1.2	Objetivos	16
1.3	Estrutura do trabalho	17
2	Banco de dados.....	19
2.1	Conceitos e Definições	19
2.2	Objetivos de um banco de dados	21
2.3	Vantagens de um banco de dados	22
2.4	Usuários de um banco de dados	23
3	Cuidando da segurança	25
3.1	SGBD	25
3.2	Privilégios.....	26
3.3	Redundância de dados.....	29
3.4	Independência de dados	29
3.5	Servidor de Backup	30
4	SQL e Acessos ao banco	35
4.1	Linguagem SQL.....	35
4.2	Instruções SQL.....	35
4.3	Controlando acesso ao banco de dados Oracle Server	36
4.4	Recuperação Baseada em Log	38
5	Segurança de um banco de dados.....	39
5.1	Recuperação e Backup	39
5.2	Backup do banco de dados é necessário	41
5.3	Como fazer o backup de um banco de dados.....	42
5.4	Gerenciamento de transações.....	43

6 Exemplos de banco de dados	45
6.1 Tipos de bancos de dados.....	45
6.2 Oracle.....	45
6.3 MYSQL.....	45
6.4 SQL Server.....	46
6.5 Sybase	47
6.6 DB2	47
6.7 PostgreSQL.....	48
6.8 Microsoft Access	48
7 Estudo de caso e conclusão final	49
7.1 Estudo de caso.....	49
7.2 Conclusão	52
7.3 Cronograma	54
7.4 Referência Bibliográfica.....	55
7.5 Referência Eletrônica	55

1 INTRODUÇÃO

Atualmente a tecnologia está em todo lugar. Ela está nas empresas (com computadores, banco de dados, sistemas para controles, nas máquinas) nos bancos (caixas eletrônicos) e até nas salas de aulas com os alunos utilizando notebook, internet sem fio, sem falar nos celulares com TV e com músicas.

Com isso vamos perceber que a tecnologia facilita nossas vidas e as tarefas do dia-a-dia. É bem mais fácil receber e-mails e enviar e-mails hoje que correspondências, pois a tecnologia vem para dominar o mundo.

Neste trabalho de pesquisa, vamos falar e entender sobre banco de dados. Com a tecnologia em alta, as empresas cada dia mais passam a serem informatizadas.

Toda empresa coleta dados. Esses dados devem ser armazenados e de forma segura.

Os dados são fatos como nome de um cliente, nome de uma rua, número de um telefone, idade de uma pessoa, tamanho de uma cidade, enfim, tudo que é fato é dado.

Para uma empresa, os dados são fundamentais. Antigamente, as empresas tinham esses dados, mas armazenados em papeis, documentos. Esses dados não estavam seguros e toda consulta ou modificação, era mais demorada, complicada. Hoje não.

Um banco de dados serve para armazenar dados. Esses dados poderão ser consultados, alterados e até excluídos. Antigamente procurar um cliente no meio de 400 clientes era um pouco mais demorado, pois os dados dele estavam armazenados em um papel ou documento. Hoje não. Temos, por exemplo, sistema para cadastro de cliente e a consulta hoje é muito mais rápida e simples.

A importância de se desenvolver este trabalho é entender como funciona realmente um banco de dados e sua segurança. Neste trabalho, vamos provar que um banco de dados não pode ser perdido e, caso ocorra algum caso sinistro, nossas políticas irão permitir a recuperação de todo o banco.

O desenvolvimento deste trabalho é feito a partir de estudo de caso, pesquisas e leitura de livros.

Um banco de dados não tem um tamanho específico. Pelo contrário, varia muito.

Muitos usuários acessam um banco de dados e tudo isso deve ser monitorado para que cada usuário acesse somente o que deve acessar.

Em um banco de dados, o recurso primário é o próprio banco de dados e o secundário é o SGBD e os softwares relacionados. A administração destes recursos cabe ao Administrador de banco de dados, o DBA. Ele é o responsável por dar acesso aos usuários ao banco de dados e por manter toda sua segurança.

1.1 JUSTIFICATIVAS E MOTIVAÇÕES

Atualmente, com a tecnologia, surgem necessidades para as empresas. Com o aumento da demanda, dos funcionários, clientes e da empresa, muitos dados são manipulados a todo o momento. Inclusão de um novo cliente, alteração, exclusão e outros processos a todo instante, passa a ser um problema para a empresa, pois não pode perder os dados e como DBA, facilitar a rotina é um objetivo. Quando um cliente, por exemplo, faz um pedido de 100 latas de cerveja, rapidamente temos que consultar se temos 100 latas no estoque, se o cliente tem cadastro na empresa, se o endereço dele no cadastro está correto para a entrega e muitas outras coisas. Por isso um banco de dados. Com os dados no banco de dados, as consultas são rápidas e caso haja a necessidade de alteração ou exclusão, isso será rápido.

Toda empresa pode ter um banco de dados, basta à empresa querer e fazer um investimento.

Sendo assim, será citado como exemplo a Casa Di Conti, cervejaria de grande porte localizada em Cândido Mota. A empresa possui um quadro de 540 funcionários. O banco de dados existe lá e no caso é Oracle. A motivação do trabalho vem da seguinte conclusão: "Toda empresa pode possuir um banco de dados. No caso, a empresa é de grande porte, portanto, concluímos que é viável ter um banco de dados, pois é o modo mais simples de se armazenar dados com segurança, tirar rápidos relatórios, gerar informações...". Vamos mostrar que um banco de dados facilita as rotinas de uma empresa e evita erros que o ser humano pode cometer.

Gilberto Cardoso gerente de TI da Casa Di Conti há dez anos afirma que um banco de dados armazena dados (fatos como nome de um cliente, nome de uma empresa, nome de uma cidade) e esses dados são processados para gerar informação, onde as informações podem ser utilizadas para ajudar na tomada de decisão, para alcançar objetivo e metas e também para ajudar nas tarefas rotineiras, como pesquisas e atualizações.

A tecnologia de um banco de dados já foi descrita como sendo uma das áreas mais rápidas do crescimento na informação. Os sistemas de banco de dados começam a serem oferecidos e vendidos no final da década de 1960 e, antigamente, não se tinha pacotes de softwares tão seguros e avançados iguais hoje.

Logo o trabalho mostra que muitas organizações tornam-se criticamente dependentes da operação contínua bem sucedida do sistema de banco de dados.

Por isso vamos ver que o gerenciamento de um banco de dados está evoluindo e torna-se essencial e necessário para uma organização.

1.2 OBJETIVOS

Com este trabalho vamos mostrar que o principal objetivo é garantir a segurança dos dados no banco de dados.

Um banco de dados é seguro, desde que suas políticas de segurança sejam bem executadas.

Será mostrado como resolver os problemas de empresas que ainda estão em dúvida se utilizam ou não banco de dados, se é seguro ou não e se é viável.

Com este trabalho será e mostrado que o banco de dados é seguro sim e que nunca ele será perdido. Com isso, será provado o quanto é viável se ter um banco de dados.

Há várias formas de se garantir a segurança de um banco de dados como, por exemplo, privilégios a usuários e/ou a grupos de usuários, SGBD e outros programas que serão utilizados para garantir a segurança de nossos dados. São os DBA que vão utilizar os SGBD para criar contas de usuários e dar privilégios aos usuários conforme sua necessidade e conforme o que ele irá utilizar.

Os SGBD são responsáveis por verificar todas as requisições de um acesso. É de suma importância para a segurança de um banco.

O DBA é responsável por administrar o banco de dados e os desenvolvedores são responsáveis para que os dados sejam armazenados corretamente.

1.3 ESTRUTURA DO TRABALHO

O presente trabalho está dividido em sete capítulos. Cada um falando de um assunto que o envolve.

Veja abaixo como vai ser o desenvolvimento deste trabalho:

BANCO DE DADOS

- ✓ Conceitos e Definições: Conceitos sobre banco de dados retirados de livros específicos para o entendimento do que vamos falar.
- ✓ Objetivos: Vamos entender os objetivos de um banco de dados
- ✓ Vantagens: Vamos falar das vantagens de utilizar banco de dados
- ✓ Usuários de um banco de dados

CUIDANDO DA SEGURANÇA

- ✓ SGBD: Vamos ver esta ferramenta e qual sua importância para um banco de dados.
- ✓ Privilégios: Entender sobre o que é privilégio e qual sua contribuição para a segurança de um banco de dados.
- ✓ Redundância de dados: Explicar que a redundância prejudica um banco de dados, pois é desnecessária e deve ser evitada, mesmo com muitos programadores se for o caso.
- ✓ Independência de dados: Quanto menos dependente, melhor.
- ✓ Servidor de backup

SQL e Acesso ao Banco

- ✓ Linguagem SQL: Introdução básica
- ✓ Instruções SQL: Comandos utilizados em um banco de dados
- ✓ Controlando acessos: Controlar acesso ajuda a manter o banco ainda mais seguro
- ✓ Recuperação baseada em log: Recuperação de dados e entendimento sobre log.

Segurança de um banco de dados

- ✓ Recuperação e backup: Recuperação de dados com nossas políticas de segurança.
- ✓ Backup do banco de dados é necessário
- ✓ Como fazer o backup
- ✓ Gerenciamento de transações

Exemplos de banco de dados

- ✓ Tipos de banco de dados: Vamos ver alguns tipos de banco de dados
- ✓ Oracle
- ✓ MySql
- ✓ SQL Server
- ✓ Sybase
- ✓ Postgresql
- ✓ Microsoft Access

ESTUDO DE CASO E CONCLUSÃO FINAL

- ✓ Estudo de caso: Vamos fazer estudo de caso para melhor entendimento do trabalho
- ✓ Conclusão
- ✓ Cronograma
- ✓ Referências

2 BANCO DE DADOS

2.1 CONCEITOS E DEFINIÇÕES

Segundo o autor C.J. Date, banco de dados pode ser definido como um sistema computadorizado de manutenção de registros, dados. Sua funcionalidade é armazenar dados de forma que os usuários busquem e atualizem esses dados. Esses dados quando processados geram informações.

Pode-se então dizer que sistemas de banco de dados não mais é que um sistema de armazenamento de dados baseado em computador, isto é, um sistema cujo objetivo global é registrar e manter informação.



Figura1 – Banco de dados

Vale lembrar que antigamente, tudo era “armazenado” em algum papel. Além de muito trabalho, inúmeras desvantagens podem ser citadas, como demora em localizar algo, densidade e menos proteção.

Basicamente, um sistema de banco de dados envolve quatro principais componentes que são dados, hardware, software e usuários.

Os dados são os fatos como o nome de um fornecedor, nome de um cliente, nome de outra empresa, enfim, tudo o que é fato são dados.

Um campo armazenado é a menor unidade de dados como um nome armazenado no banco de dados.

Um banco de dados é integrado, pois pode ser imaginado como uma unificação de diversos arquivos, onde eles têm que ser distintos, evitando-se assim a redundância de dados.

Um banco de dados também é compartilhado. Todos os departamentos devem ter acesso ao banco de dados, mas cada usuário deve ter acesso somente o que lhe é permitido e utilizado em seu ambiente de trabalho, pois assim iremos garantir sua segurança desde o princípio. Garantir que os usuários terão permissão de fazer aquilo que estão tentando fazer e não fazer o que não tem autorização, como, por exemplo, aumentar seu próprio salário no sistema de folha de pagamento, é fundamental e básico falando sobre segurança.

Vale lembrar que a segurança de um banco de dados não é simplesmente contra a perda ou danificação de dados. É também contra os acessos indevidos. Um usuário não pode alterar seu próprio salário, se ele conseguir, já temos uma falha grave na segurança dos dados.

No banco de dados temos a parte lógica. A parte lógica nada mais é que os softwares do banco de dados. Entre o banco de dados físico (os dados que estão armazenados) e os usuários, existem softwares que são utilizados como forma de garantir a segurança do banco e dar acesso aos dados. Esses softwares geralmente são desenvolvidos por programadores. Todas as solicitações de acesso ao banco feita por usuários são manipuladas pelo sistema gerenciador de banco de dados (SGBD).

Outros componentes que envolvem o banco de dados são os usuários. Eles é que “alimentam o banco” com os dados que o software pede para ser cadastrado, alterado ou excluído.

Os usuários são divididos em três classes. Primeiramente temos o programador, responsável por desenvolver softwares de aplicação que utilizam o banco de dados. Esses softwares são programados em diversas linguagens como COBOL e outras. São esses programas que operam os dados do banco de dados. Eles também fazem recuperação de informações, criação de outras e alteração, por exemplo.

Outra classe de usuários é a classe de usuários finais. Esses usuários têm acesso aos dados do banco a partir de um terminal. Estes usuários são os que vêem somente o sistema em si e não tudo o que está por trás disso, como a programação e a segurança dos dados.

Na verdade o usuário final nada mais é que a pessoa que informa ao sistema os dados solicitados.

Em um sistema de contas a pagar, as contas a pagar são lançadas pelos usuários finais. Podem ser também excluídas (se ele tiver privilégios para excluir) e alteradas.

Por último temos também outra classe de usuários que são os Administradores de banco de dados. Eles são os DBA. Um administrador de banco de dados não pode ser um usuário comum, pois é exigido dele um nível mais técnico. Ele é o responsável pelo banco de dados. O cargo de DBA em termos de banco de dados é o mais elevado, sendo de grande responsabilidade.

Um DBA deve garantir que o banco funcione perfeitamente e com segurança. Dependendo do tamanho do banco, pode existir um grupo de administradores, não sendo necessária uma só pessoa responsável.

2.2 OJETIVOS DE UM BANCO DE DADOS

O principal objetivo de um banco de dados é armazenar dados.

Dentro de uma organização, o banco de dados deve atender a necessidade da empresa e de todos os usuários em si. Os usuários devem armazenar os dados para gerar informações que serão utilizadas futuramente para algum outro fim ou objetivo. O banco de dados deve armazenar esses dados permanentemente, garantindo segurança total a esses.

O banco de dados deve ser "flexível". Esta flexibilidade deve existir, pois a cada nova necessidade deve haver uma nova solução. Por exemplo, no cadastro de clientes existia nome, idade, sexo, cidade e país. Para uma nova pesquisa de mercado havia a necessidade de se saber quantos dependes esses clientes tem como esposa e filhos, por exemplo. O sistema deverá permitir que o administrador ou programador responsável inclua no sistema um novo campo que cadastre quantos dependentes ele possui. Isso será disponibilizado para o usuário final que deverá cadastrar os dados de cada cliente, atualizando assim o banco, mantendo os dados atualizados e

garantindo que as necessidades da empresa (que no caso uma era o campo dependentes para a pesquisa) sejam atendidas.

Resumindo, um banco de dados tem como principais objetivos:

- Atender as necessidades da empresa e dos usuários
- Garantir a segurança dos dados e das transações
- Agilizar os processos de consultas, alterações e exclusões de dados
- Armazenar os dados e garantir que ficaram armazenados permanentemente

2.3 VANTAGENS DE UM BANCO DE DADOS

Um banco de dados proporciona a uma organização o controle centralizado dos dados, onde isso é necessário para uma empresa e é uma grande vantagem. Há várias vantagens do controle centralizado dos dados como, por exemplo, a redução de redundância de dados e o compartilhamento de dados.

Um banco deve:

- ✓ Garantir de integridade: Os dados armazenados devem satisfazer certos tipos de restrições. Ex: o salário de um funcionário não pode ser zero reais.
- ✓ Garantir a restrição de acesso não autorizado: Os usuários devem acessar somente o que realmente podem acessar para ajudar em seu trabalho.
- ✓ Garantir a recuperação e backup: Caso ocorra falha, o SGBD deve restaurar até um ponto anterior garantindo os dados até este ponto.
- ✓ Garantir o controle de concorrência: Um dado deve ser atualizado apenas por um usuário naquele momento. Vários usuários usando o mesmo sistema ao mesmo tempo podem acontecer de dois ou mais tentarem atualizar o mesmo dado. Isso não deve ser permitido.
- ✓ Garantir o compartilhamento de dados: os dados devem ser compartilhados e os departamentos devem interagir entre si, formando assim um sistema que se comunica e interage.

Além de todas essas vantagens, percebemos que de certo modo uma organização depende de um banco de dados, pois todos os dados deverão ser armazenados e mantidos em segurança. O banco de dados visa facilitar as transações e agilizar as operações, armazenando os dados com segurança.

2.4 USUÁRIOS DE UM BANCO DE DADOS

Segundo o autor Henry Korth a meta básica de um sistema de banco de dados é proporcionar um ambiente para recuperação de informações e para o armazenamento de novas informações no banco de dados.

Em um banco de dados vários usuários o utilizam. Dentre eles temos:

→Programadores de aplicações: São profissionais em computação, formados e capacitados que interagem com o sistema por meio de chamadas DML, as quais são envolvidas pro programas escritos na linguagem hospedeira (como por exemplo, COBOL). Exemplos em um sistema bancário incluem programas para gerar relação de cheques pagos, para débitos em conta, transferência e outros.

→Usuários sofisticados: interagem com o sistema, mas não são programadores. Exemplos são os analistas.

→Usuários Especialistas: São usuários que escrevem aplicações especializadas de banco de dados que não podem ser classificadas como aplicações tradicionais.

→Usuários Navegantes ou usuários finais: São os usuários comuns, geralmente a maioria. São eles quem coloca informações no sistema, alteram e às vezes, até apagam informações (caso tenham permissões para apagar). Eles são quem interagem com o sistema chamando um dos programas prontos já. Por exemplo, em um sistema bancário, ele abre a tela de transferência, e só completa os dados que a tela pede para ele como na figura abaixo:

Código	Conta Bancária	Valor	Tipo
			<input type="radio"/> Débito <input type="radio"/> Crédito

Emp / Filial	Data	Data Banco	Tipo Contábil

Centro de Custo	Conciliado
	<input checked="" type="checkbox"/>

Detalhes														
<table border="1"><thead><tr><th>Pessoa</th><th>Tipo Doc</th><th>Nº Doc.</th><th>Valor</th><th>Código Fin.</th><th>PC</th><th>SP</th></tr></thead><tbody><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table>	Pessoa	Tipo Doc	Nº Doc.	Valor	Código Fin.	PC	SP							
Pessoa	Tipo Doc	Nº Doc.	Valor	Código Fin.	PC	SP								

Transferir

Figura 2 – Tela Exemplo de lançamentos que o usuário pode fazer no sistema

Aqui o usuário final vai só completar os campos. Os campos devem ser todos preenchidos. No caso da transferência, ele vai só completar os campos, clicar no botão transferir e depois clicar em ok que tudo isso já será realizado pelo programa. Automaticamente se ele transferir 100 reais da conta A para a conta B, a conta B terá o saldo que tinha + 100 reais. A conta A irá ficar saldo – 100. Caso a conta A antes da transferência tinha 200 reais e a B tinha 100, a conta A vai ficar com 100 reais e a B com 200.

3 CUIDANDO DA SEGURANÇA

3.1 SGBD

SGBD é um sistema gerenciador de banco de dados. Um SGBD deve fornecer subsistemas de autorização e segurança o qual é usado pelo DBA para criar contas de usuários e especificar as restrições destas contas. Essas permissões podem ser dadas por grupos ou por usuários específicos. Quando a permissão é dada por grupos, as pessoas do grupo têm o mesmo nível de acesso.

Caso o departamento de RH de uma cervejaria tenha cinco pessoas, o DBA pode criar um grupo chamado de `gs_rh` e incluir essas pessoas, pois assim organizamos os departamentos e as permissões podem ser dadas pelo grupo ou por usuários. As permissões podem ser:

- Somente leitura
- Leitura e alteração de dados
- Controle total

Um sistema gerenciador de banco de dados é uma coleção de programas para acesso a dados. Dentre seus objetivos e funções ele visa proporcionar um ambiente conveniente e eficiente para a recuperação e armazenamento de informações.

Um sistema de banco de dados é projetado para armazenar um grande volume de dados.

Como o sistema é compartilhado, devemos ter um controle sobre isso, evitando assim que os usuários modifiquem ou acessem dados que não devam acessar.

Outro objetivo de um SGBD é proporcionar aos usuários uma visão abstrata dos dados, isto é, o sistema esconde determinados detalhes sobre certos dados. Isso é feito através de definições de níveis.

Antes do acesso ao banco, o SGBD deve estar ali para verificar se o acesso deve ser permitido ou não. Veja na imagem abaixo:



Figura 3: Imagem de um SGBD. Ele fica entre o banco de dados e os usuários.

Concluimos que um SGBD nada mais é que um conjunto de programas responsáveis pelo gerenciamento de uma base dos dados. É um sistema complexo que é responsável pela proteção dos dados, organização e recuperação de dados. Com ele vamos garantir ainda mais a segurança dos dados. Não tem como um sistema de banco de dados não possuir um SGBD, pois ele é o software responsável por controlar os acessos ao banco de dados. O DBA vai criar as contas dos usuários um a um. A partir daí, depois de criadas todas as contas, ele vai dar as devidas permissões a cada usuário.

3.2 PRIVILÉGIOS

Quando falamos em privilégios, estamos falando de usuário e locais de acesso. Para a segurança de um banco de dados isso é fundamental. Os privilégios servem para dar acesso a um determinado usuário para que ele possa acessar um determinado local. Os privilégios são dados pelo administrador de banco de dados. Cada usuário deve ter acesso somente ao que utiliza e é autorizado a utilizar. Com os privilégios corretos, devemos garantir que os usuários terão permissão de fazer aquilo que estão tentando fazer e não fazer o que não tem autorização, como, por exemplo, aumentar seu próprio salário no sistema de folha de pagamento.

Um usuário que trabalha com cadastro de clientes não deve ter acesso ao sistema de folha de pagamento, pois a segurança do banco estará sendo comprometida, onde se o acesso for liberado ele pode ter acesso às informações de salários (geralmente confidencial) e pode fazer alterações, prejudicando a empresa e se beneficiando em cima disso. No caso, ele pode ganhar apenas 700 reais e aumentar seu salário para 10000. Caso ninguém confira isso e confie no sistema (o que pode acontecer), ele irá se beneficiar em cima da empresa.

Os privilégios podem ser de:

- Controle Total (o usuário possui controle total)
- Somente Leitura (o usuário tem privilégios somente de leitura)
- Leitura e gravação (o usuário pode alterar e gravar no sistema)

Os privilégios podem ser dados por usuários ou por grupos de usuários. Os privilégios por usuários são privilégios dados somente aquele usuário. Por exemplo, temos um usuário chamado Bruno Camoleze, que tem acesso à pasta TI (tecnologia das informações) com privilégios de controle total. Com essa permissão, ele pode apagar dados, alterar dados, criar pastas dentro desta pasta e até mesmo dar permissão a outros usuários. Caso temos este mesmo usuário com permissão somente leitura, ele só poderá abrir o arquivo para leitura. Ele não poderá criar escrever ou gravar novos dados, pois sua permissão é somente leitura.

Também é possível dar permissões por grupos de usuários. Caso o departamento de rh tenha cinco usuários, por exemplo, pode se criar um grupo de usuários chamado de g_rh e colocar todos os usuários do rh nele. As permissões dadas a este grupo g_rh irá servir para todos os usuários que estiverem no grupo.

Para simplificar, temos uma pasta com o nome RH_FINANÇAS e todos os usuários do rh devem ter permissão de leitura e gravação nela. Ao invés de dar-mos permissão a cada usuário, vamos adicionar o grupo g_rh e dar o privilégio de leitura e gravação ao grupo. Isso é pratico, pois neste exemplo ainda temos poucas pessoas neste departamento. Mas e se tivéssemos 100 pessoas? Dar permissão uma a uma não seria viável. Por isso a criação de um grupo. Mas vale lembrar que todas as permissões dadas a um grupo serão as mesmas para todos os usuários que estão dentro dele. Isso significa dizer que se quero dar permissão para leitura para o usuário1 e de gravação para o usuário2, deve-se dar por usuário, pois se for por grupo isso não é possível caso os dois estejam no mesmo grupo.

Logo conclui que uma empresa possui vários usuários e departamentos, depende muito do porte dela. Para facilitar, depois de criar todos os usuários, se deve separá-los por grupos. Esses grupos deixaram todo nosso sistema organizado e não impedirá cuidar da segurança de um banco.

Veja como podem ser organizados os usuários de uma empresa:

RH

Vanda Teodoro da Silva

Viviane Flauzino

Joyce Antunes

TI

Gilberto Cardoso

Danilo Matioli

José Silva

Almoxarifado

Marcelo Alves

Paulo Marques

Rodrigo Muniz

Financeiro

Toninho Barbosa

Éderson Villela

Cada usuário na sua respectiva área de trabalho. Neste exemplo, vimos que no RH temos três usuários que são Vanda, Viviane e Joyce. Se a empresa tiver poucos departamentos, fica simples saber sobre qual departamento cada usuário pertence. Mas e uma empresa com 1000 funcionários? Por isso cada usuário novo deve ser cadastrado e colocado em seu departamento, para que o banco de dados fique organizado.

Assim deve ser feito para cada novo cliente também. Quando mais campos forem preenchidos, melhor. Quando mais dados melhor.

No caso de cadastrar um novo cliente, você deve no mínimo colocar os dados básicos como nome, endereço, telefones, cidade, idade, sexo e estado civil. Sendo assim, cada empresa pode definir como deseja fazer o cadastro. Pode colocar somente esses dados básicos como também poderá aumentar esta tela de cadastro de cliente, pois quanto mais dados, melhor, pois mais informações estarão disponíveis.

Depois de criar cada usuário é só verificar suas permissões. Para dar permissão, basta fazer uma análise e verificar qual a permissão que cada usuário deve receber.

Vale lembrar que as permissões devem ser dadas somente por quem realmente sabe sobre a segurança, pois o controle do banco e a responsabilidade devem ser do DBA.

O DBA é quem vai dizer quem tem permissões para realizar certas operações.

AS permissões devem ser dadas somente para os usuários fazer o que realmente precisam fazer e acessar somente o que realmente necessitam acessar, dificultando assim que as tarefas maliciosas (de má fé) não sejam realizadas, garantindo assim a segurança do banco.

3.3 REDUNDÂNCIA DE DADOS.

Redundância de dados prejudica o sistema e isso não pode acontecer. No processamento de dados, cada grupo da empresa tem que manter os seus dados atualizados, ou seja, a cada mudança que ocorre em um cliente, por exemplo, isso deve ser alterado no sistema. Sendo assim, redundância nos dados podem ocorrer. Quando algo for alterado, isso deve ser para um grupo todo para manter a integridade dos dados. A desvantagem é que com a redundância de dados ocorrendo, mais espaço desnecessário será gasto.

Os programas muitas vezes são criados por programadores diferentes por um longo período de tempo, onde a redundância pode acontecer a partir daí. O mesmo elemento (dado) pode ser duplicado em diversos lugares. Para evitar isso, uma análise deve ser feita e definida onde todos os programadores vão seguir para que não ocorram formatos diferentes nos arquivos.

3.4 INDEPENDÊNCIA DE DADOS

A independência de dados é definida como a imunidade das aplicações a mudanças na estrutura de armazenamento ou estratégia de acesso.

A independência dos dados é fundamental. Grande parte das aplicações hoje em dia é dependente de dados, onde as formas como os dados estão organizados na memória e a forma de ter acesso a eles são ambas ditadas pelas necessidades da aplicação, onde os dados devem ser independentes e não dependentes.

Uma aplicação pode ser considerada dependente quando é impossível mudar a estrutura de armazenamento, por exemplo, sem afetar o restante da aplicação. Por isso dizemos que a independência dos dados é fundamental para assim, caso necessário, fazer mudanças sem afetar a aplicação. Essas mudanças podem ser, por exemplo, a forma de se ter acesso aos dados, onde se os dados forem dependentes,

será impossível mudar a estrutura sem afetar a aplicação. Com a independência dos dados isso é possível.

É importante notar que as aplicações hoje em dia geralmente têm a necessidade de mudanças e é de fundamental importância a independência dos dados para poder facilitar essas mudanças, pois elas poderão ser realizadas sem alterar toda a estrutura.

O trabalho mostra que é indesejável para um sistema de banco de dados que as aplicações fossem dependentes por vários motivos, dentre eles:

→ Aplicações diferentes necessitarão visões diferentes para o mesmo dado.

→ O DBA deve ter liberdade e facilidade para alterar a forma de acesso aos dados em respostas às necessidades que podem surgir de acordo com o tempo.

3.5 SERVIDOR DE BACKUP

No nosso estudo de caso, vamos estudar a empresa Casa Di Conti. A Casa di Conti, usa como política de backup dois tipos de backup:

→ Um de todo o banco semanalmente

→ Um de todas as planilhas e docs, de aproximadamente 300 GB feito diariamente.

No estudo de caso, vamos mostrar algumas falhas na segurança que a empresa apresenta e vamos ver soluções para essas falhas.

Nosso trabalho visa contribuir com a segurança dos dados e, neste caso, vamos verificar os erros na política de backup da empresa e mostrar soluções, mas isso, no estudo de caso.

A empresa possui um servidor de backup da HP muito eficiente. Este servidor de backup tem até software próprio para fazer o backup.

No servidor "SCDC" (nome do servidor em que o servidor de backup fica localizado) é onde verificamos todo o backup.

O backup é feito em fitas de 800 GB. Mas como é feito?

Vejamos algumas telas do servidor de backup para entender melhor.

O responsável pelo backup possui várias funções. Dentre elas ele é responsável por:

- ✓ Programar o horário que o backup deve ser feito (isso depois que ele fez uma vez é o suficiente. Nesta parte ele cria a política de backup. Por exemplo, o

backup dos dados está programado para começar as 12:00 horas todo dia, de segunda a sábado, por exemplo).

- ✓ Manter o servidor de backup ligado.
- ✓ Colocar todas as fitas necessárias para o backup. Caso o backup seja só das planilhas, deverá colocar apenas uma fita que é o suficiente. Caso seja feito o backup de todo o banco, devem ter fitas para os 3 TB de informações.
- ✓ Formatar as fitas caso elas estejam cheias. Isso é de suma importância. O servidor de backup depois de programado ele faz o backup sozinho, onde para isso, o responsável deve deixar as fitas formatadas para que o servidor possa fazer o backup.
- ✓ Checar para ver se o backup foi feito com sucesso.

Essas são as principais funções da pessoa responsável pelo backup. No caso da Casa Di Conti, o DBA Gilberto é o responsável.

Como vimos, ele deve chegar para ver se o backup foi feito e se foi feito sem falhas.

Para isso ele conta com um software que o auxilia. Esse software fica instalado no servidor de backup e tudo é feito por ele.

Vejamos algumas telas.

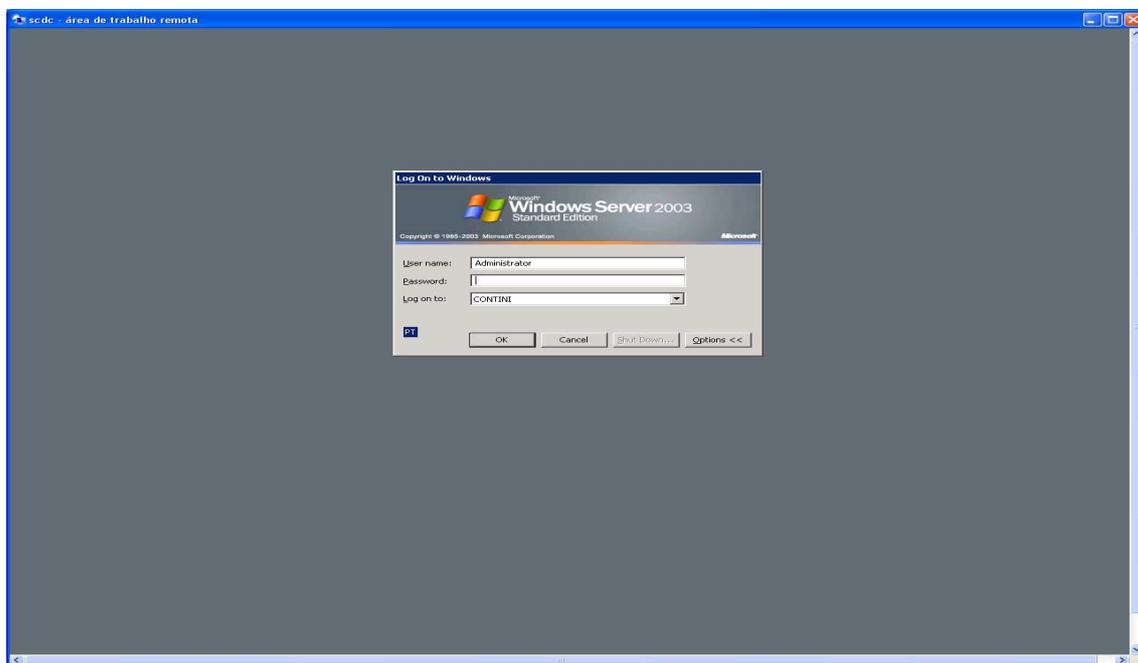


Figura 4 – Tela de login no servidor de backup.

Para entrar no servidor de backup, pode-se conectar por área de trabalho remota. Neste caso, coloca-se o nome do servidor e clica em conectar.

Depois devemos colocar a senha do Administrator. Assim ele irá acessar o servidor.

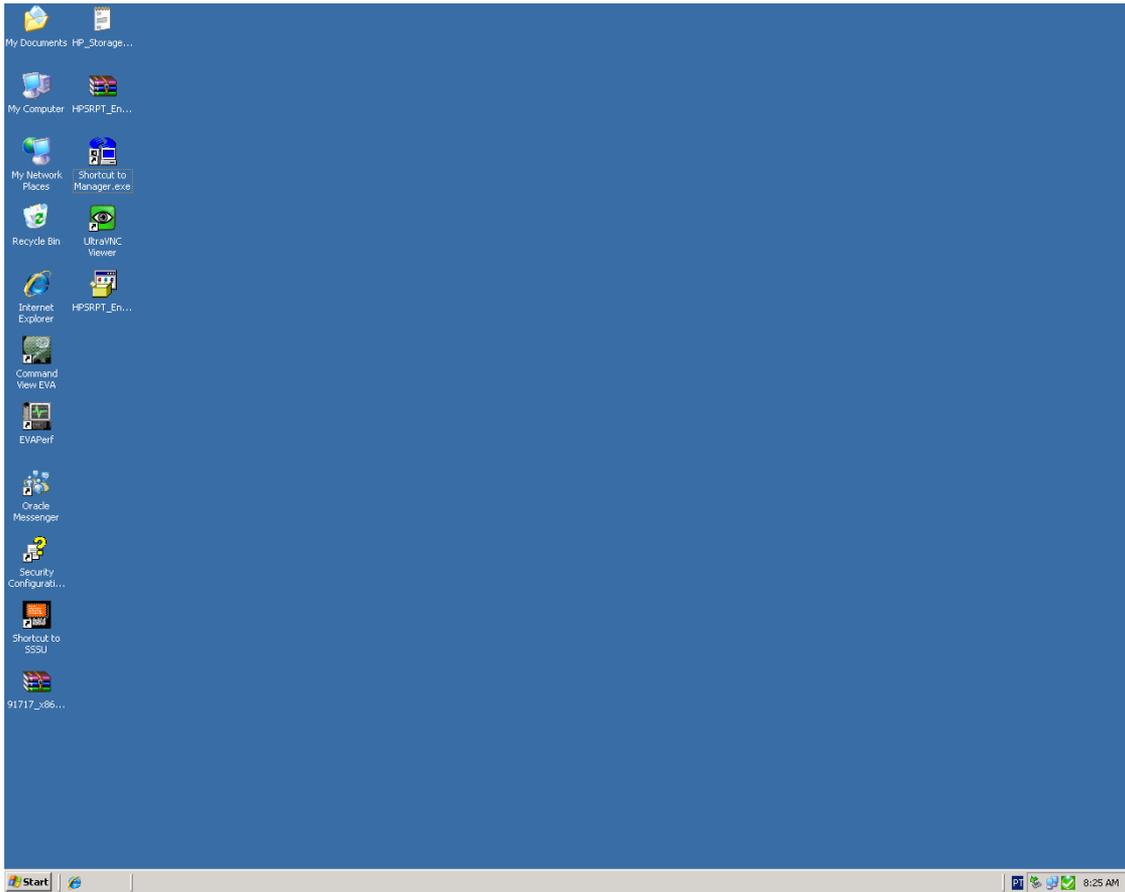


Figura 5 – Área de trabalho servidor de backup.

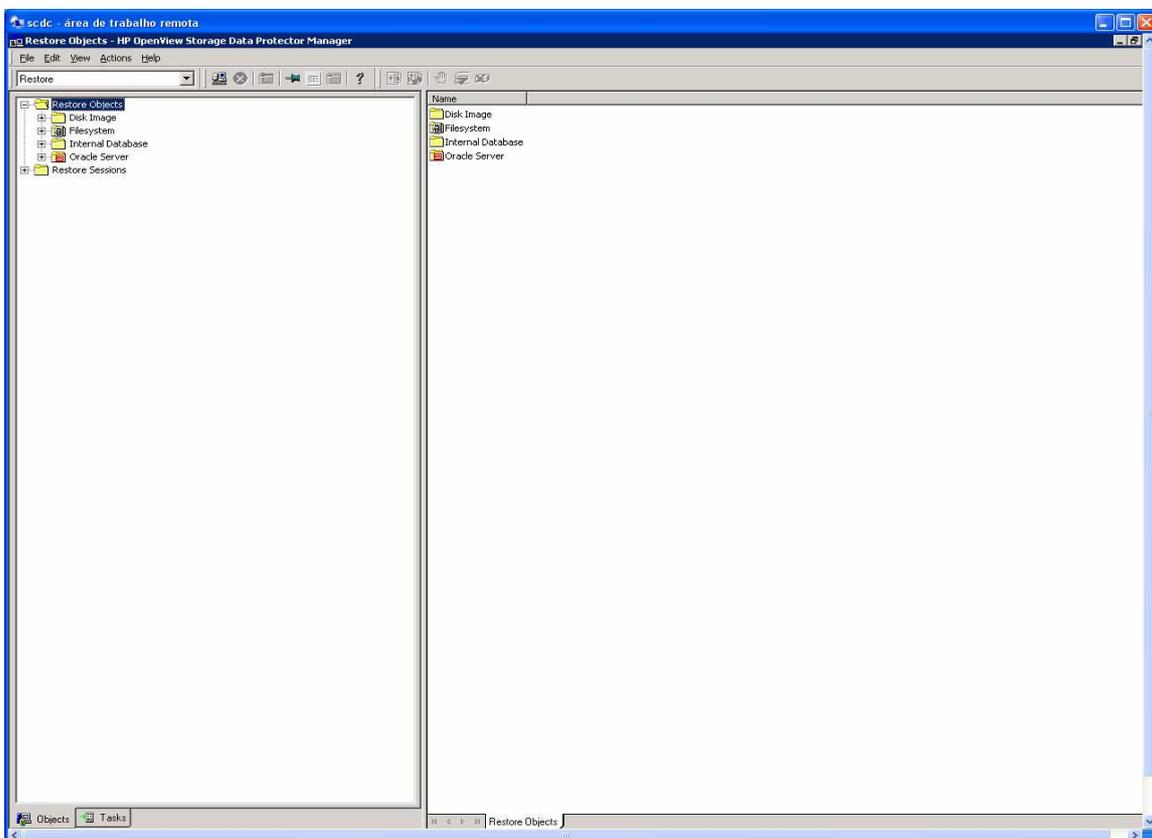


Figura 6 - Tela de Restore Objects

Para verificar que o backup ficou OK, em Restore Sessions ele irá aparecer sem o “X”.

A figura abaixo mostra a tela:

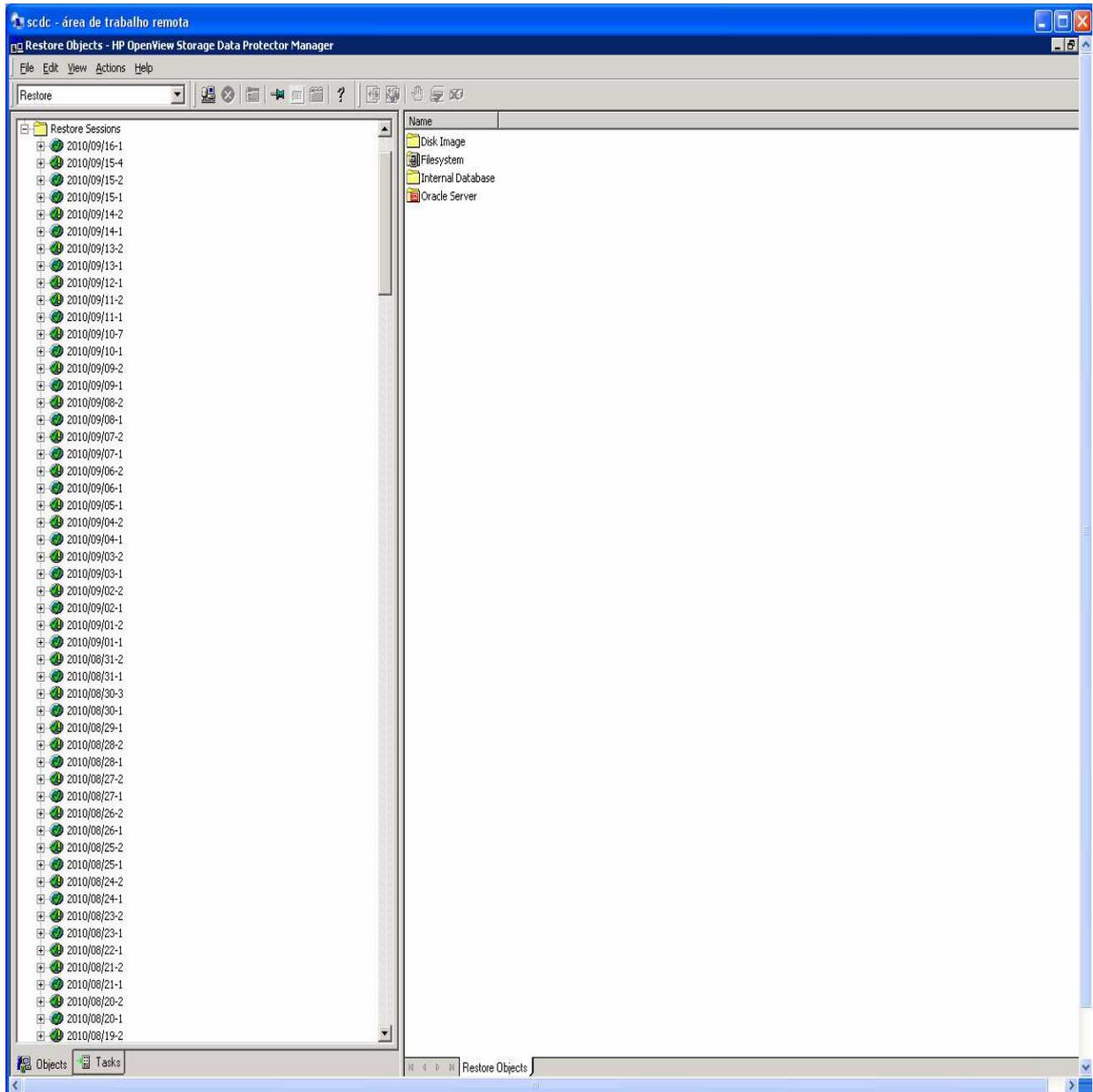


Figura 7 – Tela de Restore Sessions

Nesta figura 8 o backup do dia 16 foi feito sem erros. Já o do dia 15 foi feito mas com um alerta. Isso pode ocorrer. Só não teria feito, caso o “X” estivesse na frente do dia. Após programar o backup e colocar as fitas, o responsável pelo backup deve analisar a fita. Provavelmente ela vai estar com outro backup. Quando ela está cheia, a fita deverá ser formatada para receber o novo backup.

Veja na imagem abaixo a figura da fita cheia e depois vazia.

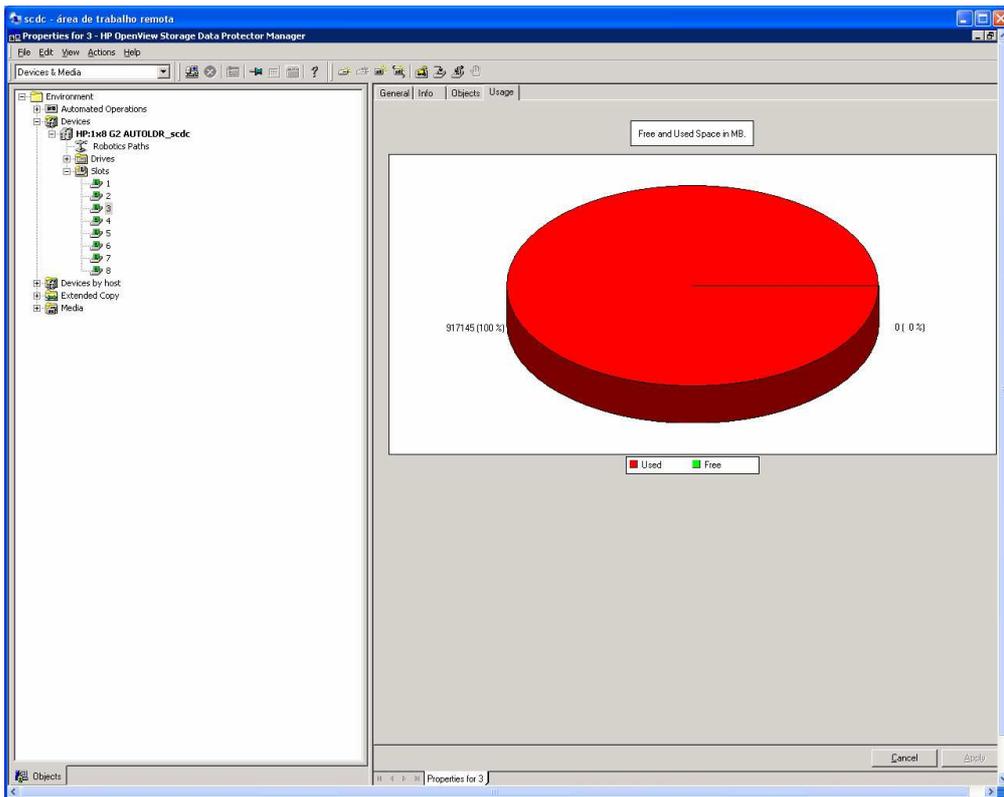


Figura 8 – Fita do servidor de backup cheia.

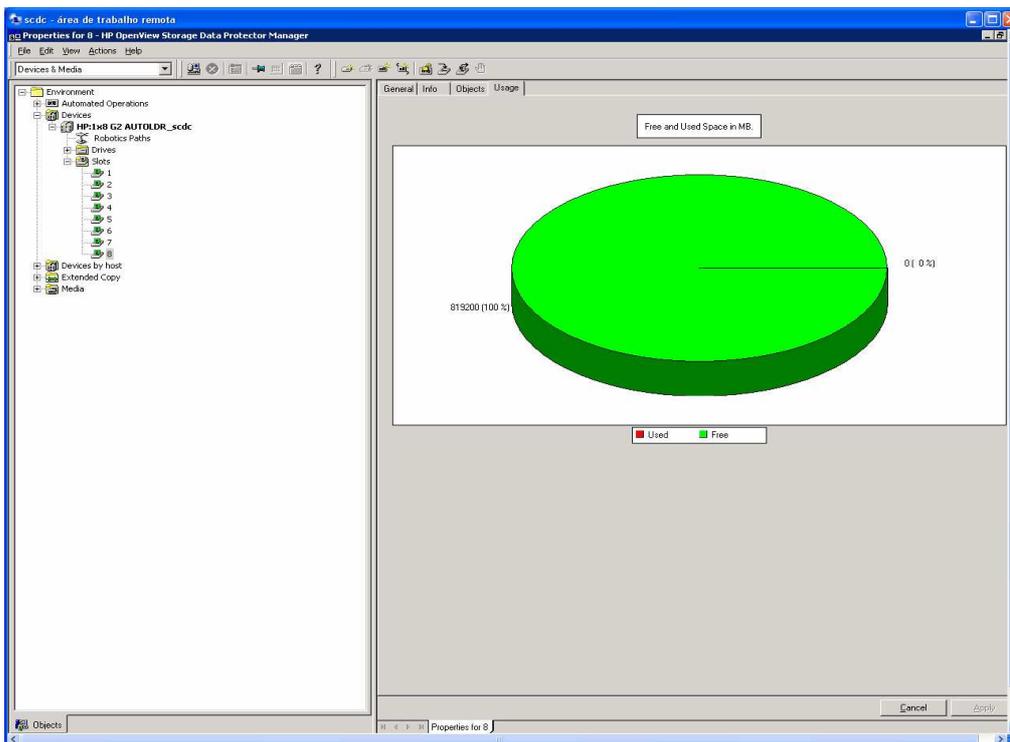


Figura 9 – Fita do servidor de backup vazia.

4 SQL E ACESSO AO BANCO

4.1 LINGUAGEM SQL

SQL (Structured Query Language) nada mais é que uma linguagem de consulta estruturada.

Esta linguagem começou a ser desenvolvida por volta dos anos 70 nos laboratórios da IBM. A linguagem SQL é um grande padrão de banco de dados, isto é, não serve só para o banco Oracle. Pode ser utilizada em vários bancos.

A grande vantagem de se utilizar SQL é justamente esta: inúmeros produtos dão suporte a ela.

SQL possui muitos recursos como consultas ao banco, modificações de dados e outros.

A linguagem SQL possui várias partes. Dentre elas:

→DDL: Linguagem de definição de dados.

→DML: Linguagem interativa de manipulação de dados.

Outra vantagem da SQL que ela é uma linguagem similar ao inglês, facilitando assim o entendimento dos comandos.

4.2 INSTRUÇÕES SQL

A linguagem SQL possui muitas instruções. Vamos ver algumas que são consideradas principais.

→**SELECT** –Recupera dados do banco de dados. Veja sua utilização:

```
SELECT * FROM alunos;
```

→**INSERT** – Insere linhas. Veja sua utilização:

```
INSERT INTO DEPTO VALUES (1,'TPD', 'FEMA"Danilo Matioli',);
```

→**UPDATE** – Altera linhas. Veja sua utilização:

```
UPDATE alunos,  
SET materia = 4
```

→**DELETE** – Deleta linhas.

```
DELETE FROM alunos
```

```
WHERE idade = 18
```

→**CREATE** – Criar estruturas ou tabelas. Veja sua utilização:

```
CREATE TABLE ALUNOS
```

→**ALTER** – Altera estruturas ou tabelas. Veja sua utilização:

```
ALTER TABLE alunos
```

```
DROP COLUMN nota4
```

→**DROP** – Elimina estruturas. Veja sua utilização:

```
DROP COLUMN depto;
```

→**RENAME** – Renomeia estruturas. Veja sua utilização:

```
RENAME depto TO departamento
```

Essas são algumas instruções SQL que podem ser utilizadas em vários bancos como Oracle, por exemplo.

4.3 CONTROLANDO ACESSO AO BANCO DE DADOS ORACLE SERVER

Quanto maior um banco de dados for, mais dados ele possui. Quando uma empresa possui muitos funcionários, mais usuários farão acesso ao banco, pois o objetivo de um banco de dados é atender as necessidades dos usuários e da empresa. Isso deve ser controlado para que a segurança do banco não seja comprometida. Todo banco de dados pode possuir sua própria segurança. O banco de dados Oracle, por exemplo, possui mais de 80 tipos de privilégios. Com a segurança do banco de dados Oracle você pode:

→Controlar os acessos ao banco de dados

→Confirmar privilégios concedidos e recebidos

→Conceder acesso a objetivos específicos

→Retirar a permissão de um usuário específico ou retirar de um grupo específico,

Os usuários não têm permissões de alto nível. As permissões de alto nível geralmente ficam para o DBA. Dentre os seus privilégios de alto nível ele pode:

- Criar novos usuários
- Remover Usuários
- Remover Tabelas
- Criar Tarefas
- Fazer backup de tabelas

Com este privilégio de criar usuários, o DBA pode criar no banco um usuário novo para cada funcionário que entra na empresa e excluir o funcionário que sai da empresa.

Veja um exemplo de comando SQL para se criar um usuário:

```
CREATE USER Danilo.Matioli  
IDENTIFIED BY 25574DDDbb@;
```

Após o usuário ser criado, o DBA irá dar privilégios para o usuário criado. Esses privilégios não podem ser de alto nível, pois estes ficaram para o DBA para facilitar a administração e ajudar na segurança do banco. O usuário só terá privilégios como, por exemplo:

- Conectar-se ao banco
- Criar tabelas em seu esquema
- Criar Seqüência no seu esquema
- Alterar estruturas no seu esquema

O usuário comum não poderá criar outros usuários, excluir usuários ou alterar usuários, pois isto cabe ao DBA. Ela poderá, por exemplo, alterar a sua própria senha, basta inserir o seguinte código no Oracle:

```
ALTER USER Danilo.Matioli  
IDENTIFIED BY 7895411DD@#;
```

4.4 RECUPERAÇÃO BASEADA EM LOG

Em um banco de dados, ocorrem modificações a todo instante, pois há muitos usuários utilizando o banco de dados ao mesmo tempo o dia todo. Existe uma estrutura que registra as modificações no banco de dados que é conhecida como log. Log nada mais é que uma seqüência que registra todas as atividades de atualização no banco de dados.

Neste, geralmente sempre aparece o valor antigo e o novo valor. O identificador e transação e o identificador de item de dados. Toda vez que uma transação realiza uma escrita é de extrema necessidade que o registro de log seja criado antes que as informações sejam mandadas para o banco, podendo assim emitir para o banco ou se depois desejar, desfazer esta alteração. Caso precise desfazer, isso é feito utilizando o campo de valor antigo, voltando assim o seu valor original.

O log sempre deve residir no armazenamento estável e deve conter o registro completo de toda atividade do banco de dados.

Mas todas essas mudanças sendo armazenados, os valores do log podem chegar a ficar muito grande, ocupando assim muito espaço. O log deve ser varrido, de trás para frente, pois assim será apagada a alteração mais antiga e mais recente não, pois caso a mais recente seja apagada, os logs não terão lógica.

5 SEGURANÇA DE UM BANCO DE DADOS

5.1 RECUPERAÇÃO E BACKUP

Todo banco de dados deve ser mantido seguro para que nada aconteça com os dados. Quando falamos em segurança não estamos simplesmente falando somente de alteração de dados ou remoção de dados. Precisamos pensar grande.

Um banco de dados está sujeito a danos a todo o momento. Por isso, políticas de recuperação e backup são necessários para garantir a segurança dos dados.

A recuperação de um banco de dados é muito simples quando temos o banco salvo para restauração. A Recuperação e backup nada mais é que uma forma de restaurar os dados no seu estado anterior (no caso o último que você tem salvado e serve).

Mais abaixo, vamos estudar casos. Neste estudo de caso vamos verificar o porquê o backup é tão importante.

No nosso caso vamos estudar o banco da Casa DI Conti. O banco de dados da empresa possui um tamanho total de 4 TB, sendo que o espaço ocupado é de aproximadamente 3 TB e livre 1TB. Esses dados do banco de dados ficam salvos em um servidor na sala de informática da empresa, trancados em um “cofre” (na verdade uma sala fechada com senha para acesso). O lugar é considerado seguro. Mas, caso uma explosão intencional ou o lugar comece a pegar fogo, o banco será muito danificado (possivelmente perdido) e deveremos estudar essa possibilidade, devendo assim ter o backup em outro local salvo para restaurar o estado anterior do banco.

A empresa possui um “robô” (servidor de backup adquirido da HP) que faz todo dia o backup deste banco, que apesar de grande, é feito backup dia-dia.

Mas como funciona?

Dois tipos de backups são feitos. Todo dia (backup só de pastas e planilhas importantes que dá 300 GB) e de todo o banco de dados no fim de semana.

O backup diário é importante e não é feito para todo o banco. Mas a frente no estudo de caso vamos mostrar uma solução para isso.

O backup feito todo dia é feito pelo robô já programado tudo automaticamente.

Funciona assim. O responsável pelo backup deve pegar a fita mais “antiga” (que possui os dados mais velhos) e formatá-la, deixando assim livre dentro do servidor de

backup. Sendo assim, em uma hora determinada do dia, se a fita tiver lá e com espaço, ele começa a fazer a cópia dos arquivos.

Após a operação terminar, o responsável retira a fita do local para que mesmo que aconteça algo sinistro, pelo menos os dados estarão salvos.

Já o backup de todo o banco é feito no final de semana, geralmente no sábado.

O backup de 3 TB é um pouco mais demorado. Geralmente estes tipos de backup de todos os dados levam aproximadamente 12 horas.

Funciona quase da mesma forma que o backup anterior, mas aqui é bem maior e bem mais demorado.

O backup dos dados também é feito pelo robô em fitas e cada fita possui um tamanho de 800 GB (menos que um TB, mas bem próximo).

Por isso, o robô é capaz de receber até 12 fitas de 800 GB. No nosso caso, como o banco de dados possui 3 TB, não serão necessárias 12 fitas.

Sendo assim, a empresa possui 2 jogos de fitas. Cada jogo tem 6 fitas.

O responsável pelo backup do banco de dados pega um jogo de fitas (com 6 fitas), coloca no servidor e deixam todas elas formatadas. O restante é o servidor que faz tudo automático. Após as fitas estarem no local e formatada, ele no sábado, há certa hora programada, começa a fazer o backup. Caso não de erros, o backup será feito em aproximadamente 12 horas. Caso de erro, assim que percebido, deverá se fazer um novo backup o mais breve possível. Após terminar o backup, as fitas são retiradas do servidor de backup e são armazenadas em outro local distante do banco, isso tudo pensando na segurança dos dados, pois caso aconteça algo sinistro na sala, seus dados estarão a salvos longe dali.

Mas vamos ver ainda no estudo de caso que mesmo assim o banco ainda contém algumas falhas de segurança. Por exemplo, fazer o backup só no sábado não é o suficiente, pois temos dois jogos de fitas e se precisar voltar, as chances de erro podem ser grandes. Mas abaixo no estudo de caso, vamos mostrar outra solução para este problema, pois caso o banco dê problema na sexta feira, só teremos backup dos dados de 6 dias a traz, isso se não der problema na hora de voltar o backup.

Hoje outro problema das empresas é que elas não levam o backup tão a sério quanto deveriam levar, pois um servidor de banco de dados geralmente não dá problema, principalmente se for novo e de qualidade boa.

Por isso nossa contribuição com este trabalho será de mostrar falhas que a empresa comete e mostrar possíveis soluções para este problema.

5.2 BACKUP DO BANCO DE DADOS É NECESSÁRIO

Como vimos à cima, na empresa Casa Di Conti o backup é feito, mas só final de semana. Semanalmente, nela só é realizado o backup de 300 GB de informações e mesmo assim ainda ocorrem falhas na segurança. Vamos verificar juntos algumas falhas que a empresa possui.

De imediato, deveríamos ter pelo menos cinco jogos de fitas, sendo que cada jogo deveria possuir 6 fitas de 800 GB para o backup.

Tudo isso para garantir a segurança. Todos esses jogos iriam ser ótimos, pois o backup em um jogo de fita só, não é seguro.

Vamos entender uma falha:

Segunda feira, dia 1 de novembro de 2010 todos os funcionários da empresa chegam para trabalhar, jogam informações no sistema (incluem funcionários, dão baixas em contas recebidas, contas a pagar, alteram dados de cliente, etc.). Isso a todo o momento. Sendo assim, terça, quarta, quinta, sexta e sábado também acontece isso a todo o momento. O backup é feito no sábado em um jogo de fitas, o jogo de FITAS1. Domingo, não tem alteração no banco, pois o pessoal não trabalha. Próxima segunda feira, os funcionários fazem a mesma rotina, alteram dados, incluem dados e fazem alterações a todo o momento no sistema. Chega sábado, novo backup feito no JOGO DE FITAS1.

Até aí, tudo ótimo, funcionando OK e sem problemas. Aí sábado (no caso o terceiro sábado do mês), vamos ter que fazer um novo backup. Para isso, temos que formatar o jogo de fitas1, conteúdo o backup mais antigo. Sábado, formatamos e ficamos com apenas 1 backup, que é o backup da FITA2. Sendo assim, apagamos a fita 1 e dispparamos o novo backup. Segunda feira, tudo ok. Mas sexta feira, por exemplo, deu pane e o banco ficou danificado. O que fazer?

Na mesma hora temos vários problemas. Dentre eles temos:

- Pane no banco de dados: Por que deu pane?
- Perdemos os dados, vamos voltar o backup e tudo será resolvido.
- Temos apenas 1 backup e ele pode conter erros.

Resumindo. A pane no banco de dados, não poderia ter acontecido. Como aconteceu? Devemos verificar o que aconteceu e por que aconteceu, onde sendo assim, tivemos falhas.

Em segundo lugar, apenas dois backup em mãos, um de semana passada e outro um pouco mais atual, mas mesmo assim sem os dados de segunda, terça, quarta e quinta feira.

Veja o tamanho do problema. Dois backups em mão é muito pouco também. Caso um deu problema na hora de fazer e o outro fez com erros, estamos com um problemão. No estudo de caso, vamos entender melhor como isso funciona e vamos verificar soluções para este problema.

5.3 COMO FAZER O BACKUP DE UM BANCO DE DADOS

Como vimos na empresa Casa di Conti, o backup é feito, mas deveria ser aperfeiçoado.

Como o backup demora mais ou menos 12 horas, isso seria possível fazer diariamente, por exemplo, das 18h00min às 06h00min do próximo dia.

Para isso, seria necessário investir em mais jogos de fitas, pois assim teria várias chances, pois mesmo com o backup em mãos, é possível ele dar erros na hora de restaurar.

Para isso, poderíamos ter mais jogos de fitas, pelo menos cinco jogos. Sendo assim, teríamos pelo menos cinco backups em mãos para que se for necessário voltar o backup, temos cinco chances.

A segurança de um banco de dados deve ser levada a sério, pois perder informação é perder dinheiro, tempo e muito mais.

No estudo de caso vamos mostrar a solução para este tipo de problema e entender como isso poderia ser aperfeiçoado.

Sendo assim, vamos mostrar que nosso trabalho contribuiu para ajudar a manter o banco de dados seguro.

Uma maneira correta de se fazer o backup seria:

Começa a semana. Segunda feira, 17h50min a empresa termina suas atividades utilizando o sistema e o banco de dados. Um pouco antes, nosso DBA responsável pelo backup, pera o jogo de fitas 1 e coloca no servidor. Formata todas elas e deixa programado para o backup começar às 18:00. Assim que começar o backup, ele

também pode ir embora. Na terça, pela manhã, os funcionários irão utilizar o sistema e o banco de dados normal. O DBA deverá verificar se o backup foi feito e se não houve falhas. Caso seja feito e não houve falhas, retirar as fitas, ticar nelas o dia que foi feito o backup, e guarda-las longe do servidor, em local seguro, pois se pegar fogo no banco, temos os dados salvos. Caso pegue fogo nas fitas, temos o banco de dados ainda inteiro. Isso é só um exemplo de algo sinistro que poderia acontecer.

Assim, terça, quarta, quinta e sexta ele deverá fazer o backup. Então, até sexta tudo ok. Sábado, ele deverá pegar a fita de segunda e formatá-la. Mas mesmo assim, ele terá o backup de terça, quarta, quinta, sexta e logo mais o de sábado no lugar do backup de segunda.

O backup dos dados (os 300 GB de planilhas e outras informações fora do banco) deverá ser realizado na hora do almoço, por exemplo, pois este backup é bem mais rápido e precisa de apenas 1 fita. Isso deverá ser feito diariamente.

Sendo assim, estamos melhorando a segurança de nosso banco de dados.

5.4 GERENCIAMENTO DE TRANSAÇÕES

A todo o momento um banco de dados está em uso e suas transações não param de acontecer. Por isso, é necessário gerenciar as transações que ocorrem no banco de dados.

Segundo o autor Henry Korth uma transação é uma coleção de operações que desempenha uma função lógica única dentro de uma aplicação do sistema de banco de dados. Cada transação é uma unidade de atomicidade e consistência. Assim as transações não podem violar nenhuma das regras de consistência dos bancos de dados. Resumindo entende-se que o banco de dados deve estar “consciente” do que vai acontecer, antes e depois.

Então é de responsabilidade do programador definir o modo mais apropriado para as diversas transações, e assegurar que as propriedades de atomicidade e durabilidade ocorram.

Apesar de tudo, uma transação pode não se completar com sucesso. Se realmente tivermos empenhados em garantir a atomicidade, uma transação incompleta não poderá afetar o estado do banco de dados.

O sistema de banco de dados é responsável por detectar as falhas e recuperar o estado do banco de dados, garantindo o seu retorno a seu último estado consistente. Mas devemos ficar atentos com a consistência do banco de dados. Muitas transações atualizando o banco de dados ao mesmo tempo, elas podem violar a consistência dos dados. Para evitar isso, é de extrema importância o gerenciador de controle de concorrência. Ele é quem vai controlar a interação entre as transações concorrentes de modo a garantir a consistência dos dados.

Acima estamos falando de um banco de dados complexo, utilizado geralmente por empresas.

Os sistemas de banco de dados projetados para o uso em computador pessoal não podem apresentar todas essas funções. Por exemplo, muitos sistemas pequenos não permitem o uso simultâneo do banco de dados por várias pessoas, somente por um usuário.

Outros bancos deixam a tarefa de backup para o usuário, pois o banco de dados é menor e possui menos funções.

Neste caso o próprio usuário é o responsável pelo banco de dados. Ele é quem deve garantir a segurança dos dados e realizar os backups conforme o necessário. Mas neste caso do banco de dados para uso em computadores pessoais é simples. O usuário do banco de dados deve estar consciente de que o backup é necessário e deve fazer o backup constantemente. O backup deste tipo de banco de dados é simples e rápido, fácil de fazer, pois o banco nem é muito grande. Já no banco de dados de uma empresa, o tamanho do banco já é maior, o banco possui mais funções e os usuários não conseguem fazer o backup. A administração de todo este banco da empresa cabe ao administrador de banco de dados.

No caso do banco de dados de uso em computadores pessoais, tudo é mais simples, pois este tipo de produto está voltado a administração de pequenos volumes de dados, exigindo poucos recursos. Apesar do pequeno custo para se ter, este tipo de banco de dados não servem para atender as necessidades de uma empresa.

6 EXEMPLOS DE BANCO DE DADOS

6.1 TIPOS DE BANCO DE DADOS

Existem vários tipos de banco de dados. Dentre eles temos:

→ORACLE – Criado pela Oracle Corporation

→MYSQL – Criado na Suécia em 1955

→SQL Server – Criado pela Microsoft

→Sybase – Surge em 1984

→DB2 – Surge em 1983

6.2 ORACLE

Oracle Corporation é uma companhia que desenvolve softwares corporativos. O seu principal produto é o sistema de gestão de bancos de dados relacionais chamado Oracle. Foi Fundada em 1977 e possui escritórios em mais de 155 países. Larry Ellison junto com os co-fundadores BoB Miner e Ed Oates, fundaram a empresa. A Oracle é uma empresa de software a desenvolver software empresarial habilitado para Internet e suas linhas de produtos como banco de dados, aplicativos empresariais e ferramentas para desenvolvimento de aplicativos e suporte a decisões. A Oracle é o principal fornecedor de software para gerenciamento de informações e atualmente a segunda maior empresa de software independente do mundo.

O ORACLE, SGBD da Oracle Corporation é líder de mercado.

6.3 MYSQL

O MYSQL, assim como o Oracle, é um sistema gerenciador de banco de dados. Ele utiliza a linguagem SQL como interface. Foi criado na Suécia por Michael Widenius na companhia suíça TcX. Em 25 de maio de 1955 sai a primeira versão do MYSQL.

Entre os principais usuários do MYSQL destacamos NASA, banco Bradesco, Nokia, Sony e HP.

Principais características:

- 🚦 Multi-plataforma, portanto suporta diferentes plataformas: Win32, Linux, FreeBSD, Unix, etc...

- ✚ Suporte a múltiplos processadores
- ✚ Um sofisticado sistema de senhas criptografadas flexível e Seguro.
- ✚ Código fonte escrito em C e C++ e testado com uma variedade de diferentes compiladores
- ✚ As tabelas criadas podem ter tamanho de até 4 GB
- ✚ Banco de dados de código aberto e gratuito
- ✚ O Cliente conecta no MySQL através de conexões TCP/IP.
- ✚ Capacidade para manipular bancos com até 50 milhões de registros
- ✚ Reduz a administração, engenharia e a sustentação custa por até 50%

Um produto como o SGBD MySQL exerce tão bem sua função e ainda é gratuito. Essa talvez é uma das principais vantagens do MYSQL.

Resumindo o MySQL, por sua vez, tem como foco a agilidade. Assim, se sua aplicação necessita de respostas rápidas e não é complexa, o MySQL é uma escolha muito interessante, pois sua otimização permite velocidade alta de processamento e tempo curto de resposta.

6.4. SQL SERVER

Também é um SGBD. Foi criado pela Microsoft, em parceria com a Sybase em 1988. Em 1944 houve o fim da parceria e a Microsoft continuou a aperfeiçoar o produto.

O SQL Server é um sistema de gerenciamento de bancos de dados cliente/servidor de alto desempenho com alta integração com o Windows NT. Suas características são:

Integração com os serviços de *multithreading* [múltiplas linhas], agendamento, Monitor de Desempenho, e log de eventos do Windows NT. Um usuário pode se conectar ao SQL Server com a mesma senha usada para a rede Windows NT.

O SQL Server possui várias ferramentas de administração. Dentre elas temos:

→ *Enterprise Manager*: Gerencia vários servidores permitindo executar qualquer tarefa relacionada ao SQL Server.

→• *Service Manager (SQLMANGR.EXE)*: permite iniciar, pausar, continuar e parar ("finalizar") os serviços do SQL Server

→ *Profiler (SQLTRACE.EXE)*: permite monitorar toda a atividade do servidor e registrar essa atividade em arquivos de log, incluindo comandos SQL executados pelo servidor

→ *Uninstall SQL Server 7.0*: permite que você remova a instalação existente do SQL Server 7.0

6.5 SYBASE

Surge em 1984 onde Mark Hoffman e Bob Epstein criam a Sybase na residência do Sr. Epstein em Berkeley, na Califórnia.

A Sybase em um determinado momento chegou a unir-se com a Microsoft e compartilharam seus códigos de servidores de banco de dados.

Em 2000, Sybase foi a primeira empresa a apresentar um servidor de aplicações J2EE.

A sybase é uma empresa que produz serviços e produtos relacionados ao gerenciamento de informação.

6.6 DB2

DB2 é um sistema gerenciador de banco de dados relacionais. Foi produzido pela IBM e foi lançado em 1983.

No início o produto teve o nome de System R. O projeto do DB2 teve início na década de 70.

Por muitos anos, o DB2 foi feito exclusivamente para rodar nos mainframes da IBM. Posteriormente, a IBM produziu o DB2 para rodar em outras plataformas, como Windows e Unix, para então colocar no Linux.

Nesta época, DB2 e oracle disputavam a ponta no mercado, onde os dois eram muito bons. Entretanto, havia outros como o Microsoft SQL que não ficavam atrás não.

O DB2 pode ser administrado tanto em uma interface de comandos de linhas ou em um ambiente gráfico.

6.7 POSTGRESQL

PostgreSQL é um banco de dados relacional orientado à objetos. O PostgreSQL é um banco de dados gratuito. É possível utiliza-lo em vários sistemas operacionais como o Windows e Linux.

O PostgreSQL teve seu início na University of California at Berkeley, no ano de 1986, onde Michael Stonebraker liderou um projeto para a criação de um servidor de banco de dados relacionais, chamado de Postgres.

6.8 MICROSOFT ACCESS

O Microsoft Access (Microsoft Office Access), também conhecido por MSAccess, é um sistema relacional de administração de banco de dados. Criado pela Microsoft, ele foi incluído no pacote Microsoft Office Professional, onde assim que você instala o Pacote, o Microsoft Access instala também. É possível também com o pacote todo em mãos, instalar somente o Microsoft Access.

O Microsoft Access possui compatibilidade com o SQL, onde consultas podem ser feitas através de comandos SQL.

A função "cortar e colar" (cut and paste) do Access pode torná-lo uma ferramenta útil para a conexão entre diversos bancos de dados (por exemplo, entre o Oracle e o Microsoft SQL Server durante conversões de dados ou bancos de dados).

Access disponibiliza várias funções de exportação e importação (import and export), que permitem a integração entre o Windows e outras aplicações de plataforma

7 ESTUDO DE CASO E CONCLUSÃO FINAL

7.1 ESTUDO DE CASO

Nosso trabalho vai estudar a Casa Di Conti, empresa de Cândido Mota.

Como vimos à cima, a empresa possui um banco de dados de aproximadamente 3 TB. Esse banco é importante para a empresa. Sem ele, muitos dados necessários para tomadas de decisões e muito mais, serão perdidos. Isso não pode acontecer em hipótese alguma.

A empresa faz dois tipos de backups como vimos mais acima. O primeiro é feito backup das principais planilhas, que dão aproximadamente 300 GB.

O outro é feito semanalmente. Esse que é feito no sábado é o do banco de dados completo, de três TB, feito e armazenados em fitas.

Como sabemos nossa principal contribuição com este trabalho será de mostrar falhas que a empresa comete na segurança do banco de dados e mostrar soluções para este problema.

O banco de dados da empresa é Oracle. Os usuários ficam conectados nele em horário comercial (das 7:30 às 12:00 das 13:30 às 16:00), onde a todo o momento fazem mudanças no banco (cadastro de clientes, alterações, mudanças e outros).

Essas alterações no banco são feitas por todos os usuários que tem acesso ao banco.

Um banco de dados de três TB possui muita informação e não pode ser perdido em hipótese alguma.

O principal backup da empresa deve ser concentrado nesses dados que ficam no servidor de banco de dados.

Para fazer o backup desses dados, a empresa tem um “ROBO” da HP. Esse robô é um servidor responsável pelo backup do banco de dados da empresa.

Esse backup de todo o banco de dados leva aproximadamente 12 horas e é feito de sábado. Está aí um dos problemas graves na segurança do banco de dados da empresa.

Como é possível perceber, o banco de dados recebe mudança de segunda à sexta constantemente, e também aos sábados. Quando é feito o backup do sábado, ele fica salvo nas fitas de backup (casa fita possui 800 GB e são 2 jogos de fitas). Aí está um problema. Como este backup demora doze horas, é possível

faze-lo diariamente. Para isso acontecer é necessário ter espaço para salvar os dados. Espaço é mais um problema que a empresa possui. A empresa possui apenas dois jogos de fitas e cada jogo possui seis fitas.

A primeira hipótese a ser analisada é:

Primeira semana do mês de outubro. A empresa trabalha todos os 6 dias (de segunda à sexta) e o backup é feito de tudo isso, mas apenas no sábado.

Segunda semana do mês de outubro. A empresa trabalha os seis dias e o backup é feito no sábado.

Ai vem a hipótese: E se a empresa trabalha a terceira semana até sexta e sexta o banco corrompe arquivos e precisa ser restaurado? O Que acontece?

Primeiramente, vamos perder os dados de segunda, terça, quarta, quinta e sexta (pois o backup não foi feito e ia ser feito no sábado.)

Segundo problema. Temos dois backups. Caso de problema ao voltar o banco, o que fazer?

Logo percebemos uma falha muito grande que ocorre na empresa. É muito pouco você ter em mãos apenas dois jogos de fitas com backups e ainda fazer backup apenas finais de semana.

Deveria se ter mais jogos de fitas, pois assim teria mais chances de voltar um backup, caso necessário.

O backup ser feito somente de sábado também é uma falha na segurança e que deve ser corrigida pelo DBA da empresa.

Uma solução para a segurança do banco de dados da empresa é se adquirir mais jogos de fitas, pelo menos uns cinco jogos de fitas.

Depois de ter as fitas, fazer o backup diariamente, afinal o backup é feito em doze horas, basta apenas colocar as fitas no servidor, formata-las e programar o backup. Depois o DBA deve conferir para ver se a formatação ficou OK e deixar tudo pronto para o backup ser realizado de madrugada.

Depois pela manhã, o DBA deve verificar se o backup foi feito sem erros.

Sendo assim, isso pode ser feito de segunda à sábado, onde de segunda à sexta pode ser feito de madrugada e sábado durante à tarde, pois não haverá mais alterações no banco.

Sendo assim, temos backups de todos os dias e temos mais chances de voltar o banco caso seja necessário.

Portanto, vimos que nosso trabalho visa verificar os problemas na segurança do banco de dados da empresa e dar opções para a solução do mesmo.

Depois que for realizado o backup, temos que pensar em hipóteses sinistras como o servidor pegar fogo, por exemplo.

Caso o servidor pegue fogo e perca os dados (que será bem lógico), deveremos ter no mínimo o backup do banco em mãos.

Por isso, ao analisar está hipótese que é possível acontecer, o que fazer para garantir a segurança dos dados?

Depois de realizado o backup nas fitas, pegar as fitas, retirar do servidor backup, tancar nelas a data do backup, dia e hora, e retirar da mesma sala que fica o servidor e armazenar em outro lugar seguro e próprio, pois não adianta fazer o backup e deixar ao lado do servidor, pois em casos como este, perderíamos todo o banco e todo o backup.

Por isso, fazer o backup e deixar em outro local seria outra solução para garantir a segurança dos dados do banco de dados.

Outro backup feito são as planilhas e documentos que a empresa possui, que possui mais ou menos o 300 GB.

Esse backup é bem mais rápido e gasta aproximadamente duas horas. Mesmo sendo bem menos que o banco de dados, é necessário fazer o backup destes dados que são importantes para a empresa.

Para garantir a segurança, devemos fazer o backup diariamente. Pode ser feito na hora do almoço, onde o procedimento seria:

→Formatar uma fita (caso esteja sem espaço, pois 800 GB dá para colocar dois backups na fita.)

→Inserir no servidor de backup

→Programar a hora do backup

→Esperar e verificar se realizou com sucesso.

Esse backup deverá ser feito diariamente também, e devemos ter fitas também para fazer este.

Como a sugestão para o banco era de cinco jogos de fitas, para este caso, um jogo é ótimo.

Para concluir, devemos entender que nosso trabalho visa verificar as falhas na segurança e mostrar soluções, onde sendo assim, nosso trabalho irá contribuir para que a segurança do banco de dados seja garantida a todo o momento.

7.2 CONCLUSÃO

Sistemas de banco de dados é um sistema de armazenamento de dados baseado em computador, isto é, um sistema cujo objetivo global é registrar e manter informação.

Um banco de dados é compartilhado, pois pode ser imaginado como uma unificação de diversos arquivos, onde eles têm que ser distintos, evitando-se assim a redundância de dados para evitar problemas como muito espaço ocupado no banco desnecessariamente.

Todos os departamentos devem ter acesso ao banco de dados, mas cada usuário deve ter acesso somente o que lhe é permitido para assim não prejudicarmos a segurança do banco de dados.

O principal objetivo de um banco de dados é atender as necessidades de uma organização e de seus usuários, além é claro de armazenar dado.

O banco de dados deve ser “flexível”. Esta flexibilidade deve existir, pois a cada nova necessidade deve haver uma nova solução.

Outro objetivo é garantir a segurança dos dados e das transações. Um banco de dados deve ser seguro. Ele também deve ser rápido para fazer consultas, alterações, facilitando assim as tarefas diárias dos usuários.

O banco de dados também tem como objetivo armazenar dados para que esses dados possam ser processados para gerar informação.

Sua principal vantagem é o controle centralizado dos dados. Quando há o controle centralizado dos dados, a redundância é diminuída e pode chegar a zero, basta o controle ser rígido.

O banco de dados deve garantir a integridade dos dados, a restrição de acesso não autorizado, recuperação, backup dos dados e o compartilhamento dos dados.

A independência dos dados é fundamental. A independência dos dados permite que possa ser feitas alterações sem mudar a estrutura da aplicação.

Essas mudanças podem ser, por exemplo, a forma de se ter acesso aos dados, onde se os dados forem dependentes, será impossível mudar a estrutura sem afetar a aplicação. Com a independência dos dados isso é possível.

Mas todo banco de dados deve possuir sua segurança. SGBD são sistemas gerenciadores de banco de dados. Um SGBD deve fornecer subsistemas de autorização e segurança o qual é usado pelo DBA para criar contas de usuários e especificar as restrições destas contas. Essas permissões podem ser dadas por grupos ou por usuários específicos.

Um sistema gerenciador de banco de dados é uma coleção de programas para acesso a dados. Ele visa proporcionar um ambiente conveniente e eficiente para a recuperação e armazenamento de informações.

Um sistema de banco de dados é projetado para armazenar um grande volume de dados.

Como o sistema é compartilhado, devemos ter um controle sobre isso.

O SGBD proporciona aos usuários uma visão abstrata dos dados, isto é, o sistema esconde determinados detalhes sobre certos dados. Isso é feito através de definições de níveis.

SGBD nada mais é que um conjunto de programas responsáveis pelo gerenciamento de uma base dos dados. É um sistema complexo que é responsável pela proteção dos dados, organização e recuperação de dados.

Veja a imagem a seguir que representa um sistema de banco de dados:

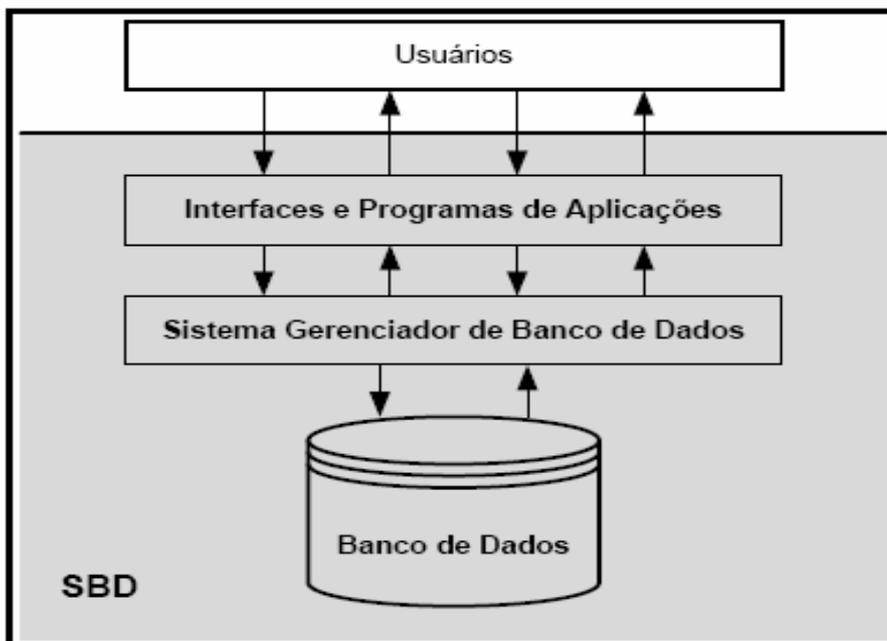


Figura 10- Representação de um sistema de banco de dados

7.2 CRONOGRAMA

Fevereiro	Escolha do orientador
Março	Escolha do tema com o orientador
Abril	Pesquisa sobre o tema escolhido
Maiο	Pesquisas e preparação do documento de qualificação
Junho	Entregar o documento de exame de qualificação para o orientador analisar
Julho	Início do desenvolvimento do projeto de pesquisa
Agosto / Setembro	Desenvolvimento do projeto de pesquisa a partir de todo o material Estudo de Caso
Outubro	Terminar o TCC e revisado e corrigido com antecedência Apresentação do TCC final para o orientador em até 1/10
29/10	Entrega do TCC no núcleo de Monografias
Dezembro	Entregar a cópia final do TCC em formato eletrônico.

7.4 REFERÊNCIA BIBLIOGRÁFICA

DATE, Christopher J.; **Introdução a Sistemas de Banco de Dados**: Editora Campus
SILBERSCHATZ, Abraham; KORTH, Henry F.; **Sistema de Banco de Dados**: Makro Books
SOUZA, Marco A.; **Oracle Banco de Dados** : Ciência Moderna
GILLENSON, Mark; **Fundamentos de Sistemas de Gerência de Banco de Dados**: LTC

7.5 REFERÊNCIA ELETRÔNICA

<http://www.mysql.com/> - Acessado dia 1/09/2010

<http://www.oracle.com/global/br/corporate/story.html> Acessado dia 1/09/2010

<http://www.oracle.com/br/index.htm> Acessado dia 2/09/2010

www.sybase.com.br Acessado dia 3/09/2010

<http://www-01.ibm.com/software/data/db2/> Acessado dia 8/09/2010