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

FÁBIO DA SILVA VIANA CAMPOS

UMA ABORDAGEM A SEGURANÇA EM BANCO DE DADOS

Assis/SP
2018

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

FÁBIO DA SILVA VIANA CAMPOS

UMA ABORDAGEM A SEGURANÇA EM BANCO DE DADOS

Projeto de pesquisa apresentado ao curso de Análise e Desenvolvimento de Sistemas do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Fábio da Silva Viana Campos
Orientador(a): Alex Sandro Romeo de Souza Poletto

Assis/SP
2018

FICHA CATALOGRÁFICA

C198u CAMPOS, Fábio da Silva Viana

Uma abordagem a segurança em banco de dados / Fábio da Silva Viana Campos. – Assis, 2018.

88p.

Trabalho de conclusão do curso (Análise e Desenvolvimento de Sistemas). – Fundação Educacional do Município de Assis-FEMA

Orientador: Dr. Alex Sandro Romeo de Souza Poletto

1.Segurança-banco de dados 2.Segurança-informação

CDD 005.8

UMA ABORDAGEM A SEGURANÇA EM BANCO DE DADOS

FÁBIO DA SILVA VIANA CAMPOS

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: Alex Sandro Romeo de Souza Poletto

Examinador: Diomara Martins Reigato Barros

Assis/SP
2018

DEDICATÓRIA

Dedico este trabalho a todos aqueles que lutam por aquilo em que acreditam.

AGRADECIMENTOS

Aos professores Alex Sandro Romeo de Souza Poletto, Diomara Martins Reigato Barros e Osmar Aparecido Machado por toda orientação e ajuda prestada durante o desenvolvimento do trabalho, sempre se mostrando muito prestativos e atenciosos.

EPÍGRAFE

“Deixem que o futuro diga a verdade e avalie cada um de acordo com o seu trabalho e realizações. O presente pertence a eles, mas o futuro pelo qual eu sempre trabalhei pertence a mim”.

Nikola Tesla

RESUMO

Esse trabalho demonstra a importância da segurança em banco de dados. Com a grande utilização de sistemas baseados em tecnologia, os Bancos de Dados são uma ferramenta fundamental paras as organizações. Um banco de dados deve ser seguro e confiável, sendo assim, proteger e garantir a segurança de uma base de dados é uma das principais tarefas do profissional conhecido como Administrador de Banco de Dados (DBA). Esses profissionais, junto com o Banco de Dados escolhido pela empresa, são responsáveis por garantir e manter a integridade, a confidencialidade e a acessibilidade dos dados e informações da organização. Esse trabalho apresenta os principais conceitos referente a banco de dados e sua segurança, abordando possíveis problemas e falhas de segurança que possam ocorrer no dia-a-dia de quem atua nessa área de Tecnologia da Informação e apontando soluções, conforme a política de segurança de informações.

Palavras-chave: banco de dados, segurança em banco de dados.

ABSTRACT

This study demonstrates the importance of database security. With the large use of technology-based systems, Databases are today a vital tool for organizations. A database must be secure and reliable. Securing and securing a database is one of the primary tasks of a database administrator (DBA). These professionals, along with the database chosen by the company, are responsible for maintaining the integrity, confidentiality and accessibility of the organization's data and information. This paper presents the main concepts regarding security and some solutions to possible problems that may occur in the day-to-day of those who work in this area of Information Technology.

.

Keywords: database, database security.

LISTA DE ILUSTRAÇÕES

Figura 1: Representação de um banco de dados..... 21

Figura 2: Representação de uma tabela de banco de dados..... 22

Figura 3: Representação de tabelas em um banco de dados relacional..... 23

Figura 4: Representação da importância dos dados, informação e conhecimento..... 25

Figura 5: Representação dos tipos de usuários de um banco de dados..... 27

Figura 6: Alguns dos SGBDs mais utilizados no mundo..... 32

Figura 7: SGBDs mais utilizados no ano de 2017..... 34

Figura 8: Os pilares da segurança da informação..... 53

Figura 9: Modelo Entidade-Relacionamento do BD de uma Loja Virtual.....74

LISTA DE ABREVIATURAS E SIGLAS

BD – BANCO DE DADOS

SGBD – SISTEMA GERENCIADOR DE BANCO DE DADOS

DBA – DATA BASE ADMINISTRATOR (ADMINSTRADOR DE BANCO DE DADOS)

SQL – STRUCTURED QUERY LANGUAGE (LINGUAGEM DE CONSULTA ESTRUTURADA)

DDL – DATA DEFINITION LANGUAGE (LINGUAGEM DE DEFINIÇÃO DE DADOS)

DML – DATA MANIPULATION LANGUAGE (LINGUAGEM DE MANIPULAÇÃO DE DADOS)

DCL – DATA CONTROL LANGUAGE (LINGUAGEM DE CONTROLE DE DADOS)

SUMÁRIO

1. INTRODUÇÃO.....13

1.1 OBJETIVOS.....15

1.2 JUSTIFICATIVAS.....16

1.3 MOTIVAÇÃO.....16

1.4 PERSPECTIVAS DE CONTRIBUIÇÃO.....17

1.5 METODOLOGIA DE PESQUISA.....17

1.6 ESTRUTURA DO TRABALHO.....18

2. BANCO DE DADOS.....20

2.1 CONCEITOS E DEFINIÇÕES SOBRE BANCO DE DADOS.....20

2.2 OBJETIVOS DE UM BANCO DE DADOS.....21

2.3 IMPORTÂNCIA DO BANCO DE DADOS.....24

2.4 TIPOS DE USUÁRIO DE UM BANCO DE DADOS.....27

2.5 SGBD, SUAS FUNÇÕES E VANTAGENS.....31

3. SEGURANÇA EM BANCO DE DADOS.....39

3.1 O ADMINISTRADOR DE BANCO DE DADOS (DBA).....39

3.2 IMPORTÂNCIA DA SEGURANÇA EM BANCO DE DADOS.....41

3.3 PRINCIPAIS ERROS COMETIDOS NA SEGURANÇA DO BANCO DE DADOS.....43

3.4 BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO.....48

4. OS PILARES DA SEGURANÇA DA INFORMAÇÃO.....52

4.1 CONFIDENCIALIDADE, INTEGRIDADE, DISPONIBILIDADE.....52

4.2 MEDIDAS DE CONTROLE.....56

4.3 PRIVILÉGIOS.....59

4.4 REDUNDÂNCIA DE DADOS.....60

4.5 INDEPENDÊNCIA DE DADOS.....61

5. LINGUAGEM SQL 63

5.1 INTRODUÇÃO BÁSICA A LINGUAGEM SQL.....63
5.2 INSTRUÇÕES SQL.....65
5.3 CONTROLANDO ACESSOS E PRIVILÉGIOS.....71

6. ESTUDO DE CASO E CONCLUSÃO.....73

6.1 ESTUDO DE CASO.....73
6.2 CONCLUSÃO.....85
6.3 REFERÊNCIAS.....88

1. INTRODUÇÃO

Primeiramente é preciso estar ciente que nos dias atuais a informação é tudo para as empresas. Informação gera lucro. Informação é dinheiro. Nós vivemos na chamada Era da Informação. A empresa que possuir informações de qualidade hoje em dia, consegue se destacar no mercado, ganhando mais agilidade, competitividade, dinamismo, eficiência e eficácia, dessa maneira, facilitando a tomada de decisões, pelos líderes do nível estratégico das organizações, que irão impactar diretamente no futuro da empresa. Uma informação útil pode ser usada a favor ou contra você ou sua empresa, dependendo de quem as usa e como as usa. É de fundamental importância para a empresa, possuir informações corretas e meios eficazes para protege-las, tendo em conta que são tão valiosas para a organização. O Banco de Dados deve ser protegido de tal maneira que se possa evitar que algum dado crítico possa ser alterado, deletado, ou divulgado sem autorização, pois isso poderia gerar grandes prejuízos tanto para a empresa, como para seus clientes e/ou usuários.

Todas as informações de uma empresa ficam armazenadas no seu banco de dados, por isso é importante entendermos o conceito de banco de dados. Segundo Date (2003, p.10) “Um banco de dados é uma coleção de dados persistentes, usada pelos sistemas de aplicação de uma determinada empresa”. Um dado é chamado de persistente, pois quando ele é inserido no banco de dados ele ficará armazenado até que ele seja deletado através de uma operação de exclusão do Sistema Gerenciador de Banco de Dados (SGBD).

A esse respeito, Date (2003, p. 10) declara:

> Mais precisamente, dizemos que os dados no banco de dados ‘persistem’ porque, uma vez aceitos pelo SGBD para entrada no banco de dados em primeiro lugar, eles só podem ser removidos do banco de dados mais tarde por alguma requisição explicita ao SGBD, e não como um mero efeito colateral de (por exemplo) algum programa concluindo sua execução.

Um banco de dados deve ser seguro e confiável. Proteger e garantir a segurança de uma base de dados é umas das principais tarefas de um Administrador de Banco de Dados (DBA).

Os bancos de dados são utilizados para armazenar diversos tipos de informações, desde dados simples sobre uma conta de e-mail até dados importantes da Receita Federal, números e senhas de cartões de crédito, etc. Se as informações são tão valiosas então elas devem ser devidamente protegidas. A segurança do banco de dados está cada vez mais em destaque com o aparecimento de novas formas de furto de informações, como o surgimento de *ransomware* que é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário. Devido ao surgimento dessas ameaças a área de segurança deve crescer e estar cada vez mais em destaque como sendo uma parte primordial nos bancos de dados das empresas.

Normalmente quando se fala em segurança as empresas se preocupam com o próprio patrimônio e não com os seus dados e com as suas informações, mas na maior parte dos casos os criminosos que cometem cibercrimes, ou crimes cibernéticos, buscam lotes de informações, com isso, principalmente as pequenas e médias empresas, que geralmente não possuem uma segurança tão rígida, são potenciais alvos desses criminosos em busca de informações que podem ser utilizadas para práticas de crimes.

Essas informações, que são tão valiosas, podem ser cadastros de clientes, que contenham informações como: números de cartões de crédito, CPF, telefones, e-mails, endereços, isto é, qualquer tipo de informação que seja útil e que possa ser usado por criminosos para cometer crimes financeiros. Devido a esses fatores, é muito importante que, além de proteger os seus próprios dados, a empresa se preocupe em proteger os dados dos seus clientes que estão gravados em seus bancos de dados e em seus servidores.

O risco de perder essas informações não pode ser desprezado, já que pode significar um grande prejuízo tanto para a empresa como para os seus clientes que tiveram suas informações violadas e furtadas. Isto pode acarretar em prejuízos a imagem e a marca da empresa além de trazer consequências graves para os seus clientes.

Levando em consideração esses fatores pode-se concluir que é de extrema importância para as empresas dar a devida atenção e o devido investimento para proteger o seu banco de dados. Não existem sistemas cem por cento seguros mas cabe aos profissionais responsáveis pela segurança do Banco de Dados, colocar o maior número de barreiras possíveis para dificultar ao máximo a invasão evitando o furto de informações sigilosas.

1.1 OBJETIVOS

Apresentar um estudo abrangente sobre segurança em banco de dados, abordando as falhas e riscos mais comuns que ocorrem nas empresas e os meios para evitar esses problemas e garantir o máximo de segurança para as informações armazenadas na base de dados. Mostrar quais são as políticas de segurança e as boas práticas que devem ser seguidas para garantir a segurança do Banco de Dados.

O uso dos computadores e da tecnologia em geral por pessoas com grande conhecimento e mal-intencionadas, (os chamados hackers) representam uma ameaça global cada vez mais presente no nosso dia a dia. Os “crimes cibernéticos”, é um termo utilizado para definir os crimes realizados no ambiente virtual por intermédio de dispositivos informáticos ligados a Rede Mundial de Computadores, popularmente conhecida como Internet.

Nesse trabalho será dado destaque aos crimes de furto de informações e acesso indevido ao banco de dados e como evitar ou minimizar essa ameaça. Será abordado no trabalho quais precauções devem ser tomadas, quais políticas de segurança devem ser adotadas e quais as boas práticas de segurança que devem ser seguidas pela empresa. De um modo geral será apresentado quais medidas de segurança são imprescindíveis para garantir a confidencialidade, integridade e disponibilidade dos dados armazenados no Banco de Dados das empresas, será abordado quais os riscos mais comuns e as falhas mais frequentes quando se trata de segurança em Banco de Dados e qual a competência do DBA com relação a esse tema.

O DBA tem um papel importante na implementação e gerenciamento da segurança de um banco de dados. De fato, ele é a figura responsável neste processo. Será abordado quais as responsabilidades do DBA relacionadas à segurança de banco de dados, quais qualificações e conhecimentos este profissional precisa ter e quais medidas devem ser tomadas para maximizar a segurança e garantir que as informações da empresa e de seus clientes estejam devidamente seguras.

Para tratar os problemas acima, foram estabelecidos objetivos de segurança que são universalmente aceitos: confidencialidade, integridade e disponibilidade.

Para proteger um Banco de Dados contra os problemas citados e garantir que os objetivos de segurança sejam cumpridos devem ser implementados 4 medidas de controle que são: controle de acesso, criptografia, controle de fluxo e controle de inferência.

O trabalho visa detalhar todas as medidas de segurança necessárias para garantir que os dados tenham a máxima proteção possível.

1.2 JUSTIFICATIVAS

É preciso salientar que muitas empresas de pequeno, médio e até mesmo empresas de grande porte, quando pensam em monitoramento e segurança, associam essas palavras com câmeras, vigias armados e proteção dos bens e patrimônio físico da empresa. Mas nos dias atuais, onde vivemos na chamada Era da Informação e Tecnologia, onde praticamente tudo e todos estão conectados à internet, apenas esse tipo de segurança não é mais suficiente.

O que muitos se esquecem é que, atualmente, as empresas produzem algo valioso e que, em muitos casos, não recebe a devida atenção da segurança: as informações e dados armazenados nos bancos de dados das empresas. Grandes corporações já sofreram ataques cibernéticos que geraram enormes custos e muita dor de cabeça para as empresas e para seus clientes.

Estamos vivendo a chamada Quarta Revolução Industrial, onde o volume e quantidade de dados e informações produzidas nunca foi tão grande. Esse volume de informações aumenta cada vez mais e se faz necessário dar a devida atenção a segurança desses dados. É fundamental que haja profissionais capacitados e qualificados para cuidar da segurança dessas informações.

Este trabalho visa abordar esses pontos, identificando as falhas mais comuns e corriqueiras na segurança do banco de dados das empresas e apontando as medidas de segurança necessárias para contornar esses problemas.

1.3 MOTIVAÇÃO

É inquestionável a relevância deste tema nos dias atuais, sendo assim é um fator motivador o aprofundamento no tema de segurança em banco de dados, não somente para o profissional DBA, mas para todos os profissionais da área de Tecnologia da Informação.

Cada vez mais surgem notícias na mídia de crimes contra empresas onde hackers furtam e sequestram dados e informações valiosas e confidências do banco de dados das empresas, de modo que esse é um tema que não pode ser ignorado e que tende a ganhar cada vez mais importância e destaque no setor de T.I.

1.4 PERSPECTIVAS DE CONTRIBUIÇÃO

Este trabalho espera contribuir para que as empresas e profissionais da área da Tecnologia da Informação tomem ciência da importância vital, de cada vez mais, darem a devida atenção a segurança das suas informações. O trabalho visa também apontar possíveis falhas de segurança na proteção do banco de dados e indicar soluções de como evitar, ou ao menos amenizar, os riscos a que estão constantemente expostos.

As empresas devem estar cientes de que se não investirem na segurança das suas informações elas ficarão para trás no mercado e além disso colocarão seus clientes, e a própria imagem e futuro da empresa, em risco. Afinal nenhum cliente vai confiar os seus dados a uma empresa que não garante a sua segurança.

1.5 METODOLOGIA DE PESQUISA

A pesquisa iniciará com um levantamento bibliográfico a respeito de Segurança em Banco de Dados. A esta primeira etapa será dada bastante importância, já que servirá de subsídio, culminando em um sólido arcabouço de conhecimento para avançar às próximas etapas, tendo em vista a busca de material bibliográfico científico sobre a problematização apresentada, bem como o desenvolvimento de estudo de caso, através da simulação de um banco de dados onde será demonstrado alguns dos principais comandos utilizados nos Sistemas Gerenciadores de Bancos de Dados, tendo como foco o controle de acesso e a concessão de privilégios aos usuários de modo a garantir a segurança das suas informações.

Será utilizado como fonte de pesquisa para o trabalho principalmente, livros, artigos em revistas especializadas no assunto, vídeo aulas, matérias publicadas em sites específicos sobre o tema, entrevistas e o quer mais for preciso para reunir o conhecimento necessário.

Em seguida serão relatados exemplos identificando os principais problemas de segurança que ocorrem nas empresas quando o assunto é segurança de banco de dados e apresentando os meios para resolve-los.

1.6 ESTRUTURA DO TRABALHO

1. INTRODUÇÃO

1.1 Objetivos
1.2 Justificativas
1.3 Motivação
1.4 Perspectivas de contribuição
1.5 Metodologia de pesquisa
1.6 Estrutura do trabalho

2. BANCO DE DADOS

2.1 Conceitos e Definições sobre banco de dados.
2.2 Objetivos de um banco de dados.
2.3 Importância do banco de dados.
2.4 Tipos de usuários de um banco de dados.
2.5 SGBD: Sistema Gerenciador de Banco de Dados, suas funções e vantagens.

3. SEGURANÇA EM BANCO DE DADOS

3.1 Perfil do DBA: Vamos falar sobre esse profissional, entender suas funções e responsabilidades como Administrador de Banco de Dados.
3.2 Importância da segurança em Banco de Dados.
3.3 Principais erros cometidos na segurança do banco de dados.
3.4 Boas práticas em segurança da informação.

4. OS PILARES DA SEGURANÇA DA INFORMAÇÃO

4.1 Os pilares da segurança da informação: integridade, confidencialidade e disponibilidade.

4.2 Medidas de Segurança e controle: controle de acesso, controle de fluxo e controle de inferência e criptografia.

4.3 Privilégios: o que é privilégio e qual sua contribuição para a segurança de um banco de dados.

4.4 de Redundância de dados

4.5 Independência de dados: Quanto menos dependente, melhor.

5. LINGUAGEM SQL - MANIPULANDO O BANCO DE DADOS

5.1 Linguagem SQL: Introdução de conceitos básicos.

5.2 Instruções SQL: principais comandos básicos utilizados em um banco de dados.

5.3 Controlando acessos e privilégios: ajuda a manter o banco de dados mais seguro.

6. ESTUDO DE CASO E CONCLUSÃO FINAL

6.1 Estudo de caso: Focando em controle de acesso e privilégios, com simulação de comandos para um melhor entendimento.

6.2 Conclusão.

6.3 Cronograma.

6.4 Referências.

2. BANCO DE DADOS

Antes de começarmos a falar sobre segurança em banco de dados, é fundamental entendermos primeiro alguns conceitos sobre banco de dados. Neste capítulo será abordado alguns assuntos cruciais para compreender o que é um banco de dados, qual o seu objetivo e importância, como um banco de dados funciona e quais os tipos de usuários de um banco de dados.

2.1 CONCEITOS E DEFINIÇÕES

Antes de começarmos a falar de segurança em banco de dados devemos entender o que é banco de dados, qual a sua função/utilidade e qual a sua importância nas empresas.

Atualmente existem disponíveis diversos tipos de banco de dados e eles estão presentes na nossa vida há muito tempo. Podemos usar como exemplo a arcaica lista telefônica, que praticamente não é mais utilizada nos dias de hoje, mas que pode ser citada como um exemplo de banco de dados, pois a sua função é armazenar informações de forma organizada para facilitar a busca feita por seus usuários.

Antigamente as empresas armazenavam informações em arquivos físicos como cadernos, cadernetas, fichas de papel, etc. Mas o surgimento e evolução dos computadores gerou uma verdadeira revolução que mudou tudo isso, possibilitando o armazenamento de dados de modo digital tornando as coisas muito mais simples, práticas e ágeis. O reflexo disso nas empresas é claro, poupa-se tempo e isso se reflete em maior eficiência e eficácia, agilizando os processos em todos os níveis organizacionais e isso é refletido em lucro para a empresa.

Segundo os autores Silberschatz et al. (2012) um banco de dados é uma coleção de dados inter-relacionados, que representam informações sobre um domínio específico.

Levando em consideração a definição de Bancos de dados podemos dizer que são um conjunto de arquivos relacionados entre si que podem armazenar informações sobre qualquer coisa como pessoas, produtos, serviços, lugares, etc.

Portanto um banco de dados são conjuntos organizados de dados com relação entre si criando sentido e transmitindo alguma informação para o usuário tornando mais eficaz uma pesquisa trabalho ou estudo.

Date (2003, p. 3) diz que “O banco de dados, por si só, pode ser considerado como o equivalente eletrônico de um armário de arquivamento; ou seja, ele é um repositório ou recipiente para uma coleção de arquivos de dados computadorizados”.

Os bancos de dados evoluíram e se tornaram o coração de muitos sistemas de informação. Não seria errado dizer que o banco de dados é a base de todo sistema de informação, pois nele é armazenado todos os dados importantes para a empresa. Essas informações que estão armazenadas no banco de dados dizem tudo sobre a empresa, quem é a empresa, quem são seus clientes, quem são seus fornecedores, quem são seus funcionários, informações sobre produtos e/ou serviços comercializados por essa empresa, estatísticas e relatórios que vão ajudar as pessoas dessa empresa na tomada de decisões.

Figura 1: Representação de um banco de dados.

Fonte: Banco de imagens Windows

2.2 OBJETIVOS DE UM BANCO DE DADOS

Agora que já entendemos o que é um banco de dados, precisamos entender também qual o seu objetivo. Date (2003) conceituou que um sistema de bancos de dados pode ser considerado como uma sala de arquivos eletrônica.

Obviamente o objetivo de um banco de dados, como o próprio nome já diz, é armazenar dados de forma organizada. E como esses dados são armazenados dentro do banco? Nos bancos de dados relacionais, que são os mais utilizados pelas empresas atualmente, os dados são armazenados na forma de tabelas. No interior dessas tabelas os dados são organizados por colunas, e em cada uma dessas colunas contém algum tipo de dado, sendo que esses dados são representados na forma de texto (*strings*, inteiros, etc.). Por exemplo: na tabela Clientes vamos ter todos os dados do cliente e esses dados ficarão organizados em colunas, cada coluna armazena um tipo de dado. No caso desse exemplo da tabela Clientes os possíveis dados poderiam ser: Nome, Endereço, Telefone, RG, CPF, data de nascimento, etc. Dentro das tabelas os dados que irão para cada coluna são guardados como suas linhas. É importante salientar também que no modelo relacional, primeiro toda a estrutura do banco de dados deve ser projetada, ou seja, antes de começar a inserir os dados é preciso primeiro criar as tabelas definindo as colunas que cada tabela irá conter. Depois que as tabelas estiverem devidamente criadas então poderemos começar a "alimentar" esse banco com dados.

Para ficar mais claro, na figura abaixo podemos ver uma representação simplista de uma tabela de um banco de dados do tipo relacional:

Clientes			
Id-clientes	Primeiro nome	Segundo nome	Telefone
01	Maria	Silva	932548267
02	José	Sousa	934189592

Figura 2 – Representação de uma tabela de banco de dados

Fonte: Banco de imagens Windows

Na Figura 2 tem-se o exemplo de uma tabela chamada Clientes, onde temos as informações necessárias divididas por coluna, tendo como colunas: id-clientes, primeiro nome, segundo nome e telefone.

Figura 3: Representação de tabelas em um banco de dados relacional.

Fonte: Banco de imagens Windows

Na Figura 3 tem-se a representação de duas tabelas sendo uma para armazenar as informações dos veículos e outra tabela para armazenar as informações dos clientes, cada tabela tendo as suas respectivas colunas e linhas.

Se for necessário deve-se criar outras tabelas para armazenar outros tipos de informações, como por exemplo uma tabela Produto, ou uma tabela Venda, ou Fornecedor, isso vai depender de cada caso e da necessidade do sistema da qual este banco de dados faz parte. Após as tabelas serem criadas deve ser feito o relacionamento (a ligação), entre elas, caso haja relação entre os dados dessas tabelas.

Vale a pena mencionar que existem bancos de dados do tipo não relacional, ou também conhecidos como NoSQL. Nesse tipo de bancos de dados a forma de se armazenar e organizar dados é diferente do modelo relacional e também é possível armazenar outros

tipos de dados como vídeos, áudios e imagens. Mas nesse trabalho vamos nos ater ao banco de dados do tipo relacional que são os mais comuns e mais utilizados pelas empresas.

Porém o objetivo de um banco de dados vai além de simplesmente armazenar os dados. Ele também precisa atender as necessidades da empresa e de seus usuários, garantir a segurança dos dados e das transações, tornar mais ágil o processo de consultas, alterações e exclusões de dados, armazenar os dados e garantir que os dados fiquem armazenados permanentemente. Esses fatores fazem com que o banco de dados seja confiável.

2.3 IMPORTÂNCIA DO BANCO DE DADOS

Importância

Nos dias atuais, com a competição cada vez mais acirrada no mercado, a empresa que não investir em tecnologia com certeza ficará para trás em relação aos seus concorrentes e provavelmente estará fadada ao fracasso. Uma das coisas mais valiosas nos dias atuais é a informação, por isso é fundamental ter sempre disponíveis informações valiosas que auxiliem as equipes responsáveis por planejar as estratégias das empresas nas tomadas de decisões, não apenas facilitando as tomadas de decisões mas também apontando os caminhos mais seguros e com menos riscos evitando ao máximo os problemas que possam levar ao insucesso das suas empreitadas.

Transformar dados em Informação e conhecimento

Primeiro é importante sabermos diferenciar o que são dados e o que é informação.

Dados sozinhos por si só não possuem significado relevante e consequentemente não conduz a nenhuma compreensão. Os dados na sua forma “bruta” representam algo ou alguma coisa que pode não fazer sentido a princípio. Apenas armazenar e acumular dados simplesmente de forma aleatória não é apenas inútil para empresa como também pode ser custoso, além de que os dados sozinhos isolados não ajudam a tirar conclusões e muito menos na tomada de decisões.

Informação é a contextualização dos dados, ou seja, é a ordenação e organização dos dados para que eles transmitam um significado, para que façam sentido e possam ser compreendidos dentro de um determinado contexto. O conjunto de vários dados devidamente contextualizados, organizados e ordenados gera informação e essa informação por sua vez pode levar a obtenção de conhecimento.

Por isso é extremante importante um banco de dados bem projetado numa empresa, para armazenar dados, que vão gerar informações que futuramente vão se transformar em conhecimento que podem refletir na maximização da eficiência, da eficácia, da agilidade e facilidade na tomada de decisões. Essas decisões serão tomadas com mais segurança, e de forma mais coesa, tudo isso irá levar a economia de tempo e consequentemente na obtenção de lucro para as organizações.

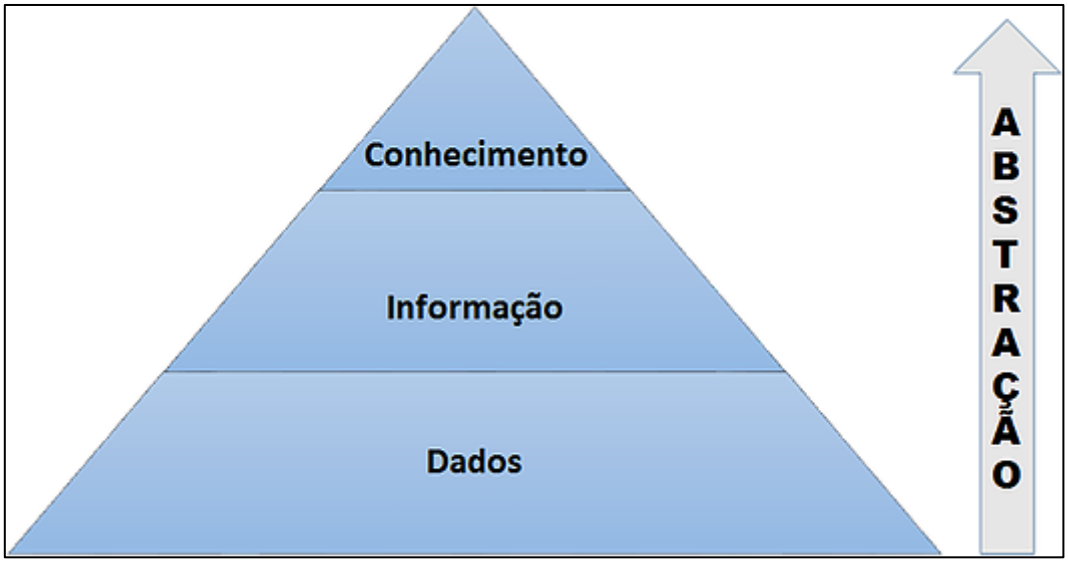

Figura 4: Representação da importância dos dados, informação e conhecimento.

Fonte: Banco de imagens Windows

Se a empresa possui um banco de dados bem estruturado ela conseguirá informações valiosas para saber exatamente o perfil dos seus clientes, de seus fornecedores, dos seus produtos e serviços, ou seja, de tudo aquilo que estiver devidamente armazenado na sua base de dados.

Essas informações vão servir para nortear várias ações da empresa, como por exemplo a capitação de novos clientes, a mudança do público alvo, uma política de promoções

personalizadas, uma campanha de marketing específica e até projetos mais ambiciosos como a expansão dos negócios em novas áreas.

Tudo isso porque essas informações, armazenadas e organizadas no banco de dados, permite a empresa saber quem é cada cliente, quais são suas preferências o seu ímpeto de consumo, quais são os produtos com a maior demanda, etc. Isso permite a empresa se adaptar a diferentes cenários e modificar suas visões, políticas e estratégias com relação ao mercado, tanto a curto como a médio e longo prazo.

É preciso ter qualidade nos dados

É importante frisar que não adianta a empresa armazenar uma quantidade enorme de dados inúteis que não servirão para nada. Muitas empresas cometem esse erro investindo uma fortuna em softwares e novas tecnologias, ferramentas e aplicativos que coletam uma infinidade de dados que muitas vezes não servirão para nada, ou por não terem pessoas capacitadas para interpretar e trabalhar com esses dados ou por simplesmente esses dados não terem qualidade.

Dito isto, é essencial que além do armazenamento adequado e organizado dos dados, deve-se conhecer como esses dados são gerados e colocados no banco, pois somente dados corretos irão proporcionar informações confiáveis que irão resultar em soluções e estratégias válidas para a empresa.

Uma grande quantidade de dados não é relevante. Nesse caso quantidade não necessariamente significa qualidade. É preciso que os dados estejam muito bem organizados, relacionados, que sejam consistentes, específicos e que sejam compreensíveis. Desse modo eles poderão, a qualquer momento, ser estudados e analisados de forma rápida e prática se transformando em informações importantes e precisas que vão gerar conhecimento. Este conhecimento gerado é que será utilizado pelos líderes das empresas, principalmente pelos diretores e presidentes, que trabalham no nível estratégico, tomando decisões que definem o futuro da empresa. Essas pessoas irão utilizar o conhecimento adquirido através da informação, para tomar decisões, que por sua vez será repassada para os funcionários, como gerentes e coordenadores, do nível tático e enfim chegará aos funcionários do nível operacional, que irão colocar em prática tudo o que foi decidido nos níveis superiores.

Tudo isso só é possível por que foi utilizado o conhecimento necessário que veio através das informações geradas pelos dados que estão armazenados no banco de dados do sistema da empresa.

É claro que o banco de dados não serve apenas para grandes tomadas de decisões pelos diretores das empresas ou para aqueles profissionais que trabalham com inteligência de negócios, mas também para o funcionamento diário da empresa, permitindo que seja possível a realização tarefas corriqueiras que fazem parte da rotina da empresa. Essas tarefas geralmente são realizadas por pessoas que trabalham no nível operacional das empresas e realizam funções como por exemplo efetuar vendas, fazer cadastros, incluir, excluir ou atualizar o cadastro de clientes, fornecedores, funcionários, produtos, serviços, realizar pesquisas, gerar relatórios, fazer controles de estoque e muitas outras coisas. Sem o banco de dados nenhum sistema de nenhuma empresa funcionaria, pois o banco de dados é a base de todos os sistemas, todo sistema começa pelo banco de dados.

2.4 TIPOS DE USUÁRIO DE UM BANCO DE DADOS

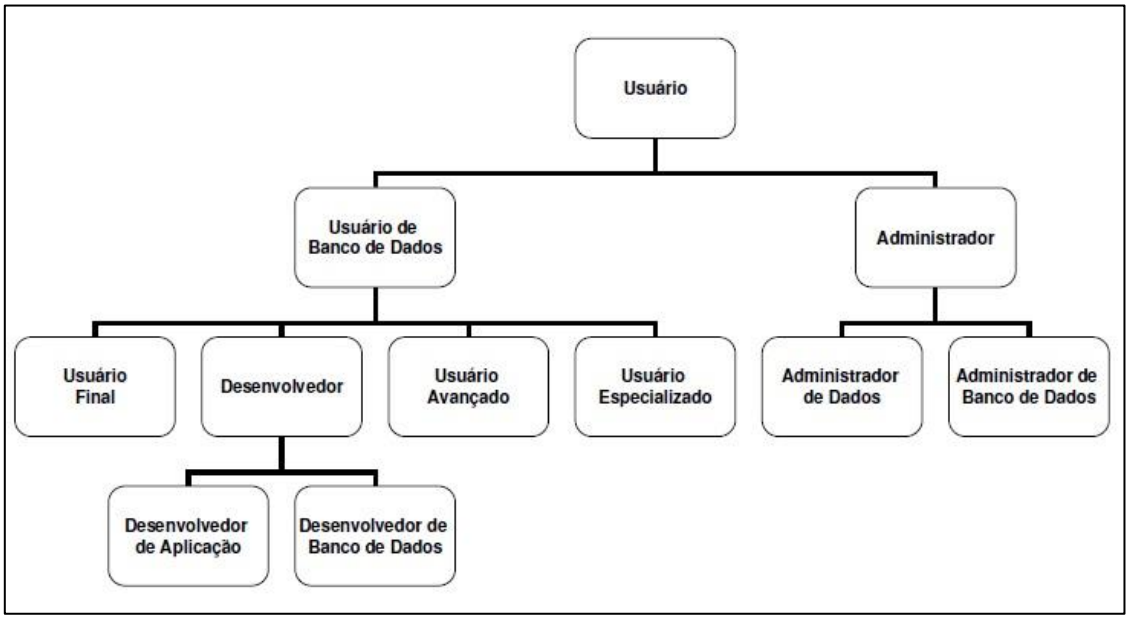

Figura 5: Representação dos tipos de usuários de um banco de dados.

Fonte: Banco de imagens Windows

Em um sistema de Banco de Dados existem muitas pessoas envolvidas, desde o projeto até a manutenção propriamente dito.

Entre estas pessoas podemos destacar os seguintes tipos de usuários:

Administrador de Dados

O Administrador de Dados (abreviado como DA – Data Administrator), segundo Date (2003) é o profissional que é encarregado de decidir quais dados serão armazenados no banco de dados e também por estabelecer as normas para manter e tratar esses dados, uma vez que venham a ser armazenados. Como já foi dito anteriormente os dados representam um dos bens mais valiosos da empresa então. Ainda segundo Date (2003, p. 15), “é imperativo que deva existir alguma pessoa que entenda esses dados e as necessidades da empresa com relação a esses dados, em um nível elevado de administração. O administrador de dados é essa pessoa”.

Pode-se dizer que o maior objetivo do administrador de dados é permitir que vários usuários compartilhem os dados corporativos. Sendo assim os dados não pertencem a nenhum sistema ou usuário especificamente, mas a organização de forma geral

Algumas características desse profissional:

- ✓ Gerenciar os dados como um recurso da organização.
- ✓ Delinear, desenvolver e propagar as bases de dados da empresa.
- ✓ Tornar possível a descentralização dos processos, mas manter os dados centralizados.
- ✓ Fazer com o acesso as informações armazenadas seja feita de maneira simples e veloz.

Administrador de Banco de Dados (DBA)

Conforme Elmasri e Navathe (2005), toda empresa que faz o compartilhamento de muitos recursos computacionais sempre vai existir a necessidade de um profissional para gerenciar esses recursos. Em um ambiente como o Banco de Dados pode-se dizer que o recurso primário seria o próprio banco de dados e o recurso secundário seria o Sistema Gerenciador de Banco de Dados.

Esse profissional de grande importância, conhecido como Administrador de Banco de Dados ou DBA (Database Administrator), segundo Elmasri e Navathe (2005), é o grande responsável por permitir a autorização de acesso ao Banco de Dados (BD) e pela coordenação e também monitoração do seu uso, além de ser também de sua responsabilidade adquirir recursos de software e hardware conforme necessário. Também é de competência do DBA definir os tipos de privilégios que cada usuário irá usufruir. É esse profissional que irá centralizar o controle dos dados e os programas de acesso a eles.

É muito importante salientar que, conforme Elmasri e Navathe (2005), o Administrador de Banco de Dados é responsável pelos eventuais problemas de quebra de segurança ou ainda problemas de baixo desempenho nos Sistemas Gerenciadores de Banco de Dados (SGBD).

Um administrador de banco de dados é responsável por várias funções referentes ao controle de um SGBD. De acordo com Silberschatz et al. (2012) as principais são:

- ✓ Definir o esquema do Banco de Dados.
- ✓ Definir a estrutura de dados e dos métodos de acesso.
- ✓ Modificar o esquema ou a organização física.
- ✓ Controlar as autorizações de acesso.
- ✓ Especificar as regras de integridade.

Projetista de Banco de Dados (DB Designer)

Esse profissional que atende pelo nome de Projetista de Banco de Dados, ou em inglês DB Designer, de acordo com Elmasri e Navathe (2005), é a pessoa responsável por identificar os dados que serão armazenados no BD. É esse profissional que irá escolher a melhor estrutura para guardar e representar esses dados, sendo que essas tarefas são, geralmente, realizadas antes que o banco de dados seja realmente implementado e alimentado com dados. Outra função do DB Designer é fazer uma avaliação das necessidades de cada grupo de usuários e criar projetos que os atendam.

Analistas de Sistema e Programadores de Aplicações

Os analistas de sistemas são os profissionais responsáveis por determinar os requisitos dos usuários finais e desenvolver especificações para transações que irão atender esses requisitos.

Os Programadores de Aplicações irão implementar essas especificações com os programas, realizando testes, depurando, documentando e dando manutenção. São profissionais, formados e capacitados que fazem a interação com o sistema por meio de chamadas DML.

Usuários Finais

Conforme Elmasri e Navathe (2005), os usuários finais são pessoas cujas profissões requerem um acesso ao banco de dados para consultas, atualização e relatórios.

Ainda segundo Elmasri e Navathe (2005), existem várias categorias de usuários finais de banco de dados que fazem operações mais simplistas nos Sistemas Gerenciadores de Banco de Dados (SGBD). Como por exemplo consultas, atualizações e geração de documentos. Esses usuários são:

- **Usuários finais casuais:** são aqueles usuários que fazem acesso ao banco de dados casualmente, sendo que podem necessitar de informações distintas a cada vez que realizam um acesso ao banco. Normalmente esses usuários são gerentes de nível médio ou elevado ou outros profissionais com necessidades ocasionais
- **Iniciantes ou usuários finais parametrizáveis:** esse tipo de usuário utiliza consultas pré-estabelecidas que já foram testadas muitas vezes. Esses usuários também são conhecidos como usuários navegantes, isto é, são usuários comuns que fazem a interação com o sistema através de interfaces pré-definidas.
- **Usuários finais sofisticados:** esse tipo de usuário já está familiarizado com o Sistema Gerenciador de Banco de Dados e por isso já são capazes de realizar consultas mais complexas. São incluídos nessa categoria, por exemplo, os engenheiros, cientistas e analistas de negócios
- **Usuários autônomos:** esses usuários mantêm um banco de dados pessoal através do uso de pacotes de programas prontos que possuem interfaces gráficas ou programas baseados em menus simples e fáceis de utilizar.

2.5 SGBD: Sistema Gerenciador de Banco de Dados, suas funções vantagens

De acordo com Silberschatz et al. (2012, p. 1) “Um sistema de gerenciamento de banco de dados (SGBD) é uma coleção de dados inter-relacionados e um conjunto de programas para acessar esses dados”.

Entre as vantagens de se utilizar um banco de dados, estão, tornar mais ágil e fácil o armazenamento e recuperação dos dados armazenados, para isso é necessário utilizar um software chamado Sistema Gerenciador de Banco de Dados (SGBD).

O Sistema Gerenciador de Banco de Dados ou Sistema de Gestão de Base de Dados (SGBD), ou Data Base Management System (DBMS) em inglês, é a ferramenta utilizada para fazer o gerenciamento da base de dados, permitindo, entre outras coisas, armazenar, criar, consultar, alterar, inserir e excluir dados em tabelas do banco de dados.

Mas essas não são as únicas funções do SGBD. O Sistema Gerenciador de Banco de Dados deve ser capaz de garantir:

- Segurança dos dados;
- Confidencialidade dos dados;
- Integridade dos dados;
- Disponibilidade dos dados;
- Controle de redundância dos dados;
- Compartilhamento de dados;
- Controle de acesso aos dados;
- Múltiplas interfaces;
- Representação de relacionamentos complexos entre os dados;
- Recuperação de falhas dos dados, caso surjam circunstancias indesejadas e/ou inesperadas.

Figura 6: Alguns dos SGBD mais utilizados no mundo

Fonte: Banco de imagens Windows

De acordo com Ramakrishnan e Gehrke (2008), fazer uso de um sistema gerenciador de banco de dados para fazer o gerenciamento dos dados possui várias vantagens, como:

- **Independência dos dados**: Os aplicativos não devem ser expostos aos detalhes de representação e armazenamento de dados, então cabe ao SGBD ocultar tais detalhes, provendo uma visão abstrata dos dados.
- **Acesso eficiente aos dados**: O SGBD utiliza possui uma variedade de técnicas para armazenar e recuperar dados de forma rápida e eficiente.
- **Integridade e segurança dos dados**: O SGBD possuiu controles de acesso para definir quais dados estão visíveis, e quais podem ser acessados e manipulados por diferentes classes de usuários.
- **Administração de dados**: Como, geralmente, os dados armazenados em um banco de dados são compartilhados por muitos usuários, centralizar a administração dos dados pode oferecer grandes melhorias. Profissionais, como o Administrador de Dados, que entendem a natureza dos dados e como são gerenciados, bem como os diferentes tipos de usuários que utilizam esses dados, são responsáveis por organizar a representação dos dados de modo que a redundância seja minimizada e ainda ajustar o armazenamento dos dados para garantir uma melhor performance na recuperação dos dados.

- **Acesso concorrente e recuperação de falha**: O SGBD é capaz de realizar o acesso concorrente aos dados de modo que os usuários podem achar que os dados estão sendo acessados por apenas um usuário de cada vez. O SGBD também tem a função de proteger os usuários dos efeitos de falhas de sistema.
- **Tempo reduzido de desenvolvimento de aplicativo**: Algumas características do SGBD, como suportar funções importantes que são comuns a vários aplicativos e possuir uma interface de alto nível, facilita e, consequentemente, agiliza o processo de desenvolvimento de aplicativos.

Em todos os sistemas de informação, presentes em praticamente todas as empresas atualmente, é necessário armazenar dados, esses dados são armazenados no banco de dados. Por isso podemos dizer que o banco de dados é a base ou o coração do sistema, pois sem ele o sistema não funciona.

O desenvolvimento de um sistema começa pelo banco de dados por isso ele é de extrema importância e merece total atenção. Um banco de dados bem projetado pode ser a diferença entre ter um sistema rápido, eficiente e eficaz ou um sistema lento e ineficiente.

Como já foi mencionado também, geralmente a informação é o bem mais precioso da empresa, pois a informação define quem é a empresa, define sua identidade, quem são seus clientes, seus fornecedores, suas estatísticas de vendas e tudo mais que possa ser importante para essa empresa tomar decisões fundamentais para o seu futuro. Por isso é de vital importância armazenar essas informações de forma permanente, organizada e segura e também que seja rápido, simples e fácil de acessar essas informações sempre que for necessário para nortear a tomada de decisões.

Todas essas ações apenas são possíveis de serem realizadas fazendo uso do SGBD, que é descrito por Date (2003, p. 8), “O SGBD é, de longe, o componente de software mais importante de todo o sistema, mas não é o único”.

Rank Jan 2017	Rank Dec 2016	Rank Jan 2016	DBMS	Database Model	Score Jan 2017	Score Dec 2016	Score Jan 2016
1.	1.	1.	Oracle	Relational DBMS	1416.72	+12.32	-79.36
2.	2.	2.	MySQL	Relational DBMS	1366.29	-8.12	+67.03
3.	3.	3.	Microsoft SQL Server	Relational DBMS	1220.95	-5.70	+76.89
4.	↑ 5.	4.	MongoDB	Document store	331.90	+3.22	+25.88
5.	↓ 4.	5.	PostgreSQL	Relational DBMS	330.37	+0.35	+47.97
6.	6.	6.	DB2	Relational DBMS	182.49	-1.85	-13.88
7.	7.	↑ 8.	Cassandra	Wide column store	136.44	+2.16	+5.49
8.	8.	↓ 7.	Microsoft Access	Relational DBMS	127.45	+2.75	-6.59
9.	9.	↑ 10.	Redis	Key-value store	118.70	-1.20	+17.54
10.	10.	↓ 9.	SQLite	Relational DBMS	112.38	+1.54	+8.64
11.	11.	↑ 12.	Elasticsearch	Search engine	106.17	+2.90	+28.96
12.	12.	↑ 14.	Teradata	Relational DBMS	74.17	+0.79	-0.78
13.	13.	↓ 11.	SAP Adaptive Server	Relational DBMS	69.10	-1.32	-14.08
14.	14.	↓ 13.	Solr	Search engine	68.08	-0.92	-7.32
15.	15.	↑ 16.	HBase	Wide column store	59.14	+0.51	+5.77

Figura 7: SGBDs mais utilizados no ano de 2017.

Fonte: DB-Engines

O SGBD dispõe de meios que, se bem utilizados pelo DBA, irão garantir a segurança ideal do banco de dados.

Segundo Casanova e Moura (1985, p.8) “O SGBD deverá, necessariamente, prover meios para definir critérios de autorização para acesso aos dados e meios para assegurar que as regras de acesso serão cumpridas”.

No capítulo seguinte iremos falar mais detalhadamente sobre esses meios que o SGBD dispõe para garantir a segurança do banco de dados.

Abaixo falaremos sobre algumas medidas de segurança, bem como, alguns objetivos que devem ser alcançados pelo SGBD:

Segurança de dados:

Segundo Silberschatz et al. (2012) “Nem todos os usuários do sistema de banco de dados devem ser capazes de acessar todos os dados”. É preciso estabelecer regras e implementar medidas de controle, como o controle de acesso de usuários, para gerenciar este tema.

Conforme Date (2003), a segurança de dados é um requisito de gerenciamento de sistemas de banco de dados que significa proteger os dados contra usuários que não possuam a devida autorização.

O Sistema Gerenciador de Banco de Dados deve ser capaz de garantir a segurança e proteger o banco de dados de acessos não autorizados. Isso é feito impondo regras que definem quais usuários tem acesso ao banco de dados, e entre esses usuários autorizados qual o nível de acesso que cada um tem dentro do banco de dados, ou seja, o que cada usuário pode fazer, quais os dados que cada um pode acessar e quais operações podem efetuar (consultar, inserir, excluir, alterar, etc).

De acordo com Ozsu e Valduriez (2001), a segurança de dados possui dois aspectos: proteção de dados e controle de autorização. A proteção dos dados é essencial para não permitir que usuários sem autorização tenham acesso ao conteúdo dos dados, tendo a criptografia como principal medida de segurança. Já o controle de autorização assegura que somente usuários devidamente autorizados possam efetuar ações que tem permissão sobre o banco de dados.

Devem ainda existir procedimentos que permitam fazer cópias de segurança e recuperar dados em caso de ocorrer alguma falha inesperada no banco de dados, podendo assim garantir a segurança e a integridade dos dados.

Confidencialidade:

O SGBD possui meios para garantir que apenas as pessoas devidamente autorizadas pelo DBA poderão acessar, visualizar e manipular os dados, isto é, o SGBD precisa assegurar que as informações armazenadas no banco de dados nunca poderão ser visualizadas e chegarem ao conhecimento de pessoas que não tenham autorização para isso. Garantir a confidencialidade é um dos princípios básicos da segurança da informação e, por consequência, da segurança de banco de dados.

Integridade:

De acordo com Date (2003, p. 17), “O problema da integridade é o problema de assegurar que os dados no banco de dados estão corretos. A inconsistência entre duas entradas que deveriam representar o mesmo ‘fato’ é um exemplo de falta de integridade”.

O Sistema Gerenciador de Banco de Dados deve assegurar a verificação das restrições de integridade afim de manter os dados validos, de modo que seja reduzido ao mínimo a redundância de dados e aumentando a consistência dos dados. Gerenciar as transações é fator de muita importância para a manutenção da integridade dos dados. Pode-se entender como transação um conjunto de ações realizadas por um usuário ou por uma aplicação.
Podemos utilizar como exemplo de transação uma operação bancária de transferência de uma quantia de dinheiro de uma conta para outra. Se por qualquer motivo essa transação sofrer uma interrupção antes de ser concluída, o SGBD deve evitar o estado de inconsistência dos dados, isso é feito acionando o *rollback*, que é uma instrução que irá desfazer o que foi feito até o momento da ocorrência do problema e retorna o banco de dados ao seu estado de consistência.

Disponibilidade:

O SGDB deve garantir que os dados estejam disponíveis para o usuário sempre que necessário, ou seja, os dados devem estar sempre disponíveis para que os usuários possam utiliza-los para exercer suas funções no âmbito da empresa. A disponibilidade dos dados é essencial para garantir que o sistema da empresa seja operacional, ou seja, para garantir que todos os funcionários da empresa, que utilizam o sistema e dependem do mesmo para exercer suas tarefas rotineiras, possam desempenhar suas funções com sucesso.

Controle de concorrência:

Segundo Casanova e Moura (1985, p. 18), “Controle de concorrência visa a garantir que, em toda execução simultânea de um grupo de transações, cada uma seja executada como se fosse a única do sistema. Isto significa que, em uma execução concorrente, transações não devem gerar interferências que levem a anomalias de sincronização”.

Nos bancos de dados com vários usuários, pode acontecer de mais de usuário tentar acessar os mesmos dados ao mesmo tempo. O Sistema Gerenciador de Banco de Dados tem um mecanismo que garante que o banco de dados seja atualizado de maneira correta, esse mecanismo é chamado de controle de concorrência.

A esse respeito Silberschatz et al. (2006, p. 427) declara:

> Uma das propriedades fundamentais de uma transação é o isolamento. Contudo, quando várias transações são executadas simultaneamente no banco de dados, a propriedade de isolamento pode não ser mais preservada. Para garantir que seja, o sistema precisa controlar a interação entre as transações simultâneas; esse controle é alcançado por meio de uma série de mecanismos chamados de controle de concorrência.

Controle de acesso:

Explicando de uma maneira sucinta, o controle de acesso é a maneira do DBA definir quem pode acessar e manipular o banco de dados. O DBA vai utilizar comandos (instruções SQL) e ferramentas do SGBD para criar usuários e definir senhas de acesso para que esses usuários possam acessar e manipular o banco e dados e também vai definir os privilégios que cada usuário irá ter, de acordo com o critério do Administrador de Banco de Dados.

A esse respeito, é preciso considerar que:

> Ao entrar no sistema (ou começar a executar, no caso de transações), haveria um mecanismo de autenticação do usuário (ou transação) estabelecendo a sua identidade perante o sistema. Finalmente, a cada acesso ao banco (ou outra unidade de trabalho mais conveniente, principalmente no caso de transações), o sistema verificaria se o usuário possui os privilégios necessários a execução do acesso. (CASANOVA E MOURA, 1985, p. 20).

Criptografia:

De acordo com Date (2003), a criptografia é o armazenamento e transmissão de dados sigilosos em forma criptografada. A criptografia é uma importante medida de segurança, pois ela garante que se os dados forem interceptados ou acessados por uma pessoa não autorizada, essa pessoa não consiga compreender as informações ao qual ela teve acesso. Criptografar os dados é o mesmo que codificar esses dados para que apenas as pessoas autorizadas possam ter acesso às informações.

Backup:

Basicamente é um mecanismo que permite criar uma cópia de segurança que possibilita recuperar dados importantes no caso de ocorrer alguma falha, acidentes, sejam eles catástrofes naturais ou por falha humana, ou qualquer tipo de imprevisto, erro, ou situação indesejada. Por isso é extremamente importante o backup estar sempre seguro e atualizado, para que no momento que for preciso utiliza-lo ele esteja pronto.

A esse respeito, Silberschatz et al. (2006, p.459) declara:

> Um sistema de computador, como qualquer outro dispositivo, está sujeito a falhas por uma série de causas: falha de disco, falta energia, erro de software, um incêndio na sala e até mesmo sabotagem. Em qualquer falha, informações podem ser perdidas. Portando, o sistema de banco de dados precisa tomar ações de antemão para garantir que as propriedades de atomicidade e durabilidade das transações sejam preservadas. Uma parte integral de um sistema de banco de dados é um esquema de recuperação que pode restaurar o banco de dados ao estado coerente que existia antes da falha.

3. SEGURANÇA EM BANCO DE DADOS

Neste capítulo será abordado sobre a figura do profissional DBA, de modo que possamos conhecer mais sobre esse importante profissional da área de T.I. Também será abordado sobre a importância da segurança em banco de dados, bem como as principais falhas e erros mais comuns quando se trata de segurança e ainda veremos quais são as principais medidas de segurança que devem ser implementadas pelo DBA para garantir que o banco de dados e as informações armazenadas nele, possam ter uma segurança adequada.

3.1 O ADMINISTRADOR DE BANCO DE DADOS (DBA)

Segundo Date (2003), o DBA é o profissional com conhecimento técnico necessário para implementar as decisões tomadas pelo administrador de dados. O DBA, diferente do administrador de dados, é um profissional da área de T.I. (Tecnologia da Informação), que tem a importante tarefa de fazer a ligação entre as funcionalidades do SGBD com os sistemas que o utilizam.

A esse respeito, Date (2003, p. 17) declara:

> Tendo jurisdição completa sobre o banco de dados, o DBA (sob orientação apropriada do administrador de dados) pode assegurar que o único meio de acesso ao banco de dados seja através dos canais apropriados e, em consequência, pode definir restrições de segurança a serem verificadas sempre que houver uma tentativa de acesso a dados confidenciais. Podem ser estabelecidas diferentes restrições para cada tipo de acesso (busca, inserção, exclusão, etc) a cada item de informação no banco de dados.

O profissional chamado de Administrador de Banco de Dados ou Database Administrator (DBA na sigla em inglês), como o nome já diz, é a pessoa responsável por administrar o banco de dados, isto é, esse profissional atua gerenciando, instalando, configurando, atualizando, otimizando e monitorando o banco de dados.

Date (2003, p.16), diz que: “O trabalho do DBA é criar o banco de dados propriamente dito e implementar os controles técnicos necessários para pôr em prática as diversas decisões

sobre normas tomadas pelo administrador de dados". O DBA também é o profissional que deve garantir que o sistema tenha um desempenho satisfatório.

Entre tantas atividades e responsabilidades que são pertinentes a esse profissional pode-se destacar algumas consideradas mais importantes:

- **Cuidar da performance**: cabe ao administrador do banco de dados garantir uma velocidade de reposta ideal do banco de dados aos aplicativos que fazem o acesso a esse banco.
- **Cuidar da segurança:** o DBA é responsável por assegurar que tanto usuários como os aplicativos tenham os acessos que são necessários para conseguirem executar suas funções. Também deve garantir que ninguém possa ter acessos indevidos para não colocar em risco a segurança do banco de dados, seja ela por meio de ataques ou invasões ou mesmo falhas humanas.
- **Recuperação de falhas:** o DBA também é responsável pelo sistema de backup do banco de dados que garante que todas as informações contidas no banco de dados estarão a salvo caso haja uma falha grave nos servidores da empresa.
- **Monitoramento constante:** Após o banco de dados ser devidamente instalado e configurado ele vai precisar ser monitorado e otimizado constantemente, por isso manutenção é extremamente importante, pois a base de dados está mudando a todo instante recebendo novas informações. Desse modo é necessário estar sempre otimizando o banco de dados para que ele não se torne lento e ineficiente.
- **Suporte:** A equipe responsável pelo desenvolvimento dos sistemas, muitas vezes não possuem conhecimentos vastos sobre as tecnologias especificas de banco de dados, sendo assim é fundamental que em toda equipe tenha um Administrador de Banco de Dados que dará todo o suporte necessário para que se obtenha um funcionamento satisfatório do banco de dados.
- **Atualização:** É necessário e completamente indispensável que haja uma atualização constante, pois sempre existem novas versões, atualizações e *patchs* de correções do SGBD sendo disponibilizadas pelos fabricantes trazendo melhorias na segurança, performance ou mesmo implementando novas funcionalidades, por isso o DBA sempre precisa estar atento e atualizado nas novidades.

Um erro que pode ocorrer em algumas empresas e em algumas equipes de desenvolvimento e achar que não é necessário a presença de um DBA, e então outros

profissionais que não são especialistas nessa área acabam fazendo o papel desse profissional. Como eles não possuem todo o conhecimento necessário e com o volume de dados e número de acessos aumentando cada vez mais, esse pode ser um erro que pode custar caro para as empresas e pode trazer muitos problemas futuros para o sistema. Por isso a presença do DBA é sempre fundamental.

É importante destacar o que dizem os autores Elmasri e Navathe (2011, p. 564) sobre segurança de banco de dados e o DBA:

> O Administrador do banco de dados (DBA) é a autoridade central para gerenciar um sistema de banco de dados. As responsabilidades do DBA incluem conceder privilégios aos usuários que precisam usar o sistema e classificar os usuários e dados de acordo com a política da organização. O DBA tem uma conta de DBA no SGBD, também conhecida como conta do sistema ou conta de superusuário, que oferece capacidades poderosas que não estão disponíveis às contas e usuários comuns do banco de dados.

Ainda segundo os mesmos autores os privilégios de superusuário do DBA incluem aqueles para conceder e revogar privilégios a contas, usuários ou grupos de usuários e para realizar as seguintes ações:

- **Criação de conta –** cria uma conta e senha para o usuário ou grupo de usuários, permitindo acesso ao SGBD
- **Concessão de privilégio –** permite que o DBA conceda certos privilégios a determinadas contas.
- **Revogação de privilégios –** permite que o DBA cancele privilégios que foram dados anteriormente a determinados usuários.
- **Atribuição de nível de segurança –** consiste em atribuir contas do usuário ao nível de liberação de segurança apropriado.

3.2 IMPORTÂNCIA DA SEGURANÇA EM BANCO DE DADOS

Em se tratando de segurança em banco de dados, conforme Ramakrishnan e Gehrke (2008), devem ser atingidos três metas principais: a confidencialidade, a integridade e a

disponibilidade. Esses são os três principais pilares quando se trata de segurança em banco de dados.

Conforme a tecnologia avança e o mundo se encontra cada vez mais conectado a internet aumentam exponencialmente o risco de ataques de hackers que buscam realizar o furto ou o sequestro de informações cometendo crimes através da rede. Esses crimes são conhecidos por vários nomes, como por exemplo cibercrime, crime informático, crime cibernético, crime eletrônico, crime digital, entre outros. Já existem divisões na polícia especializados em combater e investigar esses tipos de crimes e também existem leis especificas, como as apresentadas no Marco Civil da Internet, para tratar dessas infrações que são cada vez mais comuns. Frequentemente vemos notícias sobre ataques virtuais onde os criminosos utilizam seus conhecimentos em informática e tecnologia para burlar os sistemas de segurança das empresas afim de conseguirem algum tipo de lucro ou vantagem com isso, seja para si próprio ou para terceiros.

Perder dados/informação fatalmente irá representar um enorme prejuízo para qualquer empresa. E quando digo prejuízo não estou me referindo apenas ao prejuízo financeiro, mas a vários outros problemas como o vazamento de dados sigilosos da empresa ou de seus clientes, o comprometimento de informações sobre seus planos de negócio, exposição de dados sensíveis de todos os envolvidos com a empresa, e que tem suas informações armazenadas no seu banco de dados, e ainda é preciso observar que quando a segurança de uma empresa é invadida a própria imagem dessa empresa pode ser afetada fazendo com que seus clientes percam a confiança nela.

Atualmente um dos crimes digitais que tem obtido muito destaque na mídia, repercutindo com muitas notícias abordando esse tema, é o chamado Ransonware que é basicamente o sequestro de dados de empresas e pessoas. Explicando de maneira sucinta, conforme os autores Liska e Gallo (2017, p. 16) “Ransomware é um termo abrangente usado para descrever uma classe de malwares que serve para extorquir digitalmente as vítimas fazendo-as pagar um preço especifico”. Ou seja, o ramsonware é uma espécie de código malicioso que impossibilita acessar as informações armazenadas em um banco de dados e que geralmente requer o pagamento de um resgate (ransom) para devolver o acesso as informações.

Ainda segundo Liska e Gallo (2017, p. 16) “As duas principais formas de ramsonware são aquelas que criptografam, ofuscam ou impedem o acesso aos arquivos, e aquelas que restringem o acesso ou bloqueiam os usuários dos sistemas”.

Saíram várias notícias abordando esse assunto no ano de 2017, noticiando esse tipo de ataque a diversas grandes empresas. Uma notícia que ficou muito conhecida, no ano de 2017, com relação a esse tema, foi o sequestro de dados da emissora de TV americana HBO onde os criminosos roubaram informações confidenciais da empresa e exigiram pagamento de resgate para devolver as informações, caso contrário as tornariam públicas.

Quando esse tipo de crime ocorre a empresa se encontra em uma situação extremamente delicada, pois não existem garantias que, mesmo mediante ao pagamento do resgate, as informações serão devolvidas ou não serão expostas.

Por isso a segurança do banco de dados é tão crucial e é dado cada vez mais valor a isso. Tanto que existem profissionais totalmente especializados na área de segurança digital e que trabalham continuamente para combater e evitar esses crimes. Vale ressaltar que nenhum sistema de segurança é cem por cento a aprova de falhas ou invasões, mas cabe aos profissionais que trabalham nessa área adotar medidas e impor barreiras para dificultar ao máximo que os seus sistemas seja invadido e tenha as suas informações comprometidas.

É importante salientar, como é observado pelos autores Liska e Gallo (2017, p. 16) que “Essas ameaças não estão limitadas a nenhuma área geográfica ou sistema operacional em particular e podem atuar em vários dispositivos”.

Para evitar esses tipos de problemas é fundamental para toda e qualquer empresa e pessoa que utilize sistemas conectados a internet (que hoje em dia são praticamente todas), que cuide da segurança dos seus dados através de medidas e boas práticas de segurança que será abordado a seguir.

3.3 PRINCIPAIS ERROS COMETIDOS NA SEGURANÇA DO BANCO DE DADOS

Com a constante evolução tecnológica em que vivemos atualmente, as empresas, instituições, corporações, estão cada vez mais dependentes dos sistemas de informação. Todo esse avanço tecnológico gera muitos benefícios, mas é preciso ficar atento a todas as vulnerabilidades a que os sistemas dessas empresas estão constantemente expostos.

Todas as empresas que possuem sistemas conectados a internet são potenciais vítimas de ameaças e ataques *on-line* realizados pelos infames hackers. Esses ataques muitas vezes

só são possíveis por que as próprias empresas cometem erros que poderiam ser evitados. Esses erros levam as empresas a ser vítimas de ataques hackers, malwares, extorsões on-line através do uso de ramsonsware, entre outros.

Cabe aos profissionais da área de T.I. que forem qualificados e especializados na área de segurança, tomar todos os devidos cuidados e implementar as medidas de segurança necessárias para combater investidas não autorizadas contra o sistema. Para fazer isso é indispensável que o profissional conheça os principais erros, falhas e as brechas que podem existir na segurança dos bancos de dados empresariais.

Existem inúmeros erros que são cometidos quando se fala de segurança em banco de dados e segurança da informação, de uma forma mais abrangente. Entre os principais erros e falhas cometidas na segurança podemos citar: falta de investimento em segurança, não conhecer as principais ameaças, ausência de controle de usuários, problemas de criptografia, inexistência de politicas de segurança, exposição de mídia *storage*, falha na rotina de backup, sistemas de segurança fracos e/ou desatualizados, não contratar profissionais especialistas na área de segurança, dar privilégios demais a pessoas demais, SQL *injection*, falta de controle sobre atualizações.

A seguir vamos falar um pouco sobre esses erros, que podem colocar em risco a segurança do banco de dados, e como evita-los.

Falta de investimento ou pouco investimento em segurança.

Um grande erro cometido por muitas empresas, principalmente as de pequeno e médio porte, é não dedicar tempo e dinheiro suficientes para a área de segurança, priorizando outras áreas que julgam ser mais importantes. Esse erro é mais notado em empresas de menor porte onde os recursos são mais limitados e os profissionais especializados em segurança são mais raros. Porém esse é um grave equívoco cometido por essas empresas, pois nos dias atuais o maior bem que uma empresa possui é a informação.

As empresas cometem esse erro para tentar economizar não investindo em seguranças e contratando profissionais especializados ou mesmo pela falta de conhecimento da necessidade se proteger contra as ameaças e das consequências que tais ameaças podem causar para a empresa, e esses erros podem trazer uma série de graves prejuízos, algumas vezes irreversíveis.

Como a tecnologia avança muito rapidamente nos dias de hoje, novas ameaças surgem constantemente o que faz com que seja necessário um olhar mais atento das empresas para essa questão além de um maior investimento na área de segurança da informação.

Contratar profissionais que sejam qualificados e especializados na área de segurança pode custar caro para a empresa. Uma maneira de contornar esse problema, se a empresa não possui os recursos e/ou tempo necessários para cuidar de maneira correta da segurança dos seus dados, seria terceirizar esse serviço para uma empresa que seja especialista nessa área de segurança e que tenha os recursos, as ferramentas, as técnicas e os profissionais necessários para faze-las.

Desconhecer as principais ameaças.

Com o avanço da tecnologia é inevitável que surjam novas ameaças na forma de novos malwares ainda mais nocivos e elaborados. Devido a isso, é fundamental que os profissionais que cuidam da segurança estejam a par das novas ameaças para conseguirem combate-las de forma adequada, implementando medidas e políticas de segurança que devem ser seguidas à risca, e de forma rigorosa, por toda a empresa.

Para evitar futuros problemas, os profissionais que cuidam da segurança precisam estar sempre atualizados e antenados nas novas ameaças bem como nas novas ferramentas para combate-las.

Inexistência de controle de usuários.

Muitas empresas cometem o erro elementar de não fazer um controle de acesso da maneira correta, ou seja, um controle de usuários mais severo. Isso possibilita que qualquer usuário de qualquer nível da empresa possa ter acesso a dados sigilosos aos quais eles não deveriam ter acesso.

Para evitar esse problema se faz necessário que seja implementado um controle de acesso rigoroso, onde os níveis de permissão sejam muito bem definidos para cada usuário e que cada usuário tenha apenas as permissões e privilégios que são absolutamente necessários para desempenhar a sua função dentro da empresa.

Falta de políticas de segurança.

Esse é outro erro muito comum nas empresas. Muitas nem se quer tem uma política de segurança e outras tem políticas de segurança confusas e que não são cumpridas como deveriam. A política de segurança da empresa deve ser simples, clara, direta, objetiva e muito bem definida, para que todos os usuários possam entende-la perfeitamente. É função do DBA estabelecer e fazer com que sejam cumpridas as políticas de segurança, que devem ser rigorosas, mas ao mesmo tempo fáceis de se entender para que todos os colaboradores ajudem na árdua tarefa de manter a segurança inviolável.

Backups mal protegidos.

Proteger apenas o banco de dados no servidor original e se esquecer de proteger os backups é outro erro que pode custar caro as empresas. Ataques também podem ser feitos contra backups sem proteção ou mal protegidos e não apenas ao banco de dados principal da empresa. Levando em consideração esse fato é de extrema importância que os locais onde são armazenados os backups também tenham uma segurança equivalente a do servidor original, evitando assim possíveis brechas para futuros ataques.

Uma boa alternativa é realizar os backups na nuvem, pois desse modo estará mais seguro do que ser for armazenado localmente, estando protegido por exemplo de acidentes como incêndios, enchentes e falhas humanas e além disso o ambiente da nuvem sempre conta com novas tecnologias, ferramentas adequadas e profissionais especializados nesse tipo de serviço.

Falha na rotina de backup.

O backup é uma medida de segurança essencial para garantir que, no caso de algum problema com o banco de dados original, esses dados não serão perdidos pois existe uma cópia de segurança sempre atualizada para restaurar o banco de dados original caso seja necessário. O problema é que muitos só se lembram do backup quando acontece algum transtorno e se faz necessário utilizar o backup para restaurar o banco de dados. Muitos cometem o erro de não dar a devida atenção as rotinas de backups, deixando-os desatualizados e apenas lembrando-se do backup quando já é demasiado tarde.

A maneira de não deixar tal problema ocorrer é colocar em prática uma rotina de backup que seja eficaz e que garanta que o backup esteja sempre atualizado e pronto para ser utilizado quando for necessário, não só no caso de um ataque ou perca de dados, mas no caso de erros cometidos pelos próprios funcionários da empresa.

Falta de controle sobre atualizações.

Se um sistema está desatualizado com certeza ele estará muito mais vulnerável a possíveis invasões. Por isso as empresas desenvolvedoras de software costumam lançar novas atualizações periodicamente para manter o sistema sempre protegido e corrigir possíveis falhas e erros que possam existir. Existem empresas que não dão a devida atenção as atualizações e acabam deixando seus sistemas vulneráveis, contribuindo para que hackers mal-intencionados tenham êxito quando tentarem invadir o sistema. Para evitar esse tipo de problema é muito importante sempre conferir se existem novas atualizações e sempre estar com a atualização mais recente. Uma boa opção é deixar as atualizações para serem baixadas e instaladas automaticamente, sempre que possível, para evitar que sejam esquecidas.

Excesso de privilégios.

Mais um erro crasso que costuma ser frequentemente cometido nas empresas é dar muitos privilégios para pessoas demais ou para pessoas erradas. Uma pessoa com muitos privilégios, em um SGBD, pode acessar informações sigilosas e importantes aos quais ela não deveria ter acesso, e por um descuido, acidente ou mesmo por más intenções, pode furtar, deletar, alterar ou incluir informações no banco de dados sem a devida permissão. Para evitar esse tipo de problema o DBA deve estar muito atento a essa questão e é primordial que seja concedido apenas os privilégios que são absolutamente necessários para que o colaborador possa desempenhar as suas funções de maneira satisfatória dentro da empresa. Em outras palavras, o DBA deve saber quem pode fazer o que dentro do banco de dados e conceder o mínimo de privilégios possíveis aos colaboradores da empresa. Os privilégios devem ser concedidos de acordo com o cargo e função de cada colaborador.

SQL injection.

Segundo Silberschatz et al. (2012) SQL injection é a inserção de instruções SQL, não autorizadas, no banco de dados. O invasor entra no sistema e adiciona comandos SQL mal-intencionados no banco de dados que podem dar todo tipo de privilégios para esse invasor, como por exemplo dar a ele permissão para manipular os dados livremente, alterando, excluindo ou inserindo dados e/ou executar rotinas de acordo com a sua vontade. Para evitar que isso aconteça, é muito importante que a segurança do banco de dados esteja sempre preparada corretamente, utilizando todas as medidas de segurança. Também é importante que o sistema e os backups estejam sempre atualizados para fazer um *restore* do banco de dados caso seja necessário.

3.4 BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

Como vimos anteriormente é indiscutivelmente essencial que se cuide ao máximo da segurança do banco de dados. Mas como fazer isso? Cuidar da segurança e garantir que os dados estão devidamente protegidos não é uma tarefa simples ou fácil, mas que deve ser seguida de maneira rigorosa, criteriosa e continua, já que os ataques acontecem a todo instante. Para um nível ideal de segurança é preciso seguir as chamadas boas práticas de segurança da informação e colocar em prática políticas de segurança na empresa que devem ser seguidas à risca sempre.

Relembrando o que dizem os autores Ramakrishnan e Gehrke (2008), a segurança da informação busca assegurar a integridade, a confidencialidade, a autenticidade e a disponibilidade das informações manipuladas pela empresa.

São necessárias muitas ações para que a empresa esteja num nível considerado seguro de invasões e crimes digitais. Afim de evitar ou dificultar ao máximo a quebra da segurança é necessário adotar algumas boas práticas básicas.

Vamos citar algumas boas práticas para que a empresa possa manter suas informações em segurança:

Manter os softwares constantemente atualizados.

Qualquer pessoa que utiliza aplicativos em quaisquer plataformas, seja no desktop, notebook, smartphone, etc., sabe que os desenvolvedores de softwares lançam com frequência novas atualizações para os seus aplicativos. Essas atualizações tem o intuito de melhorar a performance dos aplicativos e também aperfeiçoar a segurança corrigindo possíveis falhas e se adaptando a novos tipos de ameaças que vão surgindo com o tempo. Um software desatualizado corre muito mais riscos de ter a sua segurança violada, por isso é muito importante realizar a atualização frequente dos softwares sempre que tiver disponível novas atualizações. Muitos softwares tem a opção de fazer essas atualizações de forma automática, mas nem sempre isso é observado pelos usuários, de maneira que é preciso ficar atento a esses detalhes para ter certeza que os softwares utilizados pela empresa estejam sempre atualizados com as suas últimas versões.

Limitar o acesso de usuários.

Em todo lugar onde existem pessoas trabalhando a sempre o risco de acontecer falhas e pode ter certeza que se existe esse risco as falhas irão acontecer. Isso é um fato, então é preciso saber lidar com ele. Pessoas são suscetíveis a erros e a serem influenciadas, manipuladas ou enganadas por outrem e também existe o risco de o próprio funcionário agir de má fé com o objetivo conseguir informações privilegiadas da empresa para vender para um concorrente por exemplo, a chamada espionagem industrial, pode ser feito tanto por pessoas de fora como por pessoas de dentro da empresa.

Exatamente por esses fatores é que se deve limitar ao máximo o acesso dos usuários concedendo apenas o acesso estritamente necessário para cada tipo de usuário. Nenhum usuário deve ter mais acesso do que ele necessita para realizar o seu trabalho ou a sua interação com o sistema.

Política de segurança.

É preciso ter uma política de segurança muito clara e objetiva que fique perfeitamente compreendida por todos os colaboradores da empresa, com regras fáceis de se entender de todas as práticas que são recomendadas, permitidas e proibidas. Pouco ou nada adianta

investir muito dinheiro em segurança e em novas tecnologias se os usuários não tomarem os cuidados necessários como por exemplo cuidados com as senhas!

Por isso deve-se dar uma atenção especial para isso com uma política de senhas para todos os usuários que interagem com o sistema, aplicativos e banco de dados. Essas práticas visam impedir o uso não autorizado de senhas. Vamos citar algumas das práticas que devem ser implementadas na política de senhas:

- ✓ A senha deve ser informada separadamente da ID do usuário.
- ✓ A senha nunca deve ser compartilhada a outras pessoas. Ela é individual e intransferível.
- ✓ A senha inicial gerada para cada usuário deve ser aleatória.
- ✓ Deve-se exigir a alteração da senha inicial que foi gerada aleatoriamente para o usuário.
- ✓ A senha tem que possuir um mínimo de caracteres previamente estabelecido, não sendo recomendado menos do que 6 caracteres.
- ✓ A senha tem que ter uma complexidade também estabelecida. O ideal é que obrigue o usuário e misturar números e letras e diferenciar letras maiúsculas e minúsculas para aumentar a complexidade da senha.
- ✓ Novas senhas criadas pelos usuários nunca podem ser iguais as senhas anteriores.

Realização periódica de backups de segurança

Fazer backups frequentes de todas as informações salvas no banco de dados é uma das práticas de segurança mais importantes. É tão importante que iremos tratar desse assunto mais adiante de forma mais detalhada. Mas é bom frisar que uma empresa que faz backups frequentes do seu banco de dados e mantem esses backups guardados em locais seguros nunca irá correr o risco de perder todas as suas informações. Dependendo do volume de informações da empresa o ideal é que seja feito backup várias vezes durante o dia e que esses backups nunca sejam mantidos armazenados em um mesmo local. Trataremos desse assunto especificamente mais adiante.

Antívírus e Firewalls.

Outra medida que se deve dar muita atenção é na aquisição de softwares de segurança, os chamados antivírus. É muito importante ter um bom e confiável antivírus instalado e

sempre atualizado assim como o firewall ativado para aumentar ao máximo o número de barreiras dificultando a vida dos hackers que possam a vir tentar invadir o sistema de alguma maneira. É sempre bom dar preferência aos antivírus conhecidos e conceituados e sempre que possível optar pela solução completa, ou seja, pela forma paga do antivírus, que geralmente oferece uma gama muito maior de funcionalidades aumentando a segurança e prevenindo contra mais tipos de perigos.

Criptografia

Toda informação disseminada, seja ela propagada interna ou externamente deve ser criptografada. E isso inclui não apenas informações secretas e importantes, mas quaisquer tipos de informação, do e-mail mais corriqueiro tratando de assuntos banais até as informações extremamente sigilosas. Todas devem ser criptografadas, isto é, codificadas, para que se alguma pessoa não autorizada obter acesso não consiga ler as informações contidas naquela mensagem.

Essas são apenas algumas práticas de segurança que são básicas, mas fundamentais para que se possa ter uma segurança minimamente adequada para proteger as informações. Mais para frente, ainda neste capítulo iremos abordar mais detalhadamente essas e outras medidas de segurança especificas para proteger o banco de dados, como por exemplo o controle de acesso, criptografia, controle de fluxo, controle de inferência, privilégios, redundância de dados, independência de dados e backup.

4. OS PILARES DA SEGURANÇA DA INFORMAÇÃO

Nesse capítulo vamos falar sobre os três principais objetivos quando se trata de segurança da informação. Esses objetivos são conhecidos como os três pilares que sustentam a segurança da informação. E como falar sobre segurança de banco de dados é também falar sobre segurança da informação, pois as duas coisas estão entrelaçadas, já que o objetivo de garantir a segurança de um banco de dados é manter as suas informações seguras Vamos falar também sobre as medidas de segurança que são necessárias para garantir que esses três pilares se sustentem.

4.1 CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE

Conforme Albuquerque (2002) entre os vários aspectos relacionados à segurança, pelo menos três deles são fundamentais: confidencialidade, integridade e disponibilidade. Esses são os três critérios mais importantes de segurança da informação e são conhecidos como CID (Confidencialidade, Integridade e Disponibilidade). Esses conceitos formam os pilares da segurança de todo e qualquer sistema de informação utilizados pelas empresas, sejam elas pequenas, médias ou grandes organizações.

Mas o que é cada um desses critérios?

Embora já tenha sido abordado sobre cada um desses critérios, de maneira mais sucinta, no capítulo anterior, se faz necessário, devido a sua importância, esmiuçar melhor o assunto para que fique bem claro.

Vamos entendê-los para compreendermos melhor porque eles são tão importantes.

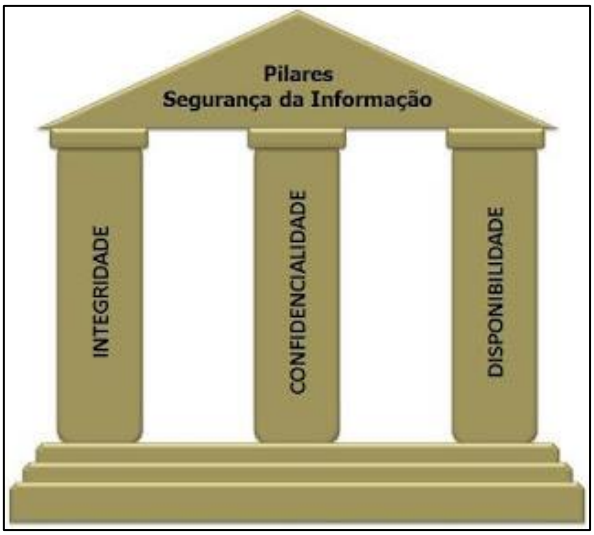

Figura 8 - Representação dos pilares da segurança da informação: Integridade, Confidencialidade e Disponibilidade.

Fonte: Banco de imagens Windows

Confidencialidade

De acordo com Stamp (2011, p. 2) “A confidencialidade lida com a prevenção de leitura não autorizada de informações”. Basicamente garantir a confidencialidade dos dados significa garantir que apenas as pessoas autorizadas e com a devida permissão vão ter acesso a determinadas informações, ou seja, vai se certificar que pessoas não autorizadas não possam acessar as informações protegidas.

Para Albuquerque (2002) garantir a confidencialidade é a capacidade de um sistema em impedir que usuários não autorizados tenham acesso a determinadas informações ao mesmo tempo em que usuários autorizados possam vê-las. Nas empresas a confidencialidade dos dados é muito importante pois é ela que protege o bem mais importante da empresa que são as suas informações.

As organizações costumam investir muito tempo e dinheiro em pesquisas, levantamentos, estudos para traçar planos e estratégias de mercado. Isso envolve, entre outras coisas, conhecer os seus clientes, o seu público alvo e os seus concorrentes, além de ter informações detalhadas sobre os produtos e/ou serviços comercializados por aquela empresa. São esses planos, que são discutidos e elaborados no nível estratégico das empresas, que vão definir qual caminhos as empresas irão seguir, vão definir o futuro da empresa. As informações definem não só quem a empresa é mais também para onde essa

empresa está caminhando, quem essa empresa vai ser no futuro. Para gerar todas essas informações a empresa geralmente investem muito tempo e dinheiro e não seria interessante que outras empresas tivessem acesso a essas informações, para não revelar os seus planos para os seus concorrentes e para não expor as informações dos seus clientes, entre outras coisas. Para que isso não ocorra a empresa precisa que a sua segurança garanta a confidencialidade das suas informações. Para garantir essa confidencialidade dos dados são necessárias algumas ações como a aplicação de diversos controles e o uso de criptografia em seus dados. Algumas outras ações para assegurar a confidencialidade das informações seria a ocultação de dados, a exclusão segura dos dados após o uso e o uso de sistemas de autorização e autenticação.

Se a empresa tiver a confidencialidade dos seus dados comprometida isso pode resultar em vários problemas para a empresa. Conforme Elmasri e Navathe (2011, p. 563), “A exposição não autorizada, não antecipada ou não intencional poderia resultar em perda de confiança pública, constrangimento ou ação legal contra a organização”.

Integridade

Conforme Stamp (2011, p. 2) “A integridade lida com a prevenção, ou pelo menos a detecção de alteração de dados não autorizada”. Falando de uma forma bem sucinta, assegurar a integridade da informação significa garantir que a informação não seja alterada de nenhuma maneira enquanto estiverem sendo armazenadas, transferidas ou processadas e que a informação está totalmente correta e é exibida de forma correta para quem a consulta. Os dados só podem sofrer alteração se tiver sido devidamente autorizado. A esse respeito Pfleeger (2012, p. 329) declara: “Se o objetivo de um banco de dados é servir como um repositório central de dados, os usuários devem ser capazes de poder confiar na precisão dos valores dos dados armazenados”.

É preciso assegurar que os recursos dos sistemas e as informações não sofram alterações de maneira não autorizada, inesperada ou até mesmo não intencionada devido a falhas humanas. Esse critério deve ser aplicado tanto para dados/informações como também para o hardware.

Sobre perda de integridade dos dados os autores Elmasri e Navathe (2011, p. 563) dizem que:

> A integridade é perdida se mudanças não autorizadas forem feitas nos dados por atos intencionais ou acidentais. Se a perda de integridade do sistema ou dos dados não for corrigida, o uso continuado do sistema contaminado ou de dados adulterados poderia resultar em decisões imprecisas, fraudulentas ou errôneas.

Com o volume de dados crescendo de forma exponencial nas empresas a integridade desses dados é absolutamente indispensável. Se não houver integridade dos dados isso irá causar diversos problemas para a empresa, resultando em perda de eficiência e consequentemente a empresa vai perder tempo e gerar menos lucro. Isso é oneroso para a empresa e deve ser evitado a todo custo.

Disponibilidade

Para Elmasri e Navathe (2011, p. 563), “A disponibilidade do banco de dados refere-se a tornar os objetos disponíveis a um usuário humano ou a um programa ao qual eles têm um direito legitimo”.

Então pode-se entender que garantir a disponibilidade significa assegurar que o dado/informação esteja sempre acessível para ser utilizada sempre que for necessário por um processo e/ou usuário devidamente autorizado, isto é, a informação deve estar sempre disponível para o usuário quando ele necessitar dela para desempenhar suas funções.

Silberschatz et al. (2006), diz que um dos objetivos no uso de banco de dados é possuir uma alta disponibilidade; ou seja, o banco de dados precisa funcionar em quase todo o tempo, mesmo que existam, vários tipos de falhas.

Se não houver disponibilidade dos dados o sistema da empresa não funciona, pois tudo depende do envio ou recebimento de informações. Se tiver problema de indisponibilidade de dados e paralisar os processos da empresa pode acarretar em perda de tempo e consequentemente gerar prejuízo para a mesma.

Estamos vivendo na era do conhecimento, na era digital, onde tudo e todos estão conectados e trocando informações constantemente. O volume de informações geradas é cada vez maior e essa informação é valiosa para qualquer empresa. Tendo isso em vista pode-se dizer que se não houver **confidencialidade** a empresa irá perder vantagem competitiva com relação aos seus concorrentes, se não houver **integridade** a empresa irá perder sua lucratividade e sem **disponibilidade** a empresa fica incapacitada de operar. Podemos concluir então que sem garantir a segurança da informação é praticamente impossível para qualquer empresa sobreviver no mercado nos dias de hoje e com certeza se tornará muito mais difícil dessa empresa prosperar e se manter competitiva.

4.2 MEDIDAS DE CONTROLE

Conforme Ozsu e Valduriez (2001, p. 176), “O controle de autorização deve garantir que somente pessoas autorizadas possam executar ações no banco de dados e somente as ações que lhe forem permitidas”.

As chamadas medidas de controle podem e devem ser aplicadas no gerenciamento de sistemas de banco de dados. Conforme Elmasri e Navathe (2011, p. 563), “Para proteger os bancos de dados contra esses tipos de ameaças, é comum implementar quatro tipos de medidas de controle: controle de acesso, controle de inferência, controle de fluxo e criptografia”. Ainda de acordo com Elmasri e Navathe (2005), em um sistema de banco de dados que possui muitos usuários, o SGBD precisa oferecer técnicas para permitir que certos usuários acessem apenas partes selecionadas de um banco de dados.

Essas medidas de controle irão ajudar a garantir a segurança do banco de dados, proteger suas informações e assegurar que os objetivos da segurança (Confidencialidade, Integridade e Disponibilidade), sejam alcançados de forma satisfatória. A seguir falaremos um pouco sobre cada uma dessas medidas de controle: controle de acesso, controle de fluxo, controle de inferência e criptografia.

Controle de acesso

Será dado um maior destaque a essa medida de controle, tendo em vista que na parte prática do trabalho será demonstrado a criação de contas de usuário e a concessão de

privilégios para os mesmos, em um banco de dados simulando o banco de dados de uma empresa fictícia.

Em um banco de dados onde existem vários usuários acessando o mesmo, o Sistema Gerenciador de Banco de Dados (SGBD) deve dispor de mecanismos que permitam restringir o acesso desses usuários somente ao conteúdo destinado a cada tipo de usuário e garantir que nenhum usuário possa acessar conteúdos aos quais ele não tenha autorização.

A esse respeito Elmasri e Navathe (2011, p. 563-564) declaram:

> Um problema de segurança comum aos sistemas de computação é o de impedir que pessoas não autorizadas acessem o próprio sistema, seja para obter informações ou para fazer mudanças maliciosas em uma parte do banco de dados. O mecanismo de segurança de um SGBD precisa incluir provisões para restringir o acesso ao sistema de banco de dados como um todo. Essa função, chamada controle de acesso, é tratada criando-se contas do usuário e senhas para controlar o processo de login pelo SGBD.

Segundo Casanova e Moura (1985, p. 19), “O objetivo da função de controle de acesso é implementar mecanismos que garantam a segurança dos dados armazenados no banco, permitindo que a informação seja lida ou modificada apenas por usuários autorizados”.

Então pode-se dizer que o controle de acesso é o controle que impõe regras de restrição através da criação de contas dos usuários, definindo um nome de usuário e uma senha. Como já vimos anteriormente, o Administrador de Banco de Dados (DBA) é o grande responsável por determinar as regras que vão existir no Sistema Gerenciador de Banco de Dados. Esse profissional é incumbido de conceder ou remover privilégios, criar e excluir usuários e atribuir o nível de segurança aos utilizadores do banco de dados. Esse tipo de controle de acesso é de extrema importância num banco de dados que é integrado com outros sistemas em uma grande empresa onde é acessado frequentemente por vários usuários. De maneira a assegurar esse controle o SGBD dispõe de um sistema de autorização de acessos que tem a responsabilidade de controlar todos os acessos feitos ao banco de dados garantindo que não possam existir acessos não autorizados. Afim de garantir esse controle são utilizados dois mecanismos:

- **Mecanismos de segurança discricionários** que são utilizados afim de conceder o devido acesso aos utilizadores do banco de dados para realizar consultas e atualizações de arquivos, registros e campos da base de dados.

- **Mecanismos de segurança obrigatórios** são os mecanismos que visam conceder acesso aos usuários do banco de dados por meio de uma especificação levando em conta a função que cada usuário exerce no banco de dados. Para realizar esse procedimento é utilizado um conceito de papéis (roles) ou os chamados perfis de usuário com a finalidade de definir qual usuário pode acessar qual informação dentro do banco de dados de acordo com o perfil de cada um.

Controle de fluxo

Segundo Elmasri e Navathe (2011, p. 579), “O controle de fluxo regula a distribuição ou fluxo de informações entre objetos acessíveis”.

Os autores Elmasri e Navathe (2011, p. 564) explicam que esse mecanismo de controle não permite que os dados fluam, de maneira que não venham a alcançar usuários sem autorização, por canais secretos e quebrem as medidas de segurança da empresa. O controle de fluxo é responsável por regular a distribuição de informação entre objetos acessíveis. Visando impedir que esses dados possam ser interceptados.

Controle de Inferência

De acordo com Elmasri e Navathe (2011, p. 564), esse tipo de controle é um mecanismo de segurança utilizados em bancos de dados estatísticos, e age de forma a proteger as informações de uma pessoa ou de um grupo de pessoas. Esses tipos de banco de dados são mais utilizados para fornecer estatísticas sobre variadas populações. O banco de dados contém informações sigilosas sobre pessoas. Sendo assim os usuários devem ter permissão somente para obter dados estatísticos, ou seja, dados em massa, sobre um grupo de indivíduos e nunca acessar dados individuais de alguma pessoa especifica, como por exemplo ter acesso ao seu endereço, telefone, etc.

Criptografia de Dados

Sobre criptografia Elmasri e Navathe (2011, p. 580) declaram:

> A criptografia é a conversão de dados para um formato, chamado texto cifrado, que não pode ser facilmente entendido por pessoas não autorizadas. Ela melhora a segurança e a privacidade quando os controles de acesso são evitados, pois em casos de perda ou roubo de dados, aqueles criptografados não podem ser facilmente entendidos por pessoas não autorizadas.

Esse mecanismo de controle é utilizado com o intuito de proteger dados/informação confidenciais que trafegam através de alguma rede de comunicação, de acesso não autorizado. A criptografia também é frequentemente utilizada para reforçar a proteção afim de que dados e informações sigilosas de um banco de dados não possam ser acessados por pessoas indevidas.

A esse respeito, é preciso considerar que:

> A segurança dos dados da aplicação precisa lidar com várias ameaças de segurança e questões além daquelas tratadas pela autorização da SQL. Por exemplo, os dados precisam ser protegidos enquanto estão sendo transmitidos; eles podem ter de ser protegidos contra intrusos capazes de burlar a segurança do sistema operacional e podem ter restrições de privacidade complexas, que vão além daquilo que um banco de dados pode impor. (SILBERSCHATZ; KORTH; SUDARSHAN, 2006, p. 229).

Para efetuar a criptografia dos dados os mesmos são codificados fazendo uso de um algoritmo de codificação. Dessa forma mesmo que ocorra algum acesso não autorizado a esses dados será impossível utilizar os dados pois eles estarão criptografados (codificados). Para “decifrar” esses dados é preciso ter o algoritmo de codificação e somente os usuários previamente autorizados é que tem acesso a chave para descriptografar os dados e utilizar os mesmos. O objetivo é fazer com que um usuário não autorizado não consiga ou tenha grande dificuldade de decifrar esses dados. Criptografar dados permite “disfarçar” as informações e assim mesmo que ela for interceptada por alguém não autorizado a mensagem não será revelada.

4.3 PRIVILÉGIOS

De acordo com Elmasri e Navathe (2011) privilégios, que também podem ser chamados de autorizações, são permissões únicas concedidas a cada usuário de maneira individual ou a um grupo de usuários. Os privilégios determinam permissões para tipos de autorização e define a maneira como deverá ser acessado determinado objeto. Os privilégios concedem ou não as autorizações necessárias para alterar ou acessar determinados recursos do

Banco de Dados. Assim que um novo usuário é criado ele não possui nenhum tipo de privilégio. Existem vários tipos de privilégios que podem ser atribuídos ao usuário, o Sistema Gerenciador de Banco de Dados deve disponibilizar acesso seletivo para cada relação do BD baseado em contas especificas. As ações que cada usuário pode exercer no banco de dados podem e devem ser controladas. O usuário que possui uma conta não tem acesso a todas as funções que o Sistema Gerenciador de Banco de Dados tem a oferecer. Podemos dizer que existem 2 níveis para se atribuir privilégios para utilização do sistema de BD:

- **Nível de conta –** o Administrador de Banco de Dados determina os privilégios distintos que cada conta possui independente das relações no BD.
- **Nível de ralação –** o Administrador de Banco de Dados controla os privilégios para acessar cada relação especifica no BD.

Concessão e Revogação de Privilégios

Usuários podem receber o direito de repassar os privilégios recebidos para outros usuários. Este repasse de privilégio deve ser tratado com o devido cuidado para que seja possível revogá-lo no futuro (SILBERSHATZ; KORTH; SUDARSHAN, 2012, p. 639).

Para criar ou excluir privilégios em bancos de dados relacionais, a linguagem SQL utiliza os comandos de concessão (GRANT) e revogação (REVOKE). Esses comandos padrões, por sua vez, incluem os privilégios de selecionar (SELECT), inserir (INSERT), modificar (ALTER) e apagar (DELETE). Estes privilégios de concessão e revogação são verificados pelo controle de acesso e representam a principal interface do usuário para controlar o subsistema de autorização ou privilégios.

4.4 REDUNDÂNCIA DE DADOS

A redundância de dados ocorre quando existe mais de uma representação para o mesmo dado, ou seja, constitui-se no armazenamento de um mesmo dado/informação em diferentes localidades podendo provocar inconsistências. Segundo Silberschatz et al. (2012) levando em consideração que diferentes programadores criam partes de programas e aplicações durante um longo período, os diversos arquivos podem ter diferentes

estruturas e os programas podem ser escritos em várias linguagens de programação. Além disso as mesmas informações podem estar duplicadas em diversos lugares (arquivos).

A redundância pode prejudicar o sistema, ocupando espaço desnecessário e tornando o sistema mais lento, portanto é preciso um controle da redundância de dados afim de evita-la. Em um Sistema Gerenciador de Banco de dados as informações armazenadas são mais sucintas, pois os dados armazenados aparecem apenas uma vez. Isto minimiza drasticamente a redundância de dados, ou seja, a necessidade de se repetir esses dados outras vezes. Diminuindo ou evitando a redundância irá acarretar em uma diminuição significativa do custo de armazenamento de dados.

4.5 INDEPENDÊNCIA DE DADOS

A independência de dados é, segundo Ramakrishnan e Gehrke (2008), a imunidade das aplicações às mudanças na estrutura de armazenamento es estratégias de acesso. Ter independência dos dados é muito importante e significa poder realizar alterações no esquema ou no nível de um BD, sem alterar um nível superior. Para que que seja possível entender o que é independência de dados se faz necessário que antes conheçamos as visões abstratas de dados. O maior objetivo de um SGBD é fornecer aos usuários uma visão simples, objetiva e abstrata das informações. Isso é feito escondendo detalhes de como esses dados são armazenados e mantidos. Mas para que esse sistema possa ser utilizado de forma satisfatória as informações armazenadas no banco precisam ser buscadas de forma rápida e eficiente. Levando-se em consideração que uma grande parte dos usuários de BD não tem conhecimentos em computação, a complexidade fica omitida deles através de vários níveis de abstração que facilitam a interação do usuário com o sistema.

- **Nível físico**: é o nível mais baixo de abstração. Nesse nível está contido como os dados estão realmente armazenados. Nesse nível existem complexas estruturas de dados de baixo nível que são descritas em detalhes;
- **Nível conceitual**: é o próximo nível de abstração. Nesse nível é descrito quais informações estão armazenados no BD e as relações que existem entre elas. No nível conceitual o banco de dados inteiro é caracterizado em termos de um pequeno

número de estruturas relativamente simples. Apesar de as implementações de estruturas simples nesse nível possa envolver estruturas mais complexas de nível físico, o usuário desse nível (conceitual) não deve se preocupar com isso. O nível conceitual de abstração é usado pelos DBAs que tem o poder para tomar decisões de quais informações devem manter no Banco de Dados;

- **Nível de visões**: esse é o nível mais alto de abstração. Nesse nível é descrito apenas parte do banco de dados. Embora utilize estruturas mais simplistas do que no nível conceitual, existe alguma complexidade devido ao grande tamanho do banco de dados. Uma grande quantidade de usuários banco de dados não terão interesse em todas as informações. Os usuários, na maioria das vezes precisam de apenas uma parte do banco de dados. O nível de abstração das visões de dados é estabelecido de modo a tornar mais simples esta interação com o sistema, que pode fornecer muitas visões para o mesmo BD.

A capacidade de alterar a definição de um nível de abstração de maneira que não afete a definição de esquema de um nível superior, isto é independência de dados.

A seguir vamos ver que essa independência de dados é separada em dois níveis distintos:

- **Independência física de dados**: trata-se da capacidade de alterar o esquema físico sem a obrigação de escrever novamente os programas aplicativos. Modificações nesse nível podem se fazer necessárias para melhorar o desempenho.
- **Independência lógica de dados**: trata-se da capacidade de alterar o esquema conceitual sem a obrigatoriedade de escrever novamente os programas aplicativos. As modificações no nível conceitual são indispensáveis quando a estrutura lógica do BD é alterada.

5. LINGUAGEM SQL – MANIPULANDO O BANCO DE DADOS.

Neste capítulo será feita uma introdução básica a linguagem SQL, demonstrando alguns comandos básicos e dando um foco maior aos comandos voltados para a segurança em banco de dados, como por exemplo os comandos para criar usuários e conceder e revogar privilégios, ou seja, os comandos utilizados para controlar acessos e definir privilégios

5.1 INTRODUÇÃO BÁSICA A LINGUAGEM SQL.

A Linguagem SQL (Structured Query Language), ou em português Linguagem de Consulta Estruturada, é uma linguagem muito conhecida por ser a mais utilizada para a manipulação dos bancos de dados relacionais (BDR).

De acordo com Elmasri e Navathe (2011), a linguagem SQL foi criada no início da década de 70 pela IBM. No início quando foi desenvolvida, o nome da linguagem era SEQUEL, acrônimo em inglês para *"Structured English Query Language",* que significa, Linguagem de Consulta Estruturada. Mais tarde a linguagem sofreu uma revisão e ampliação e seu nome foi alterado para SQL, nome que conhecemos hoje em dia. Devido a sua simplicidade e facilidade de uso, a linguagem SQL se tornou padrão para manipular banco de dados. Embora seja a mais conhecida e utilizada a linguagem SQL não é a única linguagem para manipular bancos de dados. Existem outras linguagens, mas que ficaram, de certa forma, obsoletas após a criação do SQL. A diferença da linguagem SQL para outras linguagens é que o SQL é uma linguagem declarativa e não uma linguagem procedural como as outras, isso faz com que a aprendizagem para os que começam a trabalhar com a linguagem SQL seja menor do que em outras linguagens. Além disso, uma outra diferença da linguagem SQL para as outras é que uma consulta SQL especifica a forma do resultado, e não o caminho para chegar a ele, como em outras linguagens. Por causa do sucesso dessa linguagem de consulta e manipulação de dados, seu uso cresceu muito se tornando a linguagem mais importante para realizar consultas e manipulação de dados dentro dos bancos de dados. Apesar da linguagem SQL ter sido desenvolvida pela IBM, não demorou muito para aparecer várias linguagens semelhantes baseadas na SQL feitas por outros desenvolvedores. Isso levou a necessidade de se criar um padrão para a linguagem o que

foi feito mais tarde em 1986 pela ANSI e ISSO em 1987 (SILBERSCHATZ et al., 2012). Mas mesmo sendo criado um padrão para a linguagem, existem muitas variações criadas pelos vários fabricantes de SGBD (Sistemas Gerenciadores de Banco de Dados). Normalmente a linguagem SQL pode ser transferida entre diferentes plataformas sem mudanças na estrutura principal. A linguagem SQL foi revista algumas vezes em 1992, 1999 e 2003, sofrendo mudanças, alterações a atualizações até chegar na linguagem que conhecemos atualmente.

Diversos Sistemas Gerenciadores de Bancos de Dados (SGBD), utilizam a linguagem SQL como padrão para manipular os BD. Entre os principais e mais utilizados no mercado, podemos mencionar alguns nomes como por exemplo:

- ORACLE da Oracle Corporation
- MySQL da Oracle Corporation
- SQL Server da Microsoft
- DB2 da IBM

A Linguagem SQL é dividida em subconjuntos, de acordo com as operações que queremos efetuar, entre eles podemos citar:

- **Data Definition Language (DDL)**

A Linguagem de Definição de Dados possibilita ao usuário definir a estrutura e organização dos dados armazenados e das relações que existem entre eles.

- **Data Manipulation Language (DML)**

A Linguagem de Manipulação de Dados possibilita ao usuário executar instruções para incluir, remover, selecionar ou atualizar dados armazenados no banco de dados.

- **Data Control Language (DCL)**

A Linguagem de Controle de Dados controla as permissões, autorizações e privilégios dos usuários para definir quem tem ou não acesso para consultar ou manipular o banco de dados.

5.2 INSTRUÇÕES SQL – PRINCIPAIS COMANDOS BÁSICOS UTILIZADOS EM UM BANCO DE DADOS

A linguagem SQL possui muitas instruções para manipular o banco de dados. Entre as instruções consideradas básicas e principais, podemos citar:

- **A Linguagem de Manipulação de Dados (DML - Data Manipulation Language)**

De acordo com Ramakrishnan e Gehrke (2008) a Linguagem de Manipulação de Dados é um subconjunto da linguagem SQL que permite aos usuários formular consultas, inserir, excluir e modificar dados do banco de dados. As principais instruções DML são:

INSTRUÇÃO SQL	**FUNÇÃO**
INSERT	INSERIR LINHAS EM UMA TABELA
UPDATE	ALTERAR LINHAS EM UMA TABELA
DELETE	DELETAR LINHAS EM UMA TABELA

Exemplos das utilizações das instruções DML:

- **INSERT**

  A instrução/comando para inclusão de dados nas tabelas é o INSERT e possui a seguinte estrutura:

  INSTERT INTO Clientes (id, nome, idade, sexo, nascimento)
  VALUES (1, ‘Fabio Viana Campos’, 36, ‘masculino’, ’20/05/1981’);
  Nessa instrução está inserindo um novo cliente com os seguintes dados: id, nome, idade, sexo e data de nascimento, na tabela Clientes.

- **UPDATE**

  A instrução/comando para atualizar dados em uma tabela é o UPDATE e possui a seguinte estrutura:

UPDATE Professor
SET salario = salario*1.15;

Nessa instrução está sendo alterado o salário de todos os professores da tabela Professor, pegando o salário atual e multiplicando por 1.15, ou seja, um aumento de 15% no salário dos professores.

- **DELETE**

  A instrução/comando para excluir dados em uma tabela é o DELETE e possui a seguinte estrutura:

  DELETE FROM Clientes
  WHERE id = 1;

  Nessa instrução está sendo excluído da tabela Clientes o cliente com o número de id igual a 1.

- **A Linguagem de Definição de Dados (DDL - Data Definition Language)**

  A Linguagem de Definição de Dados é, segundo Ramakrishnan e Gehrke (2008), um subconjunto da SQL utilizada para definir as estruturas de dados concedendo instruções para criar, modificar, ou eliminar tabelas. É utilizada também para criar índices (chaves) e definir ligações entre as tabelas. As principais instruções DML são:

INSTRUÇÃO SQL	**FUNÇÃO**
CREATE	CRIAR TABELA
ALTER	ALTERAR TABELA
DROP	DELETAR TABELA
RENAME	RENOMEAR TABELA
TRUNCATE	EXCLUIR DADOS DA TABELA

Exemplos das utilizações das instruções DDL:

- **CREATE TABLE**

  Instrução utilizada para criar uma nova Tabela:

  CREATE TABLE Clientes
  (id NUMBER(2),
  nome VARCHAR2(50),
  sexo CHAR(1),
  data_nasc DATE);

Essa instrução é o comando para criar uma nova Tabela chamada Clientes, com as seguintes colunas: id, nome, sexo e data de nascimento.

- **ALTER TABLE**

  Instrução utilizada para adicionar, excluir ou modificar as colunas de uma tabela.

  ALTER TABLE Clientes
  DROP COLUMN nome;

  Essa instrução está dando o comando para excluir a coluna nome da Tabela Clientes.

- **DROP**

  Comando utilizado para excluir dados.

  DROP TABLE Clientes;

  Essa instrução está dando o comando para excluir a Tabela Clientes.

- **RENAME TABLE**

  Instrução utilizada para renomear Tabelas.

  RENAME TABLE Clientes **TO** Cliente

Essa instrução está dando o comando para alterar o nome da Tabela Clientes para Cliente.

- **TRUNCATE TABLE**

  Instrução utilizada para excluir os dados de uma tabela e não a tabela em si.

  TRUNCATE TABLE Clientes

  Essa instrução está dando o comando para excluir todos os dados armazenados na tabela Clientes, porém a tabela em si não será deletada.

- **A Linguagem de Consulta de Dados (DQL - Data Query Language)**

  A Linguagem de Consulta de Dados é a parte da linguagem SQL mais utilizada no banco de dados, pois através do comando SELECT é possível ao usuário consultar os dados armazenados no banco de dados. Esse comando é composto de várias cláusulas e opções o que possibilita ao usuário realizar desde consultas extremamente simples até consultas mais complexas e elaboradas.

INSTRUÇÃO	**FUNÇÃO**
SELECT	Realiza consultas a dados pertencentes a uma tabela.

Exemplos das utilizações da instrução SELECT:

- **SELECT**

  Instrução utilizada para recuperar/consultar dados armazenados nas tabelas do banco de dados.

  SELECT * FROM Clientes;

Essa instrução está listando todos os campos/colunas armazenados na tabela Clientes.

SELECT codigo, nome, salario
FROM Medicos
WHERE salario **BETWEEN** 5000 **AND** 7500;

Essa instrução está consultando/listando o código, nome e salario de todos os médicos da Tabela Médicos que possuam salário entre 5000 e 7500.

SELECT código, nome, sexo, telefone
FROM Clientes
WHERE data_nascimento **IS NULL;**

Essa instrução está consultando quais clientes não possuem a data de nascimento cadastrada.

- **A Linguagem de Controle de Dados (DCL - Data Control Language)**
  A Linguagem de Controle de Dados controla as permissões, autorizações, privilégios dos usuários para definir quem tem ou não acesso para consultar ou manipular o banco de dados. Essa linguagem DCL é a mais importante para essa pesquisa, tendo em vista que está diretamente relacionada com a segurança do banco de dados.

INSTRUÇÃO	**FUNÇÃO**
GRANT	Fornece privilégios
REVOKE	Remove privilégios

Exemplos das utilizações das instruções DCL:

- **GRANT**

  Instrução utilizada para conceder privilégios para um usuário ou grupos de usuários e especificar qual o tipo de privilégio dado ao usuário ou grupos de usuários.

  GRANT tipo_do_privilegio
  ON nome_do_objeto
  TO usuário/role

  Essa instrução está concedendo um determinado tipo de privilégio, que será determinado pelo DBA, sobre um objeto do banco de dados para um usuário especifico ou um grupo de usuários.

- **REVOKE**

  Instrução utilizada para remover privilégios de usuários ou grupo de usuários.

  REVOKE tipo_do_privilegio
  ON nome_do_objeto
  TO usuário/role

  Essa instrução está removendo um determinado tipo de privilégio, que será determinado pelo DBA, sobre um objeto do banco de dados de um usuário especifico ou de um grupo de usuários.

Essas são apenas algumas das principais instruções básicas que são utilizadas nos bancos de dados relacionais que utilizam a linguagem SQL, como o Oracle por exemplo.

5.3 CONTROLANDO ACESSOS E PRIVILÉGIOS

Garantir a segurança no banco de dados, segundo Date (2003), significa proteger os dados contra usuários não autorizados. Para garantir a segurança do banco de dados podem ser implementados vários mecanismos de segurança que irão ajudar na proteção contra uma variedade de tipos de ameaças. Podemos identificar como ameaças quaisquer ações, intencionais ou acidentais, que venham a comprometer a confidencialidade, integridade e/ou disponibilidade dos dados armazenados no banco de dados. O SGBD possui uma série de medidas de segurança que podem e devem ser utilizados pelo DBA.

Segundo Elmasri e Navathe (2005) as medidas mais comuns são utilizar criptografia, controle de fluxo, controle de inferência e controle de acesso. Em um banco de dados que possui vários usuários é fundamental que o Sistema Gerenciador de Banco de dados permita ao DBA estabelecer o controle de acesso, que vai garantir que apenas os usuários devidamente autorizados possam acessar e/ou manipular conteúdos determinados pelo DBA, ou seja, o DBA irá especificar quem pode acessar o que dentro do banco de dados e o que cada usuário pode fazer com esses dados.

De acordo com Elmasri e Navathe (2011), o método mais utilizado para controlar o acesso ao banco de dados é baseado em conceder ou revogar privilégios do usuário. Para conceder privilégios ao usuário primeiramente é preciso criar uma conta para o usuário. Isso é feito utilizando a seguinte sintaxe:

CREATE USER usuario
IDENTIFIED BY senha

- **Usuário:** nome do usuário a ser criado.
- **Senha:** estabelece uma senha para que o usuário efetue login

Depois do usuário devidamente criado, cabe ao DBA definir os privilégios ao qual esse usuário terá direito e concede-los. A sintaxe básica usual para a concessão de privilégio é:

GRANT tipo_do_privilegio
ON nome_do_objeto
TO usuário/role

É importante frisar que os usuários comuns não possuem privilégios de alto nível, sendo que esses são reservados apenas para o DBA.

Alguns dos privilégios que o DBA pode conceder para o usuário são:

PRIVILÉGIO/INSTRUÇÃO	**FUNÇÃO**
CREATE SESSION	Conectar-se ao banco de dados
CREATE TABLE	Criar tabelas em seu esquema
CREATE SEQUENCE	Criar sequência em seu esquema
CREATE VIEW	Criar view em seu esquema
CREATE PROCEDURE	Criar função, pacote ou procedimento

É importante salientar também que apenas o DBA possui privilégios de alto nível, sendo eles:

- Criar novos usuários.
- Remover usuários.
- Remover tabelas.
- Fazer backup de tabelas.

Privilégios do Administrador de Banco de Dados:

INSTRUÇÃO/ PRIVILÉGIO	**FUNÇÃO**
CREATE USER	Criar novo usuário
DROP USER	Remover usuário
DROP ANY TABLE	Eliminar tabela
BACKUP ANY TABLE	Fazer backup de tabelas

6. ESTUDO DE CASO E CONCLUSÃO

A parte prática do trabalho será focado no controle de acesso de usuários ao banco de dados e a concessão e/ou revogação de privilégios aos mesmos. Será feito a simulação de um banco de dados de teste de uma empresa fictícia, onde eu, no papel de DBA, irei ser o responsável pelo controle de acesso criando os usuários e concedendo os privilégios para estabelecer o que cada um pode fazer dentro do banco de dados.

6.1 ESTUDO DE CASO

Como vimos ao longo do trabalho o método mais utilizado para imposição do controle discricionário baseia-se na concessão e revogação de privilégios. Conforme os autores Elmasri e Navathe (2011), existem dois níveis para se atribuir privilégios de utilização de sistemas de banco de dados:

Nível de conta: O DBA especifica os privilégios individuais de cada conta existente no banco de dados, independente das suas relações no mesmo. Podem incluir privilégios como CREATE TABLE, CREATE VIEW, ALTER, DROP, MODIFY e SELECT.

Nível de relação: O DBA pode controlar o privilégio para acessar cada relação ou visão individual no banco de dados. Tais privilégios especificam para cada usuário as relações individuais sobre as quais cada tipo de comando pode ser aplicado.

Como mencionado anteriormente, nesse estudo de caso, vamos nos focar no mecanismo de controle de acesso, mais precisamente na criação de contas de usuário e na concessão de privilégios. Para isso iremos começar modelando o banco de dados, que será utilizado para realizar os testes.

É muito importante salientar que esse banco de dados será criado apenas com o intuito de realizar testes, para agregar valor ao trabalho e contribuir com o aprendizado. Por tanto esse banco de dados é extremamente simples e de maneira alguma retrata o banco de dados de uma empresa real e nem o nível de segurança de uma empresa real.

Esse é um banco de dados para testes que simula uma loja virtual e vamos fazer a modelagem do banco de dados utilizando a ferramenta DBdesigner, de modo a estabelecer o modelo Entidade-Relacionamento que irá compor esse banco de dados.

O banco de dados ao qual serão concedidas permissão de acesso as relações está representado no modelo Entidade-Relacionamento da figura 9.

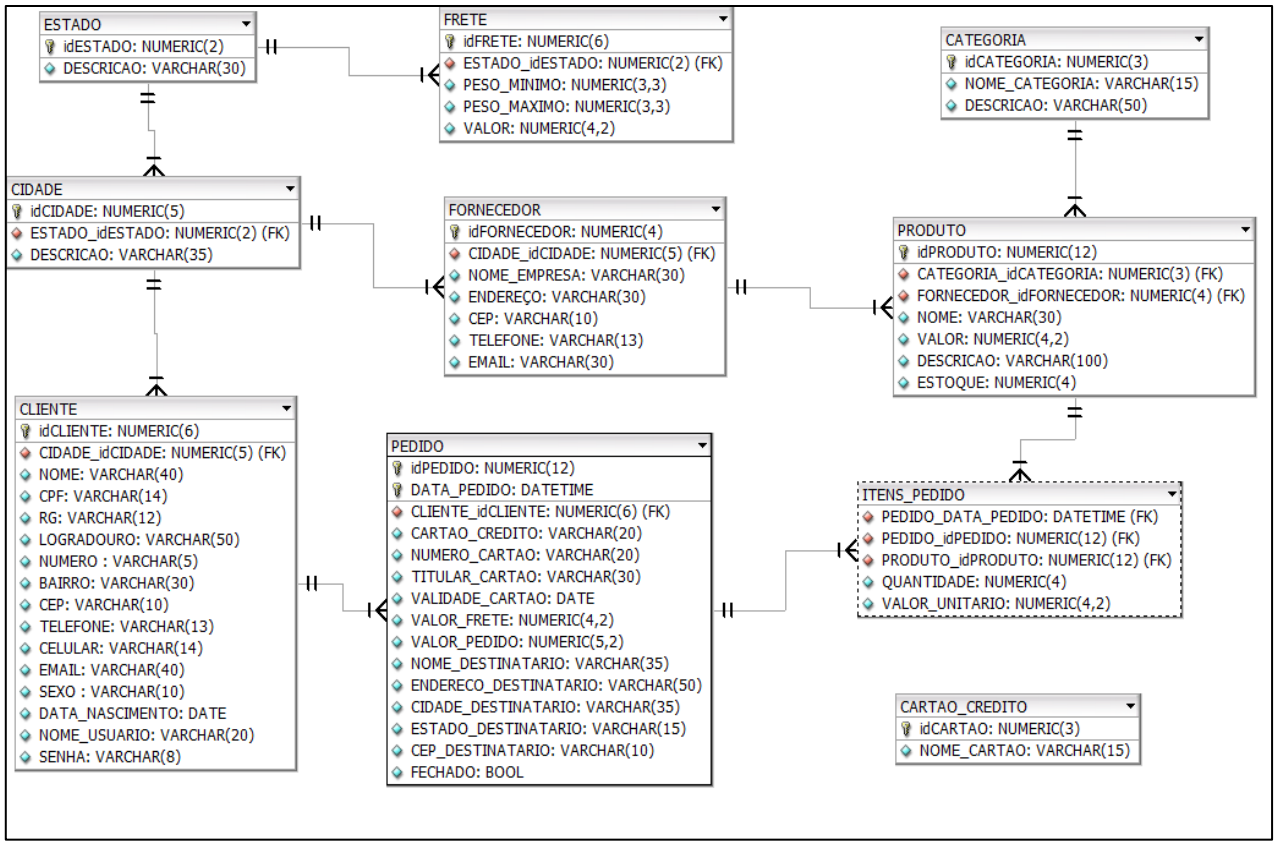

Figura 9: Modelo Entidade-Relacionamento do banco de dados de uma loja virtual.

Agora que o nosso banco de dados já está modelado representando todas as suas tabelas e relacionamento entre elas, vamos criar as tabelas do banco de dados da loja virtual utilizando para isso o programa SQL Developer, onde serão executadas as instruções SQL listadas abaixo:

Tabela Estado:

```
CREATE TABLE ESTADO
(ID_ESTADO NUMERIC(2),
```

DESCRICAO VARCHAR(30),

CONSTRAINT ESTADO_ID_PK PRIMARY KEY (ID_ESTADO));

Tabela Cidade:

CREATE TABLE CIDADE

(ID_CIDADE NUMERIC(5),

ID_ESTADO NUMERIC(2),

DESCRICAO VARCHAR(35),

CONSTRAINT CIDADE_ID_PK PRIMARY KEY (ID_CIDADE),

CONSTRAINT CIDADE_ID_ESTADO_FK FOREIGN KEY (ID_ESTADO) REFERENCES ESTADO);

Tabela Cliente:

CREATE TABLE CLIENTE

(ID_CLIENTE NUMERIC(6),

ID_CIDADE NUMERIC(5),

NOME VARCHAR(40),

CPF VARCHAR(14),

RG VARCHAR(12),

LOGRADOURO VARCHAR(50),

NUMERO VARCHAR(5),

BAIRRO VARCHAR(30),

CEP VARCHAR(10),

TELEFONE VARCHAR(13),

CELULAR VARCHAR(14),

EMAIL VARCHAR(40),

SEXO VARCHAR(10),

DATA_NASCIMENTO DATE,

NOME_USUARIO VARCHAR(20),

SENHA VARCHAR(8),

CONSTRAINT CLIENTE_ID_PK PRIMARY KEY (ID_CLIENTE),

CONSTRAINT CLIENTE_ID_CIDADE_FK FOREIGN KEY (ID_CIDADE) REFERENCES CIDADE);

Tabela Pedido:

CREATE TABLE PEDIDO

(ID_PEDIDO NUMERIC(12),

DATA_PEDIDO DATE,

ID_CLIENTE NUMERIC(6),

CARTAO_CREDITO VARCHAR(20),

NUMERO_CARTAO VARCHAR(20),

TITULAR_CARTAO VARCHAR(30),

VALIDADE_CARTAO DATE,

VALOR_FRETE NUMERIC(4,2),

VALOR_PEDIDO NUMERIC(5,2),

NOME_DESTINATARIO VARCHAR(35),

ENDERECO_DESTINATARIO VARCHAR(50),

CIDADE_DESTINATARIO VARCHAR(35),

ESTADO_DESTINATARIO VARCHAR(15),

CEP_DESTINATARIO VARCHAR(10),

CONSTRAINT PEDIDO_ID_PK PRIMARY KEY (ID_PEDIDO, DATA_PEDIDO),

CONSTRAINT PEDIDO_ID_CLIENTE_FK FOREIGN KEY (ID_CLIENTE) REFERENCES CLIENTE);

Tabela Frete:

```
CREATE TABLE FRETE
(ID_FRETE NUMERIC(6),
ID_ESTADO NUMERIC(2),
PESO_MINIMO NUMERIC(3,3),
PESO_MAXIMO NUMERIC(3,3),
VALOR NUMERIC(4,2),
CONSTRAINT FRETE_ID_PK PRIMARY KEY (ID_FRETE),
CONSTRAINT FRETE_ID_ESTADO_FK FOREIGN KEY (ID_ESTADO) REFERENCES ESTADO);
```

Tabela Fornecedor:

```
CREATE TABLE FORNECEDOR
(ID_FORNECEDOR NUMERIC(4),
ID_CIDADE NUMERIC(5),
NOME_EMPRESA VARCHAR(30),
ENDERECO VARCHAR(30),
CEP VARCHAR(10),
TELEFONE VARCHAR(13),
EMAIL VARCHAR(30),
CONSTRAINT FORNECEDOR_ID_PK PRIMARY KEY (ID_FORNECEDOR),
CONSTRAINT FORNECEDOR_ID_CIDADE_FK FOREIGN KEY (ID_CIDADE) REFERENCES CIDADE);
```

Tabela Categoria:

```
CREATE TABLE CATEGORIA
(ID_CATEGORIA NUMERIC(3),
```

NOME_CATEGORIA VARCHAR(15),

DESCRICAO VARCHAR(50),

CONSTRAINT CATEGORIA_ID_PK PRIMARY KEY (ID_CATEGORIA));

Tabela Produto:

CREATE TABLE PRODUTO

(ID_PRODUTO NUMERIC(12),

ID_CATEGORIA NUMERIC(3),

ID_FORNECEDOR NUMERIC(4),

NOME VARCHAR(30),

VALOR NUMERIC(5,2),

DESCRICAO VARCHAR(100),

ESTOQUE NUMERIC(4),

CONSTRAINT PRODUTO_ID_PK PRIMARY KEY (ID_PRODUTO),

CONSTRAINT PRODUTO_ID_CATEGORIA_FK FOREIGN KEY (ID_CATEGORIA) REFERENCES CATEGORIA,

CONSTRAINT PRODUTO_ID_FORNECEDOR_FK FOREIGN KEY (ID_FORNECEDOR) REFERENCES FORNECEDOR);

Tabela Itens do Pedido:

CREATE TABLE ITENS_PEDIDO

(ID_PEDIDO NUMERIC(12),

DATA_PEDIDO DATE,

ID_PRODUTO NUMERIC(12),

QUANTIDADE NUMERIC(4),

VALOR_UNITARIO NUMERIC(4,2),

CONSTRAINT ITEMS_PEDIDO_ID_PEDIDO_FK FOREIGN KEY (ID_PEDIDO) REFERENCES PEDIDO,

CONSTRAINT ITEMS_PEDIDO_DATA_PEDIDO_FK FOREIGN KEY (DATA_PEDIDO) REFERENCES PEDIDO,

CONSTRAINT ITEMS_PEDIDO_ID_PRODUTO_FK FOREIGN KEY (ID_PRODUTO) REFERENCES PRODUTO);

Tabela Cartão de Credito:

CREATE TABLE CARTAO

(ID_CARTAO NUMERIC(3),

NOME_CARTAO VARCHAR(15),

CONSTRAINT CARTAO_ID_PK PRIMARY KEY (ID_CARTAO));

- **Criando Usuários:**

Agora que o banco de dados da Loja Virtual já está criado, o próximo passo será a criação das contas de usuário, para as pessoas que irão ter acesso ao banco.

Lembrando que o único que pode criar contas de usuário e conceder e/ou revogar privilégios é o DBA. Para ser possível realizar esse estudo de caso, o professor (e meu orientador) Alex Sandro Romeo de Souza Poletto, criou uma conta de superusuario, para que eu pudesse fazer o papel de DBA neste estudo de caso, sendo possível, dessa maneira, demonstrar o funcionamento do controle de acesso ao banco de dados através da criação de contas de usuários e da concessão de privilégios.

Para esse estudo de caso, serão criadas apenas duas contas de usuário, para facilitar e simplificar o entendimento: uma conta para um estagiário e uma conta para um funcionário da empresa da área de T.I., aos quais serão concedidas as seguintes permissões;

- Funcionário: Privilégios de modificação e SELECT.
- Estagiário: Privilégio de SELECT.

A seguir pode ser observado a sintaxe de criação dos dois usuários que receberão os privilégios posteriormente:

Criação da conta de usuário Funcionário:

```
CREATE USER FUNCIONARIO
IDENTIFIED BY FEMA123;
```

Criação da conta de usuário Estagiário:

```
CREATE USER ESTAGIARIO
IDENTIFIED BY ADS123;
```

Repare que o comando CREATE USER permite a definição de um nome para um novo usuário, enquanto que o comando IDENTIFIED BY define a senha para acesso do usuário criado ao banco de dados.

- **Criando Visões (VIEW):**

A determinados usuários, como é o caso do usuário ESTAGIARIO nesse nosso estudo de caso, é concedido o privilégio SELECT, para que esse usuário possa consultar/visualizar informações que estão armazenadas no banco de dados, porém apenas dados não confidenciais podem ser consultados por esses usuários. Desse modo, informações como CPF, RG, nome de usuário e senha, por exemplo, que estão presentes na tabela CLIENTE, não podem ser visualizadas pelo ESTAGIARIO. Sendo assim, existe a necessidade de criar visões para controle de recuperação dos dados por usuários autorizados.

A seguir vamos verificar a sintaxe de criação da visão (view) que permite ter o controle de recuperação de dados dos clientes do banco de dados.

```
CREATE VIEW LISTARCLIENTES AS
SELECT NOME, CELULAR, EMAIL, DATA_NASCIMENTO, CIDADE
FROM CLIENTE;
```

Observe que a instrução CREATE VIEW define o nome da visão que está sendo criada e o comando AS antecede a consulta que será implementada através da visão, neste caso apenas dados não confidenciais podem ser recuperados, ou seja, quando o usuário ESTAGIARIO fizer uma consulta para verificar os Clientes da Loja Virtual, as únicas informações que ela irá visualizar são as que foram definidas na VIEW, isto é: o nome, o número do celular, o e-mail, a data de nascimento e a cidade dos clientes. Todas as outras informações são confidencias, de modo que o estagiário não tem privilégio para ter acesso a tais informações.

- **Concedendo Privilégios aos usuários:**

Agora cabe a mim, no papel de DBA, estabelecer os privilégios que cada usuário irá receber. Como foi especificado anteriormente a conta de usuário FUNCIONARIO irá receber privilégios de modificação e SELECT.

A seguir será demonstrado como é feita a concessão de privilégios para os usuários através das instruções SQL.

Concessão de privilégios ao FUNCIONARIO:

Para a conta de usuário FUNCIONARIO será concedido o privilégio de SELECT e modificação (INSERT, UPDATE e DELETE).

Abaixo estão os comandos para a concessão desses privilégios ao FUNCIONARIO:

- **CREATE SESSION:** Concede ao FUNCIONARIO o privilégio de criar novas sessões;
- **GRANT:** Define o privilégio concedido ao FUNCIONARIO;
- **ON:** É seguido pelos objetos que podem ser acessados pelo FUNCIONARIO;
- **TO:** É seguido pelo nome do usuário ao qual será concedido o privilégio;

```
GRANT CREATE SESSION
TO FUNCIONARIO;

GRANT SELECT, INSERT, UPDATE, DELETE
ON CLIENTE
TO FUNCIONARIO;

GRANT SELECT, INSERT, UPDATE, DELETE
ON PRODUTO
TO FUNCIONARIO;

GRANT SELECT, INSERT, UPDATE, DELETE
ON CATEGORIA
TO FUNCIONARIO;

GRANT SELECT, INSERT, UPDATE, DELETE
ON FORNECEDOR
TO FUNCIONARIO;

GRANT SELECT, INSERT, UPDATE, DELETE
ON CIDADE
TO FUNCIONARIO;

GRANT SELECT, INSERT, UPDATE, DELETE
ON ESTADO
TO FUNCIONARIO;
```

```
GRANT SELECT, INSERT, UPDATE, DELETE
ON CARTAO_CREDITO
TO FUNCIONARIO;

GRANT SELECT
ON PEDIDO
TO FUNCIONARIO;
```

Concessão de privilégios ao ESTAGIARIO:

Para a conta de usuário ESTAGIARIO será concedido apenas o privilégio de SELECT em algumas tabelas, ou seja, o usuário ESTAGIARIO não vai poder alterar nada dentro do banco de dados, ele apenas poderá fazer consultas no banco de dados, em tabelas previamente autorizadas e exibindo apenas dados autorizados (não confidenciais).

Abaixo estão os comandos para a concessão desses privilégios ao ESTAGIARIO:

- **CREATE SESSION:** Concede ao ESTAGIARIO o privilégio de criar novas sessões;
- **GRANT:** Define o privilégio concedido ao ESTAGIARIO;
- **ON:** É seguido pelos objetos que podem ser acessados pelo ESTAGIARIO;
- **TO:** É seguido pelo nome do usuário ao qual será concedido o privilégio;

```
GRANT CREATE SESSION
TO ESTAGIARIO;

GRANT SELECT
ON LISTARCLIENTES
TO ESTAGIARIO;
```

```
GRANT SELECT
ON PRODUTO
TO ESTAGIARIO;

GRANT SELECT
ON FORNECEDOR
TO ESTAGIARIO;

GRANT SELECT
ON CATEGORIA
TO ESTAGIARIO;
```

- **Revogando Privilégios**

Se por algum motivo for necessário mudar/revogar privilégios concedidos aos usuários do banco de dados, caberá também ao DBA executar essa tarefa. De modo que apenas, e tão somente, cabe ao DBA tanto conceder como revogar privilégios caso seja necessário.

Para revogar privilégios concedidos aos usuários deve-se fazer uso da instrução REVOKE, como é demonstrado na sintaxe a seguir.

- **REVOKE:** Instrução utilizada para remover privilégios de usuários ou grupo de usuários.
- **ON:** É seguido pelos objetos que podem ser acessados pelo ESTAGIARIO;
- **TO:** É seguido pelo nome do usuário ao qual será concedido o privilégio;

```
REVOKE tipo_do_privilegio
ON nome_do_objeto
TO usuário/role
```

Essa instrução está removendo um determinado tipo de privilégio, que será determinado pelo DBA, sobre um objeto do banco de dados de um usuário especifico ou de um grupo de usuários.

Vimos aqui nesse estudo de caso uma pequena demonstração de como funciona o método de controle de acesso através da criação de contas de usuário e da concessão de privilégios. Embora parecendo simples o controle de acesso é a principal e mais elementar medida de segurança a ser implementada num banco de dados. A criação das contas de usuário define quem vai poder ter acesso ao banco de dados e a concessão de privilégios define o que cada usuário pode fazer no banco de dados. No estudo de caso proposto nesse trabalho, observa-se que a conta de usuário ESTAGIARIO pode apenas fazer SELECT para consultar algumas informações (não confidenciais) de algumas tabelas. Já a conta de usuário FUNCIONARIO além do privilégio de fazer SELECT nas tabelas ele também pode fazer modificações nas tabelas, pois possui privilégios de INSERT, UPDATE e DELETE. A intenção desse estudo de caso foi deixar claro que sem o controle de acesso e sem a definição das permissões seria impossível controlar e garantir a segurança do banco de dados.

6.2 CONCLUSÃO

O tema de segurança em banco de dados/segurança da informação é um tema muito vasto, complexo e abrangente. Neste trabalho abordou-se, de uma forma mais sucinta, alguns dos principais tópicos que envolvem a segurança do banco de dados, falando um pouco sobre algumas das principais ameaças e apresentando algumas das principais medidas de segurança para combater essas ameaças.

Depois de muita pesquisa e muita leitura, para o desenvolvimento desse trabalho de conclusão de curso, pode-se concluir que mesmo o Administrador de Banco de Dados sendo o principal responsável pela gestão da segurança do banco de dados, é necessário convencer todos os colaboradores de que a proteção dos dados e a segurança da informação, ou seja, a segurança do banco de dados, deve ser uma prioridade para todos.

O objetivo de manter os dados seguros só será possível de ser alcançado se todos tiverem essa consciência e ajudarem seguindo as políticas de segurança da empresa. De nada adianta ter um bom sistema de segurança com muitas medidas de controle se a política de segurança não for cumprida por todos os colaboradores da empresa, então é fundamental deixar isso bem claro. Muitas ameaças acabam surgindo de dentro da própria empresa, seja por falha dos funcionários, por falta de atenção, descuido ou até mesmo por intenções maliciosas. Para conscientizar os colaboradores, o DBA pode investir em palestras, cursos e capacitações para disseminar uma política de segurança na empresa e mostrar os riscos existentes nas mais simples ações.

A cooperação dos colaboradores é essencial para o sucesso de uma estratégia de segurança, já que, mesmo com as melhores ferramentas de proteção e medidas de segurança bem estabelecidas, o elo mais fraco é sempre o usuário.

Para manter os dados da empresa em segurança, e consequentemente os dados dos seus clientes e parceiros de negócios, é preciso estar sempre atento aos erros, e as medidas que foram apresentadas para combater tais erros, que podem comprometer a segurança e que foram apresentados neste trabalho.

Também é importante relembrar nesta conclusão do trabalho que nenhum sistema, técnica, ferramenta, medida ou política de segurança é infalível. Se um hacker habilidoso e mal-intencionado estiver disposto e comprometido a invadir o seu banco de dados pode ser que ele consiga. Cabe ao DBA estabelecer o maior número de barreiras de segurança para dificultar ao máximo possível a vida do hacker de maneira a desestimular essa pessoa da tentativa de quebrar a segurança da sua empresa e ir procurar um alvo mais fácil, com menos proteção e que de menos trabalho para ele. Podemos fazer uma comparação com a vida real, se um ladrão quiser invadir a sua casa com o intuito de rouba-la, mas ele percebe que a sua casa é protegida por muros altos, cerca elétrica, câmeras de vigilância, cão de guarda, alarme, sensores de movimento, etc., e ele olha para a casa do vizinho e a casa do vizinho não tem nenhuma dessas proteções, provavelmente o ladrão irá desistir de invadir a sua casa e irá tentar invadir a casa do vizinho. O ladrão do mundo real, bem como o hacker do mundo virtual sempre irão procurar o caminho mais fácil, que seja menos trabalhoso para ele, ou seja que tenha menos barreiras de segurança entre ele e o seu objetivo.

Como ficou claro neste trabalho é função do DBA zelar pela segurança dos dados da empresa, mas para que isso seja possível é necessário que a empresa tenha profissionais

competentes e qualificados para cuidar dessa tarefa, não importa se esses profissionais sejam da própria empresa ou terceirizados. É preciso ter conhecimento sobre as tecnologias que garantem maior segurança e também conhecimento sobre os novos tipos de ameaças que surgem frequentemente. É obvio que investir em segurança tem um custo, mas as empresas precisam estar cientes que o custo de investir na segurança dos seus dados, com certeza, serão menores que os prejuízos de uma invasão, um roubo, ou um vazamento de informações sigilosas e cruciais para os negócios da empresa. Erros de segurança podem o vazamento e a exposição de dados confidenciais e a perda de informações valiosas para a empresa, por isso esses erros devem ser evitados a todo custo para que nunca aconteçam dentro da empresa.

É preciso estar sempre atento as questões de segurança dentro da empresa, é preciso estabelecer medidas de segurança e medidas de controle, treinar a equipe e criar uma política de segurança que seja simples, clara, direta e objetiva, para que todos os colaboradores da empresa possam entenda-la sem dificuldades e segui-la de maneira correta, afim de evitar que invasores explorem as possíveis brechas do sistema. A empresa precisa tratar a segurança dos seus dados com uma estratégia que requer investimento, dedicação, foco e capacitação quanto as principais ameaças e meios para enfrenta-las.

Enfim, deixar para agir somente depois que a empresa sofre um ataque é um grande erro. Parar de investir em segurança porque não houve nenhum ataque ou ameaça nos últimos tempos é outro. Não cometa esses erros se quiser garantir a segurança do banco de dados, o futuro da empresa e manter uma boa imagem que transmita confiança junto aos seus clientes e parceiros de negócios.

6.3 REFERÊNCIAS

ALBUQUERQUE, Ricardo. **Segurança no desenvolvimento de software: como garantir a segurança de sistemas para seu cliente usando a ISSO/IEC**. Rio de Janeiro: Editora Campus, 2002.

CASANOVA, Marco A.; MOURA, Arnaldo V.; **Princípios de Sistemas de Gerência de Bancos de Dados Distribuídos.** 1 ed. Rio de Janeiro: Editora Campus, 1985.

DATE, Christopher J. **Introdução a Sistemas de Banco de Dados**. 8 ed. São Paulo: Editora Elsevier, 2003.

ELMASRI, Ramez; NAVATHE Shamkant B.; **Sistemas de Banco de Dados.** 1 ed. São Paulo: Editora Pearson, 2005.

ELMASRI, Ramez; NAVATHE Shamkant B.; **Sistemas de Banco de Dados.** 6 ed. São Paulo: Editora Pearson, 2011.

LISKA, A.; GALLO T. **Ramsonware: Defendendo-se da Extorsão Digital.** 1 ed. São Paulo: Editora Novatec, 2017

OZSU, M. Tamer; VALDURIEZ, Patrick. **Princípios de sistemas de banco de dados distribuídos.** 2ª ed. Rio de Janeiro: Editora Campus, 2001.

PFLEEGER, Charles P.; PFLEEGER, Shari L. **Security in computing.** 4ª ed. Massachusetts: Editora Prentice Hall, 2012.

RAMAKRISHNAN, R.; GEHRKE, J. **Sistemas de Gerenciamento de Banco de Dados.** 3 ed. São Paulo: Editora AMGH, 2008.

SILBERSCHATZ, A.; KORTH, Henry F.; SUDARSHAN, S. **Sistema de Banco de Dados**. 6 ed. São Paulo: Editora Elsevier, 2006.

SILBERSCHATZ, A.; KORTH, Henry F.; SUDARSHAN, S. **Sistema de Banco de Dados**. 5 ed. São Paulo: Editora Elsevier, 2012.

STAMP, Mark. **Information security: principles and practice**. 2 ed. New Jersey: Editora John Wiley & Sons, 2011.