UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

DANIEL LUCAS DOS SANTOS

CONTROLE DE ACESSO EM SISTEMAS GERENCIADORES DE BANCO DE DADOS

MONOGRAFIA

CURITIBA
2014

DANIEL LUCAS DOS SANTOS

CONTROLE DE ACESSO EM SISTEMAS GERENCIADORES DE BANCO DE DADOS

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Me. Christian Carlos Souza Mendes

CURITIBA

2014

RESUMO

DOS SANTOS, Daniel L. **Controle de acesso em sistemas gerenciadores de banco de dados.** 2014. 50 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

A presente monografia descreve uma análise técnica sobre como o controle de acesso em sistemas gerenciadores de banco de dados são implantados, quais suas vantagens e vulnerabilidades e como atendem às necessidades de uma política de segurança. Este trabalho inicia com o levantamento sobre segurança da informação, servindo de base e sustentação à pesquisa dos principais mecanismos de controle de acesso disponíveis em sistemas gerenciadores de banco de dados. Em seguida apresenta os detalhes sobre o controle de acesso no banco de dados Oracle e finaliza com uma análise sobre os resultados da pesquisa e quais as perspectivas destes mecanismos atenderem as políticas de segurança.

Palavras-chave: Banco de Dados, Controle de Acesso, Segurança de Dados.

ABSTRACT

DOS SANTOS, Daniel L. **Control access on database management system.** 2014. 50 p. Monograph (Specialization in Configurationand Management of Servers and Network Equipments) - Federal Technological University of Paraná. Curitiba, 2014.

The present monograph describes a technical analysis over how the access control on data bank's managing systems is implanted, what are their advantages and vulnerabilities and how they serve the needs of a security policy. This work starts with the data collection over information security, serving as foundation to the research of the main access control mechanisms available on data bank managing systems. Next, it presents the details over control access the database Oracle and concludes with the analysis of the research results and what are the perspectives of these mechanisms to attend the security policies.

Keywords: Database, Control Access, Data Security.

LISTA DE SIGLAS

API - Interface de Programação de Aplicação
C - Confidencial
DAC – Controle de Acesso Discriminatório
DBA – Administrador de Banco de Dados
DDL – Linguagem de Definição de Dados
DML – Linguagem de Manipulação de Dados
MAC – Controle de Acesso Obrigatório
NPD – Domínio de Proteção Nomeada
PII – Informações Pessoalmente Identificáveis
PL/SQL – Linguagem Procedural/Linguagem de Consulta Estruturada
RBAC – Controle de Acesso Baseado em Papéis
S - Secreto
SGBD – Sistemas Gerenciadores de Banco de Dados
SQL – Linguagem de Consulta Estruturada
TI – Tecnologia de Informação
TS – Altamente Confidencial
U – Não Classificada
VPD - Banco de Dados Virtual

LISTA DE ILUSTRAÇÕES

Figura 1 – Gráfico de concessão de autorização.....25

Figura 2 – Gráfico de concessão de privilégio entre si.....25

Figura 3 – Tentativa de burlar o controle de segurança.....26

Figura 4 – Sintaxe para criar uma role.....38

Figura 5 – Exemplo de utilização de papéis.....39

Figura 6 – Sequência de verificação DAC.....45

Figura 7 - Como rótulos de dados e usuários trabalham juntos.....47

SUMÁRIO

1 INTRODUÇÃO 8
1.1 TEMA 8
1.2 PROBLEMAS E PREMISSAS 9
1.3 OBJETIVOS 10
1.3.1 Objetivos Gerais 10
1.3.2 Objetivos Específicos 10
1.4 JUSTIFICATIVA 11
1.5 PROCEDIMENTOS METODOLÓGICOS 11
1.6 ESTRUTURA 12
2 REFERENCIAIS TEÓRICOS 13
2.1 INTRODUÇÃO 13
2.1.1 Conceitos Sobre Segurança em Banco de Dados 13
2.1.2 Segurança da Informação 14
2.2 CONFIDENCIALIDADE 15
2.2.1 Privacidade de Comunicação 15
2.2.2 Armazenamento Seguro de Dados Sensíveis 16
2.2.3 Autenticação de Usuários 16
2.2.4 Controle de Acesso Granular 17
2.3 INTEGRIDADE 18
2.4 DISPONIBILIDADE 18
3 CONTROLE DE ACESSO EM SGBDS 19
3.1 INTRODUÇÃO 19
3.2 CONTRÔLE DE DADOS SEMÂNTICOS 19
3.2.1 Administrador de Banco de Dados 20
3.2.2 Gerenciamento de Visões 21
3.2.3 Controle de Segurança 21
3.2.4 Controle de Integridade Semântica 22
3.3 PRIVILÉGIOS 22
3.3.1 Privilégios de Sistema 23
3.3.2 Privilégios de Objeto 23
3.4 CONCESSÃO E REVOGAÇÃO DE PRIVILÉGIOS 24
3.5 CONTROLE DE ACESSO BASEADO EM PAPÉIS 26
3.6 CONTROLE DE ACESSO DISCRICIONÁRIO 28

3.7 CONTROLE DE ACESSO OBRIGATÓRIO 30
4 CONTROLE DE ACESSO NO SGBD ORACLE 33
4.1 ESTUDO DE CASO COM O SGBD ORACLE 33
4.2 PRIVILÉGIOS DE SISTEMAS E OBJETOS.....34
4.2.1 Privilégios de Sistema 35
4.2.2 Privilégios de Objeto.....36
4.3 USO DE PAPÉIS PARA ADMINISTRAR PRIVILÉGIOS.....38
4.3.1 Papeis de Banco de Dados 38
4.3.2 Papéis de Empreendimentos 39
4.3.3 Papéis Globais 40
4.3.4 Papéis de Aplicações Seguras.....40
4.4 USO DE STORED PROCEDURE PARA ADMINISTRAR PRIVILÉGIOS.....41
4.5 USO DE INSTALAÇÕES DE REDE PARA ADMINISTRAR PRIVILÉGIOS.....41
4.6 USO DE VISÕES PARA ADMINISTRAR PRIVILÉGIOS 41
4.7 SEGURANÇA EM NÍVEL DE REGISTRO 42
4.7.1 Segurança Baseada em Rótulo.....42
4.7.1.1 Conceito de *Virtual Private Database* (VPD) 43
4.7.1.2 Oracle Label Security.....44
4.7.1.3 Rótulos de Dados e Rótulos de Usuários Trabalhando Juntos 46
5 CONSIDERAÇÕES FINAIS 48
REFERÊNCIAS.....49

1 INTRODUÇÃO

Inicialmente este trabalho tem como objetivo abordar os mecanismos de segurança em sistemas gerenciadores de banco de dados (SGBD), através da consistência dos dados e a segurança de acesso.

1.1 TEMA

Pode-se observar que, paralelamente ao avanço da tecnologia de informação (TI), criou-se uma gigantesca quantidade de recursos disponíveis tanto para o processamento como para o armazenamento de dados. Esses recursos por sua vez, têm como finalidade criar, organizar e manter as informações das organizações, visando garantir a segurança e persistência das mesmas.

Os SGBDs surgem com a necessidade de armazenar, proteger e disponibilizar informações. Para todos os casos, sejam estes dados, registros triviais como a quantidade de um produto em estoque, ou o conteúdo sigiloso sobre a conta bancária de uma pessoa, ou ainda, as informações estratégicas de uma grande corporação, o tema segurança de bancos de dados enfrenta os mesmos desafios da segurança de informação, que é garantir a integridade, disponibilidade e confidencialidade dos dados.

A preocupação em implantar e manter ambientes seguros tem sido uma das principais, senão a principal ocupação dos administradores de redes e administradores de banco de dados (DBA). Pesquisas mostram que os ataques internos, ou seja, aqueles conduzidos por pessoas de dentro da própria empresa chegam a 18% dos casos estudados (VERIZON, 2014, p. 14). Profissionais responsáveis pela segurança da informação, estão continuamente criando, implantando e monitorando mecanismos que possam detectar e ou inibir as tentativas de acesso não autorizado ou pelo menos diminuir as chances de sucesso das tentativas de invasão sejam elas externas ou internas. O controle de acesso a SGBDs busca garantir que apenas usuários autorizados consigam ler, inserir ou

alterar dados, de acordo com regras de segurança e privilégios previamente estabelecidos.

1.2 PROBLEMAS E PREMISSAS

Um sistema de banco de dados é uma forma de armazenar dados e gerir informações para posterior recuperação ou atualização dessas informações por um usuário. Por consequência, deve evitar perdas de dados por falhas no sistema, acessos não autorizados e anomalias de dados (TANENBAUM, 2003, p. 21).

Os avanços tecnológicos têm proporcionado uma crescente melhora no gerenciamento da segurança da informação. Concorrente a estes avanços, as tentativas de acesso indevido aumentam na mesma proporção. O avanço da tecnologia pode, em alguns casos, acabar colocando muitas empresas em situação delicada. Problemas internos ou externos têm marcado presença no dia a dia das instituições, principalmente daquelas que não possuem política de segurança implantada e bem definida. Na medida em que o comércio eletrônico e os aplicativos na internet continuam crescendo, encontrar o equilíbrio entre a disponibilidade e a proteção dos dados, torna-se um desafio fundamental.

Diante deste contexto, os sistemas gerenciadores de banco de dados, assumem um papel cada vez mais importante, devendo proporcionar que seus usuários consigam compartilhar os dados de forma seletiva, com capacidade para limitar o acesso, fornecendo mecanismos de segurança e proteção.

Proteger dados contra o acesso não autorizado, destruição maliciosa, alterações acidentais ou inconsistências estão entre as principais funções de um sistema gerenciador de banco de dados. As perdas acidentais de consistência, normalmente são causadas por erros do sistema, esse tipo de perda são normalmente mais fácil de solucionar. Já os acessos maliciosos são mais difíceis de serem rastreados, pois podem ser decorrentes de acesso não autorizado e normalmente causam alterações ou destruição de dados (PISSINOU, 1994 apud ACKERMANN, 2003 p. 13).

Diante deste cenário, onde a informação e o controle de acesso a estas

informações despontam como um dos bens mais valiosos de uma empresa surge o questionamento: o controle de acesso em sistemas gerenciadores de banco de dados é suficiente para garantir a confidencialidade, integridade e disponibilidade da informação de acordo com a política de segurança? Como são feitos os controles de acesso em SGBDs? Como é implantada e gerenciada a concessão e revogação de privilégios?

1.3 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.3.1 Objetivos Gerais

Fazer uma análise técnica sobre os mecanismos de controle de acesso em SGBDs e detalhar particularmente como são implantados em um banco de dados Oracle.

1.3.2 Objetivos Específicos

- Descrever os conceitos sobre segurança da informação e traçar seus paralelos com a segurança em Banco de Dados.
- Descrever os tipos mais conhecidos de controles de acesso em SGBD, os modelos de acesso discricionários e obrigatórios;
- Abordar particularmente os itens que fazem referência ao controle de acesso no SGBD Oracle, tipos de privilégios disponíveis e como podem ser usados*;*
- Verificar como o controle de acesso em SGBDs atende as necessidades de uma política de segurança.

1.4 JUSTIFICATIVA

São cada vez maiores as quantidades de informações armazenadas pelas empresas. Junto com este crescimento, aumentam também as responsabilidades do DBA. Quanto maiores os volumes de dados, mais complexos se tornam os mecanismos para garantir a disponibilidade da informação e controle de acesso às mesmas. O aumento dos números de usuários e a forma de acesso ficam cada vez mais complexas.

É preciso pesquisar e entender as necessidades da segurança de acesso, para poder criar mecanismos que garantam a qualidade dos dados, direitos de propriedade intelectual e sobrevivência do banco de dados (ELMASRI; NAVATHE, 2012, p. 563).

1.5 PROCEDIMENTOS METODOLÓGICOS

Esta é uma pesquisa de caráter teórico a respeito de segurança no controle de acesso a SGBD, sendo utilizados como fontes de pesquisa: livros, artigos científicos, dissertações, revistas, normas técnicas, internet e outros. O método de estudo, essencialmente bibliográfico, parte de uma revisão sobre o conceito básico de segurança da informação e seus três pilares de sustentação: a confidencialidade, a integridade e a disponibilidade (ALBUQUERQUE, 2002). Em seguida levanta os conceitos sobre o controle de acesso padrão de um SGBD, controles semânticos, privilégios, concessões e revogações, papéis, modelos de controle de acesso discricionários e os modelos de controle de acesso obrigatórios (ELMASRI; NAVATHE, 2012, cap. 24).

1.6 ESTRUTURA

A monografia é composta por cinco capítulos, começando por este de caráter introdutório, onde será apresentado o tema, objetivos pretendidos, a justificativa para escolha do tema e a disposição do problema. Além disso, serão apresentados o procedimento metodológico adotado e a estrutura da monografia.

O segundo capítulo aborda os referenciais teóricos, descrevendo os conceitos básicos sobre segurança, sua relevância para a segurança dos dados e tipos de controles.

O capítulo 3 trata dos controles de acesso padrões, descrevendo os controles semânticos, o que são privilégios, quais são os tipos de concessões e o funcionamento de atribuição e revogação. Apresenta o conceito de controle de acesso baseado em papéis e como são controlados pelos SGBDs. E finalmente conclui o estudo com a apresentação dos controles de acesso discricionários e obrigatórios.

O quarto capítulo é dedicado ao estudo de controle de acesso em um SGBD específico, no caso escolhemos o banco de dados Oracle, por ser considerado um dos mais completos em termos de controle de acesso a dados. São abordados os privilégios de sistemas e objetos e segurança em nível de registro.

No quinto e último capítulo relatamos as conclusões desta pesquisa, apontando seus resultados e perspectivas futuras.

2 REFERENCIAIS TEÓRICOS

2.1 INTRODUÇÃO

Este capítulo pretende apresentar os conceitos básicos sobre a segurança da informação, suas correlações com a segurança em SGBDs e ainda, descrever o desafio e a complexidade dos mecanismos de segurança para manter o equilíbrio entre a necessidade de concessão de privilégios e a proteção de informações privadas.

2.1.1 Conceitos Sobre Segurança em Banco de Dados

Quando se fala de segurança em banco de dados, de acordo com Ramakrishnan e Gehrke (2008 cap. 21), três objetivos principais devem ser alcançados: a confidencialidade, a integridade e a disponibilidade. A confidencialidade diz respeito ao acesso a informação por pessoa não autorizada, ou quando um usuário não deve ter acesso a dados confidenciais de outro usuário. A integridade refere-se à alteração de dados não autorizada, um cliente pode consultar seu saldo bancário, mas não pode alterar os valores deliberadamente. E por fim, a disponibilidade, trata da garantia que a informação estará disponível quando necessária. Para que se obtenha sucesso na busca destes objetivos, é preciso em primeiro lugar desenvolver uma política de segurança clara e consistente capaz de descrever que tipos de ações são de caráter obrigatório.

Uma política de segurança consistente deve ser aplicada em diversos níveis, começando pela definição dos tipos de dados e qual é a sensibilidade deles. Em seguida é preciso delimitar quais são os dados que precisam ser protegidos e quais usuários terão acesso a qual parte destes dados. Posteriormente são implantados os procedimentos de segurança do SGBD, do sistema operacional implícito, e também os métodos que irão garantir a segurança ao acesso físico dos prédios e

equipamentos que armazenam as informações (RAMAKRISHNAN; GEHRKE, 2008 cap. 21).

Falhas de segurança em sistemas operacionais ou em conexões de rede podem arruinar com sistemas de segurança de um SGBD. Se uma pessoa não autorizada obtiver acesso como administrador em um banco de dados, terá todos os privilégios inerentes a conta de um administrador, podendo causar perda de dados alterações e quebras de sigilo irreversíveis. Da mesma forma, um funcionário autorizado a acessar dados confidenciais, porém mal intencionado, poderá por em riscos a segurança do SGBD. Ou ainda, um usuário que escolhe uma senha fraca ou não guarda sigilo da mesma, também estará causando uma brecha na política de segurança. Erros como esses são responsáveis por uma boa porcentagem das falhas em sistemas de segurança. O foco deste trabalho são os mecanismos de controle de acesso a SGBD, portando não entraremos nos detalhes dos aspectos de segurança físicos, humanos, de redes e sistemas operacionais (RAMAKRISHNAN; GEHRKE, 2008 cap. 21).

2.1.2 Segurança da Informação

O tema segurança e extremamente vasto e não caberia falar sobre toda sua abrangência neste trabalho. Por este motivo o foco será a segurança da informação. Quando se pensa em segurança da informação deve-se, ao invés de questionar quanto se deseja de segurança, perguntar qual nível de disponibilidade da informação necessita-se ou quais são os requisitos mínimos de confidencialidade. Entre os diversos aspectos sobre segurança, pelo menos três deles são essenciais. (ALBUQUERQUE, 2002)

- Confidencialidade;
- Integridade;
- Disponibilidade.

2.2 CONFIDENCIALIDADE

A confidencialidade lida com a prevenção de leitura não autorizada de informações (STAMP, 2011, p. 2). 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 (ALBUQUERQUE, 2002). A confidencialidade é uma questão chave quando se trata de bancos de dados, por causa do problema de inferência, em que um usuário pode acessar dados sensíveis de forma indireta. Inferência é uma forma de obter acesso a dados confidenciais a partir de dados não confidenciais. O problema de inferência é uma vulnerabilidade sutil em segurança de banco de dados (PFLEEGER, 2012, p. 17-19).

A maior dificuldade no gerenciamento da confidencialidade ocorre quando dois usuários possuem o mesmo acesso a determinada informação ou tabela no SGBD, mas cada um destes só deve acessar uma parte da informação. Um sistema seguro precisa garantir que a informação privada somente possa ser vista por quem tem direito. Sendo assim a confidencialidade possui várias dimensões diferentes (ACKERMANN, 2003, p. 19).

- Privacidade de comunicação
- Armazenamento seguro de dados sensíveis
- Autenticação de usuários
- Controle de acesso granular

2.2.1 Privacidade de Comunicação

A comunicação é uma das variáveis mais importantes dentro de uma organização, pois tem a finalidade de ligar as demais variáveis umas com as outras.

De que maneira pode-se assegurar a privacidade na comunicação de dados? A privacidade é um conceito bastante amplo e tem diferentes visibilidades que variam de acordo com o tipo de informação e as necessidades da organização. Para uma empresa comercial, a privacidade pode estar no segredo comercial sobre produtos e processos, nas análises de concorrência ou ainda nas estratégias de marketing e vendas. Para uma um instituição governamental, a privacidade exige competência para manter em sigilo dados pessoais de milhares de pessoas, além de proteger informações que afetam a segurança do país.

2.2.2 Armazenamento Seguro de Dados Sensíveis

Há vários razões para que dados sejam vistos como sensíveis. Assuntos pessoais e privados, comunicações, segredos comerciais profissionais, planos da empresa para o marketing ou finanças, informação militar, ou os planos do governo para pesquisas, compras ou outras ações.

Dados sensíveis são informações de caráter particular que podem causar discriminação ou censura do seu proprietário quando for objeto de tratamento não autorizado, como por exemplo, informações raciais, étnica, religiosa, filosófica ou moral. Dados confidenciais devem ter sua integridade e privacidade garantida quando armazenados em um BD.

2.2.3 Autenticação de Usuários

Como evitar que uma pessoa se passe por outra para obter acesso privilegiado? A autenticação de usuários consiste na verificação tanto da identidade do usuário como dos sistemas e ou processos que pretende utilizar.

Os sistemas de autenticação de usuários se dividem em três categorias (PFLEEGER, 2012, p. 219):

- Baseada no conhecimento (o que se sabe) – uso de senhas, chave de criptografia, número de identificação pessoal (*personal identificator number* -

PIN), frases secretas ou nome de solteira da mãe.

- Baseada na propriedade (o que se tem) – caracteriza-se por um objeto físico que o usuário possui, como um cartão inteligente (*smart card*), uma chave física ou o uniforme de trabalho.
- Baseada em características (o que se é) – são autenticadores chamados de biométricos e que se baseiam em características físicas do usuário, como impressão digital, os padrões de voz de uma pessoa ou um rosto (foto).

2.2.4 Controle de Acesso Granular

A granularidade diz respeito ao nível de detalhamento, de linha e coluna, com o qual se deseja permitir o acesso a informação para determinado usuário. O controle e manutenção do acesso granular aos dados, principalmente para organizações que possuem vários bancos de dados, é um problema difícil de resolver através de um método ou solução única. O controle de acesso precisa ser hábil para isolar partes do banco de dados, de forma que o acesso não seja aberto a todos ou censurado a todos.

Existe uma diferença entre a autenticação a autorização e o controle de acesso. Ao autenticarmos um usuário, sua identidade é verificada certificando que ele é autorizado a acessar uma determinada aplicação. A autorização é o processo que fará a verificação dos privilégios que este usuário possui para esta aplicação. E o controle de acesso é a maneira como será limitado o acesso do usuário as informações físicas na aplicação (ACKERMANN, 2003, p. 20).

Quanto maior a granularidade, maior será o número de permissões a serem definidas. Definir as permissões para um grupo de usuários gerentes, por exemplo, necessita menos detalhamentos do que se tiver que definir permissões para cada gerente particularmente. Um gerente pode necessitar acesso a tabela de salários, mas não a todos os salários, somente os dos funcionários do seu departamento.

2.3 INTEGRIDADE

A integridade lida com a prevenção, ou pelo menos a detecção de alteração de dados não autorizada (STAMP, 2011, p. 2). 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 (PFLEEGER, 2012, p. 329).

Existem diversos fatores que podem comprometer a integridade dos dados, esses fatores podem ter cunho intencional ou não, como por exemplo: usuários mal-intencionados, *hackers,* erros de *software*, ação de *malware*, falhas de *hardware*, erro humano, entre outros. Independente da forma ou motivo pela qual os dados perdem sua integridade, a pergunta que devemos fazer é: qual a importância destes dados para a empresa e quanto ela irá gastar para recuperá-los? Não restam dúvidas de que é de fundamental importância para as empresas manter a integridade dos dados ou pelo menos, caso sejam corrompidos, construir mecanismos que garantam a sua recuperação o mais rapidamente possível.

2.4 DISPONIBILIDADE

A disponibilidade de um sistema é indicada pela quantidade de vezes que foi capaz de executar uma tarefa solicitada, sem falhas, dividido pelo número de vezes que a tarefa foi solicitada (ALBUQUERQUE, 2002).

A perda de disponibilidade ocorre quando ela deixa de estar acessível para quem dela necessita. Como nos casos onde há perda de conexão com um sistema, queda de um servidor, falhas internas ou externas de um equipamento. No caso de ameaças a redes de computadores ou sistemas, essas ameaças podem vir de agentes maliciosos.

3 CONTROLE DE ACESSO EM SGBDS

3.1 INTRODUÇÃO

Este capítulo irá discutir a maneira como são normalmente implantados, através do uso da linguagem de consulta estruturada (*structured query language* - SQL), os controles de acesso nos SGBDs relacionais.

Inicialmente serão demonstradas as funcionalidades do controle de dados semânticos, como auxiliam no gerenciamento de visões, no controle de segurança e de integridade semântica e também uma breve visão das atribuições e responsabilidades de um administrador de banco de dados.

Na sequência será apresentado o conceito de privilégios e suas duas ramificações: os privilégios de sistema e os privilégios de objeto. E em seguida como são administradas as concessões e revogações de privilégios.

Finalizando o capítulo, serão discutidos os três principais mecanismos de controle de acesso em SGBDs: o controle de acesso baseado em papéis, o controle de acesso discricionário e o controle de acesso obrigatório.

3.2 CONTRÔLE DE DADOS SEMÂNTICOS

O controle semântico dos dados contidos em um SGBD e uma das suas funcionalidades mais importantes. Ela é responsável pelo devido gerenciamento das visões, pelo controle de segurança de acesso, pela manutenção da integridade semântica e também pela disponibilidade da informação.

Os modelos semânticos surgiram com a necessidade de aprimorar o nível de detalhamento das aplicações. Os SGBDs comerciais, em geral não oferecem um nível adequado e que atenda a todas as necessidades de segurança das aplicações. Mesmo assim os mecanismos de controle de dados semânticos são largamente utilizados como ferramentas auxiliares no desenvolvimento de aplicações.

Segundo Özsu e Valduriez (2001, p. 170), a principal função do controle semântico de dados é garantir que usuários autorizados, ao executarem ações, não comprometam a integridade do banco de dados. Administrar o controle de dados semântico faz parte das tarefas de responsabilidade do DBA e abrangem:

- Gerenciamento de Visões;
- Controle de Segurança;
- Controle de Integridade Semântica.

3.2.1 Administrador de Banco de Dados

Um administrador de banco de dados é responsável por várias funções referentes ao controle de um SGBD. De acordo com Silberschatz, Korth e Sudarshan (1999 p. 14) as principais são:

- Definição do esquema;
- Definição da estrutura de dados e métodos de acesso;
- Esquema e modificações na organização física;
- Fornecer autorização de acesso ao sistema;
- Especificação de regras de integridade.

O DBA tem a importante tarefa de fazer a ligação entre as funcionalidades do SGBD com os sistemas que o utilizam. Ele deve prover aos analistas de sistemas e desenvolvedores, as informações necessárias para o desenvolvimento de aplicações de banco de dados (ACKERMANN, 2003 p. 33).

3.2.2 Gerenciamento de Visões

Uma visão é “uma relação virtual, definida como o resultado de uma consulta sobre relações básicas (ou relações reais) – mas não materializadas como uma relação básica – armazenada no banco de dados” (ÖZSU; VALDURIEZ, 2001, p. 171). Através das visões e possível proteger o acesso direto as tabelas, criando uma espécie de tabela virtual, onde são selecionados apenas os registros das tabelas desejadas, ocultando aquilo que não se queira mostrar. O acesso por visões é uma forma simples de manter os dados protegidos, permitindo que o usuário veja as informações sem poder manipulá-las (ÖZSU; VALDURIEZ, 2001, p. 171).

Os SGBD são bastante restritivos quanto a atualizações através de visões. As visões só podem ser atualizadas se for possível propagar as suas relações básicas sem que haja duplicidades. Para que isso seja possível a visões dever ser gerada de relações únicas. Visões criadas a partir de junções ou uniões não podem ser atualizadas pela visão (ÖZSU; VALDURIEZ, 2001, p. 174, 175).

3.2.3 Controle de Segurança

O controle de segurança deve proteger os dados, de acesso não autorizado. Um dos aspectos da segurança está relacionado com a proteção dos dados, que pode, por exemplo, ser implantada através do uso de criptografia. Outro aspecto da segurança se refere ao controle de autorização que é um processo intimamente ligado aos SGBD. 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. Esse controle é implantado de forma centralizada em sistemas de arquivos onde são especificados subconjuntos de objetos por seus predicados (ÖZSU; VALDURIEZ, 2001, p. 176).

3.2.4 Controle de Integridade Semântica

A integridade semântica deve garantir que um dado inserido em uma linha da tabela tenha um valor válido. E para que este valor seja válido ele deve ser do mesmo tipo de dado definido na especificação da coluna na tabela. Por exemplo, um atributo definido como data, só deverá armazenar informações relativas à data. Se por algum motivo o SGBD permitir que se grave outro tipo de dado diferente do definido, teremos uma violação da integridade semântica.

Garantir a consistência em um SGBD é uma atividade difícil e importante. Para seu sucesso é necessário satisfazer um conjunto de regras chamadas de restrições de integridade semântica. Essas regras devem garantir que o controle de concorrência dos programas não cause inconsistências nos dados do SGBD. Programas que violem as restrições de integridade devem ser rejeitados (ÖZSU; VALDURIEZ, 2001, p. 188).

3.3 PRIVILÉGIOS

Os privilégios, também chamados de autorizações, são concessões únicas feitas a usuários ou grupos de usuários e que define a maneira como deverá ser acessado determinado objeto. Através dos privilégios são concedidas as autorizações para modificar ou acessar determinados recursos do BD; como por exemplo, autorização para consultar uma tabela, permissão para que um usuário se conecte ao BD, criação de tabelas no próprio escopo, fazer consultas nos registros de tabelas de outros escopos, ou utilizar procedimentos de outros escopos do BD (HAZEL, 2001, apud ACKERMANN, 2003 p. 34).

Essas autorizações também são armazenadas nos catálogos dos próprios BD, visto que os grupos de autoridade já possuem privilégios predefinidos, concedem implicitamente privilégios a seus membros. Quando um usuário é criado ele não possui nenhum privilégio. Existe uma grande variedade de privilégios que podem ser

concedidos. Eles são divididos e dois tipos diferentes:

- Privilégios de sistema
- Privilégios de objeto

3.3.1 Privilégios de Sistema

Receber privilégios de sistema dá ao usuário permissão para criar e manipular objetos no banco de dados, mas não dá acesso aos objetos que já existem no BD.

Os privilégios de sistema permitem que usuários executem ações específicas de sistema ou ações particulares de um objeto, como por exemplo, a criação, alteração e remoção de tabelas, removerem registros de tabelas e executar *stored procedures*. Normalmente por serem privilégios muito poderosos, são concedidos apenas administradores e desenvolvedores (HAZEL, 2001, apud ACKERMANN, 2003 p. 35).

3.3.2 Privilégios de Objeto

Quando um objeto é criado no BD (uma tabela, por exemplo), quem cria este objeto é o seu dono. Por padrão apenas o dono de um objeto tem permissão para realizar operações com este objeto. Para que outros usuários também utilizem este objeto e necessário que privilégios sejam concedidos. Privilégios de objeto permitem que uma ação específica possa ser executada um objeto específico. Estas ações podem ser comandos DML (*Data Manipulation Language*) que permitem a execução

de seleções, alterações, inserções ou deleções; ou comandos DDL (*Data Dictionary Language*) que permitem a criação de índices, novas tabelas, adição e remoção de atributos, remoção de tabelas e criação de chave estrangeira para referenciar tabelas de outros esquemas ou donos.

Usuários podem receber apenas alguns, todos ou combinações destes privilégios. As permissões de comandos DML permitem ações diretamente com os objetos, e as permissões de comandos DDL dão o direito de fazer modificações no esquema do banco de dados (SILBERSHATZ; KORTH; SUDARSHAN, 1999, p. 637).

3.4 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, 1999, p. 639).

Para poder conceder ou remover privilégios em bases de dados relacionais, a linguagem SQL padrão propõe a utilização dos 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.

Um privilégio é concedido sempre a partir do DBA. Esta passagem de privilégios de um usuário para outro pode ser entendida como um gráfico de autorização, onde $U_i \rightarrow U_j$. Suponhamos uma autorização de seleção na tabela aluno do banco de dados do sistema acadêmico de uma universidade. O DBA concede autorização a três usuários U_1, U_2, e U_3 que também recebem o direito de repassarem seus privilégios a outros usuários (SILBERSHATZ; KORTH; SUDARSHAN, 1999, p. 639). Na figura 1 vemos a representação deste gráfico.

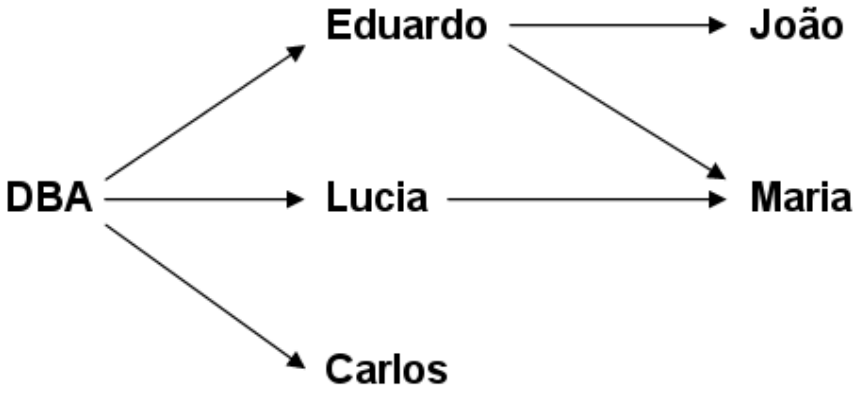

Figura 1 – Gráfico de concessão de autorização.
Fonte: Adaptado de Silbershatz, Korth e Sudarshan (1999)

Os nomes na figura representam os usuários e as setas representam de quem e para quem está sendo concedido o privilégio. Pode-se observar que Eduardo, Lucia e Carlos recebem privilégios do DBA. João recebe privilégios de Eduardo e Maria recebe privilégios tanto de Eduardo como de Lucia. Se o DBA revogar os privilégios de Eduardo, João e Maria automaticamente perdem os privilégios que receberam de Eduardo, porém Maria continuará com acesso a tabela aluno por conta do privilégio recebido de Lucia.

Atenção especial deve ser tomada quando usuários, sem conhecimento ou mal intencionados, burlam as regras de concessão de privilégios, concedendo privilégios entre si. Imaginemos que no exemplo anterior, Lucia conceda privilégios a Carlos e Carlos privilégios a Lucia, como mostra a figura 2.

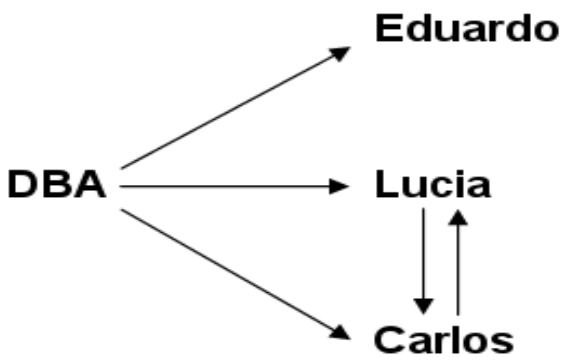

Figura 2 – Gráfico de concessão de privilégio entre si.
Fonte: Adaptado de Silbershatz, Korth e Sudarshan (1999)

Se o DBA revogar os privilégios concedidos a Lucia e Carlos, as setas que concedem privilégios mútuos entre Lucia e Carlos não fazem parte do caminho que inicia com o DBA e ambos manterão os privilégios como mostra a figura 3.

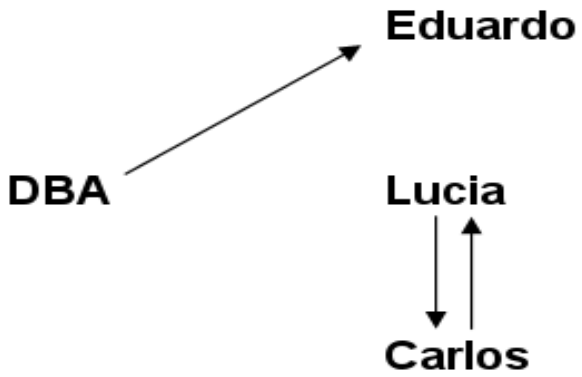

Figura 3 – Tentativa de burlar o controle de segurança.
Fonte: Adaptado de Silbershatz, Korth e Sudarshan (1999)

Para que isto não ocorra, o banco de dados exige que as setas de autorização façam parte de algum caminho que tenha como origem o administrador do banco de dados.

3.5 CONTROLE DE ACESSO BASEADO EM PAPÉIS

O aspecto principal no uso de papeis está na sua capacidade de organizar e prover um grande número de privilégios em objetos, com flexibilidade, diminuindo o esforço necessário na administração de políticas de segurança complexas. Porém, para os sistemas disponíveis atualmente, a granularidade do controle de acesso não são, sozinhos, suficientes para atender os requisitos de aplicações particulares. O controle de acesso em tabelas de banco de dados relacionais, por exemplo, não pode ser definido a um subconjunto de registros específicos, fazendo-se necessário a utilização de visões do banco de dados para satisfazer as necessidades.

Um papel é estabelecido de acordo com o conceito de domínio de proteção

nomeado (*named protection domain* - NPD). Dentro deste modelo, um papel e uma imagem de um conjunto de privilégios estabelecidos e utilizados pelos administradores de sistemas de usuários. Em um papel são definidos privilégios e também outros papéis e sua sintaxe e representada da seguinte maneira:

$$\mathbf{r = role\ (priv_{1,} \ldots\ldots, pirv_n, r_{1,} \ldots., r_n\ )}$$

Onde **r** representa o nome atribuído ao papel $\mathbf{priv_{1,} \ldots\ldots, pirv_n,}$ são os privilégios concedidos diretamente ao papel e $\mathbf{r_{1,} \ldots., r_{n,}}$ são nomes de sub-papéis concedidos a **r**.

O conceito básico do controle de acesso baseado em papeis (*role-based access control* - RBAC) se apóia numa abordagem para restringir os privilégios de usuários autorizados e é uma alternativa aos sistemas de controle de acesso do tipo MAC e DAC. O conceito de controle de acesso baseado em papéis apareceu junto com os primeiros sistemas computacionais multiusuários interativos. A idéia central do RBAC é fazer a associação de permissões a papéis e então associar estes papéis a usuários. Estes papéis podem ser criados de acordo com os diversos cargos dentro de uma organização, e assim os usuários são associados aos papéis de acordo com suas funções e responsabilidades. Vários usuários podem ser indicados para um mesmo papel. Os atributos de segurança comuns a um papel são associados ao seu nome, assim qualquer usuário designado para este papel recebe automaticamente os seus direitos e privilégios (ELMASRI; NAVATHE, 2011, p. 572).

Outra tarefa que os papéis podem executar é a exclusão mútua de papéis, muito útil quando há a necessidade de impedir que um usuário realize sozinho o trabalho que exige o envolvimento de duas ou mais pessoas, impedindo assim a conivência. Dois papéis são considerados mutuamente exclusivos quando ambos não puderem ser usados ao mesmo tempo por um usuário. Existem dois tipos de exclusão mútua (ELMASRI; NAVATHE, 2011, p.573):

- Estática - chamada de *exclusão em tempo de autorização*, onde dois papéis, indicados como mutuamente exclusivos, não podem fazer parte

da autorização de um usuário ao mesmo tempo.

- Dinâmica – chamada de *exclusão em tempo de execução*, quando dois papéis podem ser autorizados a um usuário desde que não sejam ativados ao mesmo tempo.

A hierarquia de papéis organiza as linhas de autoridade e responsabilidade, conectando papéis de menor autoridade (junior) a papéis progressivamente mais elevados na hierarquia (sênior). Desta forma um usuário que tem um papel recebe automaticamente os papéis inferiores na hierarquia (ELMASRI; NAVATHE, 2011, p. 573).

Os modelos RBAC oferecem recursos de flexibilidade, neutralidade política e suporte para administrar a segurança, tornando-se excelentes ferramentas para serem usadas no desenvolvimento de aplicações Web seguras. Os modelos MAC e DAC tradicionais não oferecem os recursos do RBAC, enquanto RBAC inclui as capacidades dos modelos DAC e MAC e são de fácil implantação pela internet (ELMASRI; NAVATHE, 2011, p. 573).

3.6 CONTROLE DE ACESSO DISCRICIONÁRIO

Os controles de acesso discricionários são baseados na concessão e revogação de privilégios. Um privilégio permite que um usuário acesse um determinado objeto de dado e execute ações pré-definidas. O usuário que cria um objeto no banco de dados tem automaticamente todos os privilégios referentes ao objeto. Por conseqüência, o SGBD monitora como estes privilégios são concedidos ou revogados, controlando para que apenas usuários autorizados tenham acesso aos objetos (RAMAKRISHNAN; GEHRKE, 2008, P. 578). Trata-se de um sistema que foi inicialmente desenvolvida para a linguagem SQL e posteriormente boa parte dos SGBDs passaram a utilizar variações do mesmo (ELMASRI; NAVATHE, 2011, p. 567).

O controle de acesso do tipo discricionário (discretionary *access control* - DAC) do SGBD mantém o controle ao acesso de dados em apenas uma direção. O administrador irá conceder privilégios aos usuários que irão designar as operações permitidas por estes, como leitura ou alteração por exemplo. Para o usuário acionar ou efetuar alguma tarefa deverá possuir os privilégios pertinentes para aquela ação (SANDHU, 1994, p. 145-160).

Existem dois níveis de atribuição de privilégios (ELMASRI; NAVATHE, 2011, p. 567):

- **Em nível de conta** – especificam quais são os privilégios que a conta de um usuário tem, independente das relações desta conta com o BD.
- **Em nível de relação (ou tabela)** – controla individualmente quais as relações ou visões poderão ser acessadas no BD.

Privilégios em nível de conta capacitam uma conta a criar *schemas* (**CREATE SCHEMA**), tabelas (**CREATE TABLE**) e visões (**CREATE VIEW**). Também incluem os privilégios **ALTER**, para fazer mudanças no *schema*, como inclusão e exclusão de atributos; **DROP**, para exclusão de relações ou visões; **MODIFY**, para inserir, excluir ou atualizar linhas; e **SELECT**, para executar consultas no BD. Todos esses privilégios se aplicam a conta em geral, portanto se uma conta não possuir o privilégio de **CREATE TABLE**, outras relações não poderão ser criadas baseadas nesta conta (ELMASRI; NAVATHE, 2011, p. 567).

Privilégios em nível de relação aplicam-se as permissões nas tabelas de base e visões. Elas especificam relações individuais que cada usuário pode ter com cada um dos comandos que podem ser aplicados e em alguns casos, também sobre os privilégios de uma coluna. Estas concessões costumam seguir um modelo conhecido como matriz de acesso. Em uma matriz, usuários, contas e programas são representados como sujeitos, e as relações, registros, colunas e visões, representam objetos. Cada posição na matriz representa o tipo de privilégio que um sujeito tem sobre um objeto (ELMASRI; NAVATHE, 2011, p. 567).

O método de concessão de privilégios consiste basicamente em dar

permissões ou revogá-las através de declarações na própria linguagem de consulta. A SQL suporta o controle de acesso discricionário através dos comandos **GRANT** e **REVOKE**. O primeiro concede os privilégios a tabelas e visões e tem a seguinte sintaxe (RAMAKRISHNAN; GEHRKE, 2008, P. 579):

GRANT tipo_de_privilegio **ON** nome_do_objeto **TO** nome_do_usuario;

O segundo é o comando complementar que permite a retirada de privilégios, e possui a seguinte sintaxe:

REVOKE tipo_de_privilegio **ON** nome_do_objeto **FROM** nome_do_usuario;

3.7 CONTROLE DE ACESSO OBRIGATÓRIO

De acordo com ELMASRI; NAVATHE (2011, p. 570), as técnicas de controle de acesso discricionário, concedendo e revogando privilégios em relações, tem sido a maneira tradicionalmente utilizada como mecanismo de segurança em sistemas de banco de dados relacional. Trata-se de um método onde você permite tudo ou não permite nada. Porém, para muitas aplicações há a necessidade de se criar uma política de segurança adicional, a fim de classificar dados e usuários com bases em classes de segurança. A técnica utilizada é conhecida como controle de acesso obrigatório (MAC – Mandatory Access Control), e normalmente é combinada com os mecanismos de acesso discricionários. Uma observação importante é que na maioria dos SGBDs comerciais, são oferecidos apenas os métodos para controle de acesso discricionário (ELMASRI; NAVATHE 2011, p. 570).

Muitas organizações governamentais, militares ou de Inteligência, assim como sistemas industriais e corporativos, necessitam de algum tipo de segurança multinível. Diante desta necessidade, alguns SGBDs, como a Oracle, por exemplo,

implantam versões especiais que incorporam controle de acesso obrigatório para uso governamental.

O controle de acesso obrigatório não se baseia apenas na identidade do usuário, sendo assim, os privilégios a determinado objeto não é estabelecido por sua identidade. A classificação do sujeito e do objeto dentro do sistema e que será o fator responsável pelo controle.

Cada objeto protegido recebe uma classificação, ou *label,* que demonstra a importância do recurso representado por aquele objeto. O sujeito também possui uma classificação de segurança, ou *clearance*, que representa a confiança que o sistema possui neste usuário de que ele não irá repassar as informações para pessoas não autorizadas.

Esse tipo de controle de acesso, como foi dito é muito utilizado por militares e agências governamentais, onde as classes de segurança típicas são altamente confidenciais e os níveis de segurança em ordem decrescente de relevância são: altamente confidencial (*top secret* -TS), secreto (*secret* - S), confidencial (*confidential* - C) e não classificada (*unclassified* - U) (ELMASRI; NAVATHE, 2011, p. 570). Existem também outros sistemas de classificação de segurança mais complexos, onde as classes de segurança não são organizadas em um retículo, mas para simplificar usaremos o modelo proposto com quatro níveis.

O método comumente utilizado no controle de acesso obrigatório é conhecido como modelo de Bell LaPadula (desenvolvido por David Elliott Bell e Leonard J. LaPadula). Este modelo é descrito por objetos (tabelas, visões, linhas, colunas), sujeitos (usuários, programas), classes de seguranças e liberações. Cada objeto recebe uma denominação de segurança (TS > S > C > U) e cada sujeito recebe uma permissão de acesso a uma classe de segurança. Desta forma, o modelo de *Bell-La Padula* impõe duas restrições em todas as requisições de leitura ou gravações no banco (RAMAKRISHNAN; GEHRKE, 2008, P. 587):

- Propriedade se segurança simples – um sujeito só pode ler um objeto se sua classificação de permissão for igual ou superior a classificação de segurança do objeto. Por exemplo, um usuário com permissão S pode ler uma tabela com permissão C, mas um usuário com permissão C não pode ler uma tabela

com permissão S.

- Propriedade de segurança estrela – um sujeito só pode gravar em um objeto se sua classificação de permissão for igual ou inferior a classificação de segurança do objeto. Por exemplo, um usuário com permissão S pode gravar em uma tabela com permissão TS, mas um usuário com permissão TS não pode gravar em uma tabela com permissão S.

A primeira regra é intuitiva, pois não permite que um sujeito com permissão de segurança inferior leia em um objeto com classificação de segurança superior. Já a segunda regra é um menos intuitiva, pois não permite que um sujeito grave em um objeto com classificação de segurança inferior. A necessidade desta regra é para evitar que informações com classificação de segurança superior possam migrar para objetos com classificação de segurança inferior, violando uma regra de confidencialidade (ELMASRI; NAVATHE, 2011, p. 571).

4 CONTROLE DE ACESSO NO SGBD ORACLE

4.1 ESTUDO DE CASO COM O SGBD ORACLE

Se por um lado, a internet acelerou o desenvolvimento de novas aplicações nos diversos aspectos do processamento empresarial, por outro, o controle sobre as informações de cunho sigiloso ou confidencial, requerem hoje, administração e regulamentações muito mais rígidas. Surgiram na última década diversos regulamentos que demandam controles internos e proteção de PII ("*personally identifiable information*", informações pessoalmente identificáveis). A maioria das aplicações conta com segurança em nível de aplicação para controlar o acesso a informações confidenciais, por isso são necessários soluções de segurança transparentes, capazes de oferecer controles mais seguros. Conceitos como o de atribuir privilégio mínimo e *need-to-know*, são considerados menos importantes do que a escalabilidade e a alta disponibilidade. A Oracle propõe oferecer um SGBD com complementações de segurança em nível de aplicação, de forma a permitir que as organizações cumpram com regulamentações e a disponibilização de controles internos mais rígidos (ORACLE, 2008, p. 2).

A SGBD Oracle possui diversos itens de segurança. Como vários deles não fazem parte do escopo deste trabalho, neste capítulo faremos uma abordagem somente a tópicos referentes ao controle de acesso aos dados.

O motivo para escolher o banco de dados Oracle como um capítulo particular para esta pesquisa, se deve ao fato deste SGBD ser líder mundial em bancos de dados corporativos segundo pesquisas da Gartner Group divulgadas em sítios da internet, além do sitio da própria Oracle (2008).

> "De acordo com o instituto de pesquisa de mercado Gartner, a Oracle é o fornecedor líder mundial de software de sistemas de gerenciamento de bancos de dados relacionais (RDBMS), com base na receita total do software para 2007.
>
> Participação de mercado: software de sistemas de gerenciamento de

> bancos de dados relacionais por sistema operacional em todo o mundo, 2007" [1], recente relatório do Gartner, constata que a Oracle lidera o segmento de software de RDBMS mundial em 2007, com uma participação de 48,6% – quase 28 pontos percentuais à frente do concorrente mais próximo.
>
> A Oracle lidera o segmento de RDBMS mundial em Linux, com uma participação de 79% em 2007.
>
> [1] Market Share: Relational Database Management System Software by Operating System, Worldwide, 2007– Colleen Graham, Bhavish Sood, Horiuchi Hideaki, Dan Sommer – 11 de julho de 2008."

4.2 PRIVILÉGIOS DE SISTEMAS E OBJETOS

O SGBD Oracle oferece vários mecanismos para gerenciar segurança de acesso, controle de recursos e a política de senhas para usuários. Utilizando perfis, é possível controlar de forma transparente o mecanismo de privilégios e atribuições, permitindo conferir aos usuários, as devidas autorizações para as tarefas que necessitam executar.

Privilégios são permissões concedidas a um usuário, por outro usuário com permissões de administrador para o privilégio a ser concedido. A permissão concede ao usuário, acesso a objetos de maneira prescrita, por exemplo, para conectar ao banco de dados (*create session*), criarem uma tabela no próprio esquema (*create table*), examinar uma tabela sua ou de outro usuário, selecionar registros de outra pessoa ou executar *stored procedures* de outro usuário (ACKERMANN, 2003, p. 55).

A sintaxe para criação de um usuário é a seguinte:

CREATE USER nome_de_usuario **IDENTIFIED BY** senha_do_usuario

[DEFAULT TABLESPACE nome_da_tablespace**]**

[TEMPORARY TABLESPACE tablespace_temporaria**];**

Onde:

- **nome_de_usuario** – É o nome do usuário a ser criado;
- **senha_de_usuario** – É a senha para usuário a ser criado;
- **nome_da_tablespace** - É a tablespace padrão onde os objetos do banco de dados são armazenados. Se essa opção for omitida, o banco assume a tablespace SYSTEM padrão;
- **tablespace_temporaria** – É a tablespace padrão onde são armazenados os objetos temporários, como tabelas temporárias por exemplo. Se essa opção for omitida um tablaspace temporário TEMP é assumida.

Basicamente, existem duas categorias distintas de privilégios dentro de um banco de dados (ACKERMANN, 2003, pág. 55):

- **Privilégios de sistema.**
- **Privilégios de objeto.**

4.2.1 Privilégios de Sistema

São os privilégios que permitem ao usuário executar instruções DDL em um tipo particular de objeto do esquema, como por exemplo: *create user*, *create session*, *create sequence*, *create synonym*, *create table*, *create view* e muitos outros. Muitos destes privilégios são concedidos apenas para administradores por se tratarem de privilégios muito poderosos (LEVINGE, 2002ª apud ACKERMANN, 2003, p. 55).

O comando básico para liberar privilégio de sistema e:

```
GRANT create session,create table,create view TO nome_do_usuario;
```

No exemplo, foram liberados três privilégios para o usuário: o de criar uma sessão de conexão no banco e o de criar tabelas e *views.* Sempre que disponibilizamos permissões para um usuário, temos a opção de utilizar a cláusula **WITH ADMIM OPTION**, essa cláusula concede ao usuário permissão para propagar as permissões recebidas para outros usuários.

```
GRANT create session,create table,create view TO nome_do_usuario WITH ADMIN OPTION;
```

Com o uso da cláusula **WITH ADMIM OPTION**, o usuário poderá estender seus privilégios de sistema para outros usuários.

4.2.2 Privilégios de Objeto

Normalmente o controle de acesso a dados e feito em nível do próprio SGBD ou por tabela especifica. O privilégio de objeto permite executar instruções DML em objetos específicos do esquema, como por exemplo, instruções de *select*, *insert*, *update*, delete entre outros. E também privilégios para executar operações DDL de alteração, indexação e referência a uma tabela.

Estes privilégios podem definir permissão para inserção ou alteração de colunas específicas da tabela, ou restringir em nível de registros, operações de seleção, inserção, alteração e eliminação de registros, para usuários específicos.

O comando básico para liberar privilégios de objeto é:

```
GRANT select,update ON nome_do_esquema.nome_da_tabela TO nome_do_usuario;
```

Neste comando foram liberados privilégios de *select* e *update* para a tabela de um esquema específico, para um usuário específico. Sempre que estiver liberando privilégios para objetos de outro usuário, é necessário colocar o nome do usuário (esquema) antes do nome do objeto, como no exemplo. Da mesma forma que ocorre na concessão de privilégios de sistema, pode-se acrescentar ao final da instrução a cláusula **WITH GRANT OPTION**, permitindo que o usuário possa repassar a outros usuários os privilégios recebidos, como mostra o exemplo a seguir:

GRANT select,update **ON** nome_do_esquema.nome_da_tabela **TO** nome_do_usuario **WITH GRANT OPTION;**

A cláusula **REVOKE** é utilizada para remover os privilégios de um usuário, sejam eles privilégios de objeto ou de sistema. O exemplo a seguir mostra como remover o privilégio de sistema **CREATE VIEW** de um usuário:

REVOKE create view **FROM** nome_do_usuário;

Para remover um privilégio de objeto de um usuário (**INSERT,** por exemplo), usa-se a instrução como no exemplo:

REVOKE insert **ON** nome_do_esquema.nome_da_tabela **FROM** nome_do_usuario;

A princípio, os privilégios de objetos só podem ser concedidos pelo dono do objeto, a não ser que este autorize outro usuário à permissão para autorgar privilégios. Como padrão, o administrador possui todos os privilégios para executar ações em objetos do esquema. O administrador pode repassar esses poderes para um desenvolvedor de sistema ou para o DBA, com a finalidade de facilitar as tarefas de configurações de segurança necessárias (LEVINGE, 2002ª apud ACKERMANN, 2003, p. 55).

4.3 USO DE PAPÉIS PARA ADMINISTRAR PRIVILÉGIOS

Um papel (role) é um grupo de privilégios associados a um nome de identificação. Desta forma, ao invés de atribuir vários privilégios para um único usuário, cria-se um único papel que recebe vários privilégios e atribui-se este papel a quantos usuários forem necessários. A figura 4 mostra a sintaxe de uma role.

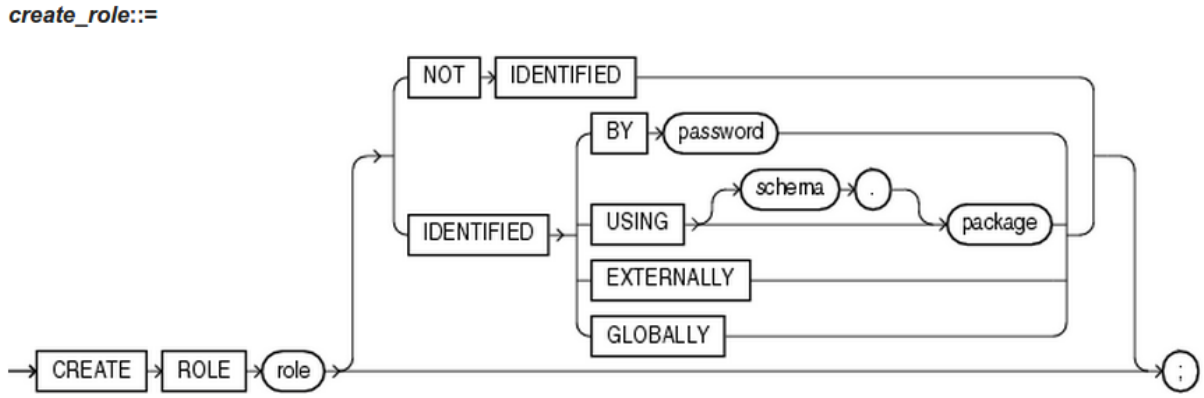

Figura 4 – Sintaxe para criar uma role.
Fonte: Oracle Help Center (p. 387)

Existem vários níveis de papéis:

- Papéis de Banco de Dados;
- Papéis Globais;
- Papéis de Empreendimento;
- Papéis de aplicação seguro.

4.3.1 Papeis de Banco de Dados

Papéis de banco de dados permitem alteração de dados no BD. Normalmente são concedidos privilégios ao papel e não ao usuário, pode-se então habilitar ou desabilitar os privilégios de maneira seletiva para cada usuário, facilitando o controle específico de privilégios. Existe ainda a opção de proteger um papel com o uso de

uma contra-senha. Ao associar uma senha para habilitar o papel em uma aplicação, o usuário só poderá habilitá-la se conhecer a contra-senha (LEVINGE, 2002a apud ACKERMANN, 2003, p. 58).

A figura 5 mostra como é possível usar vários níveis de papel e privilégios, pare se alcançar um maior detalhamento no controle de acesso. Lembrando que quanto menos privilégios o usuário tiver, melhor.

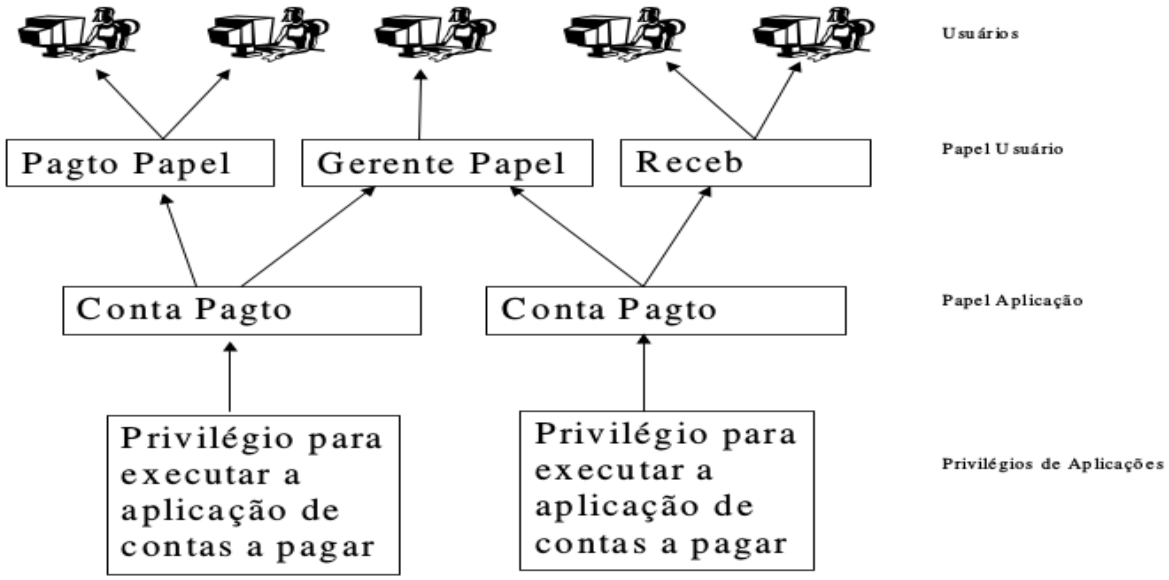

Figura 5 – Exemplo de utilização de papéis.
Fonte: Ackermann (2003).

4.3.2 Papéis de Empreendimentos

Papéis de empreendimento são estruturas de diretórios que contém vários papéis globais em múltiplos BDs, e que são concedidos a usuários de empreendimentos.

Com a utilização de papéis de empreendimentos, é possível concentrar a administração de informações e autorizações de um usuário, através do armazenamento em um serviço de diretório (LDAP - based) (LEVINGE, 2002ª apud ACKERMANN, 2003, p. 60).

4.3.3 Papéis Globais

Os papéis globais são atributos de segurança de usuários de empreendimentos. Ele se aplica a apenas um BD para o qual estão definidos os direitos, mas pode ser associado a papéis de empreendimentos. Os papéis globais são definidos localmente no BD. A eles são atribuídos privilégios e papéis, porém não podem ser associados a nenhum usuário ou outro papel no BD. Quando o usuário do empreendimento se conectar ao BD, serão verificados quais são os papéis globais associados a este usuário (ACKERMANN, 2003, pág. 59).

4.3.4 Papéis de Aplicações Seguras

Prevenir que usuários burlem a lógica das aplicações para obter acesso diretamente aos dados, é um problema de segurança de difícil resolução. Em aplicações Web, por exemplo, validar a aplicação que é usada para obter acesso aos dados pode ser um problema. É possível que não se queira que nem mesmos os usuários conhecidos do BD, tenham acesso direto aos dados, pois um usuário mal intencionado poderia escrever um programa que se fizesse passar por uma aplicação aparentemente válida.

Um papel de aplicação segura é um papel implantado por um pacote. Este pacote executa validações para assegurar que as permissões apropriadas sejam conhecidas antes do usuário executar os privilégios concedidos ao papel no BD. Ele é usado por uma aplicação e só por ela é habilitado, não sendo necessário o uso de contra-senha.

Essa característica do papel de aplicação segura permite, por exemplo, escrever um papel que só permita que um usuário se conecte a partir de um determinado IP, ou que só tenha acesso a uma camada intermediaria particular do banco de dados (LEVINGE, 2002a apud ACKERMANN, 2003, p. 61).

4.4 USO DE STORED PROCEDURE PARA ADMINISTRAR PRIVILÉGIOS

O uso de *stored procedure* é uma forma de limitar as transações dos usuários no BD, podendo ser executadas apenas procedimentos e funções com direitos pré-definidos. Quando um usuário dispara um procedimento, ele é executado com os privilégios do dono do procedimento. Desta forma pode-se conseguir que um usuário possa fazer atualizações em uma tabela ao mesmo tempo em que nega o acessa a tabela propriamente dita (LEVINGE, 2002a apud ACKERMANN, 2003, p. 62)

4.5 USO DE INSTALAÇÕES DE REDE PARA ADMINISTRAR PRIVILÉGIOS

Os papéis em banco de dados também podem ser escritos para atender serviços externos responsáveis por autenticação (grupos de DCE e autorizações RADIUS), desta forma podem administrar de forma centralizada todos os privilégios de uma rede, onde o banco de dados é apenas um pedaço desta rede (LEVINGE, 2002a apud ACKERMANN, 2003, p. 62).

4.6 USO DE VISÕES PARA ADMINISTRAR PRIVILÉGIOS

As visões são tabelas lógicas baseadas em uma ou mais visões ou tabelas. Visões não contêm os dados em si mesmos e podem suportar visões de objetos, ou uma visão relacional que suporta tipos de objetos e tabelas aninhadas. Uma visão de objetos é uma visão de um tipo definido pelo usuário, onde cada linha contém objetos, cada objeto com um identificador único (ORACLE HELP CENTER, p. 471).

Visões adicionam mais dois níveis de segurança: limitando o acesso a colunas somente selecionadas na tabela base ou usando uma cláusula WHERE na sua definição.

Como as visões apenas necessitam de privilégios para a própria visão, não se faz necessário dar privilégios aos objetos de base das visões para que os usuários

possam acessá-los, bastando dar direito apenas a visão (ACKERMANN, 2003, p. 62).

4.7 SEGURANÇA EM NÍVEL DE REGISTRO

Em casos onde o acesso a registros específicos de uma tabela necessitem basear-se em alguns argumentos como o departamento a que pertence o usuário, titulação, ou outros fatores significantes, pode-se usar uma forma mais granular de acesso, que é o acesso em nível de registro. Existem duas maneiras de atender este problema: usando um Banco de Dados Privado Virtual (VPD), onde são criadas implementações de segurança em nível de registro, e o controle de acesso rótulo-base (*label-based*), onde se personaliza uma política de VPD (LEVINGE, 2002a, apud ACKERMANN, 2003, p 63).

4.7.1 Segurança Baseada em Rótulo

O trabalho para administrar restrições de acesso a tabelas e isolar dados confidenciais em bancos de dados independentes é bastante custoso. Para facilitar esta tarefa, o Oracle disponibiliza no Oracle Database 11g Release (11.1), o Oracle Label Security, que habilita o controle de acesso em nível de linha.

Seu funcionamento se baseia em associar a cada tabela ou visão, uma política de segurança, assim, toda vez que uma consulta é executada ou uma tabela é alterada, a política de segurança e consultada. Desta forma, os desenvolvedores podem executar diretamente em suas aplicações para bando de dados Oracle, controle de acesso baseado em rótulo (ELMASRI; NAVATHE, 2011 pág. 584).

4.7.1.1 Conceito de *Virtual Private Database* (VPD)

Há pouco tempo atrás a garantia de segurança em um banco de dados era garantida com aplicação de restrições em seus objetos e controle das operações DML básicas como *select*, *insert*, *update* e *delete*. Porém, o crescimento cada vez maior das aplicações voltadas para ambiente web, gerou a necessidade de um banco de dados com características diferentes, como por exemplo, a centralização de dados de diversos bancos, em uma única database, que acabam por gerar agrupamentos de informações de várias organizações em um único objeto.

Em bancos de dados voltados para web, a simples aplicação de privilégio no objeto não é suficiente para garantir a confidencialidade dos dados. É preciso especificar não apenas o objeto ao qual o usuário possui permissão, mas também qual parte deste objeto. Ou seja, é necessária uma aplicação de segurança em nível de linha (*Row Level Security*). Existe a possibilidade de implantar *row level security* no próprio desenvolvimento da aplicação, mas a criação e manutenção das políticas de segurança se tornam muito complicadas. Além disso, os objetos só estarão sujeitos a aplicação das políticas enquanto acessados através da aplicação que as implantou, se um usuário puder acessar o objeto através de outra aplicação ou ferramenta que não esteja sujeito a política de segurança (SQL Plus, SQL Developer, Tod, etc), terá acesso total as informações.

O Oracle disponibiliza, a partir da versão *Enterpraise* 8i em diante, recursos para implantar VPD. Esta funcionalidade insere atributos ao domínio do usuário, limitando suas permissões de maneira confiável tanto para o usuário como para a aplicação.

O Oracle oferece nativamente à linguagem de programação PL/SQL (*Procedural Language/Structured Query Language*). Em forma de uma interface de programação de aplicação (API), a PL/SQL permite que a manipulação de dados seja incluída em unidades de programas. Desta forma os responsáveis pela administração de segurança, desenvolvedores e DBAs, podem implantar controle de acesso baseados em políticas VPD em nível de objeto ou segurança em nível de linha, retirando as regras de segurança da aplicação e concentrado-as no banco de

dados (ELMASRI; NAVATHE, 2011 pág. 584).

O conceito básico do VPD é associar uma política de segurança a uma tabela, visão ou sinônimo. Quando uma aplicação solicita uma operação no banco de dados, a função associada à política de segurança daquele objeto é consultada. Esta função retorna uma condição na forma de uma cláusula WHERE que é acrescentada ao script da operação solicitada. Desta maneira, independente da aplicação ou ferramenta que tente acessar os dados, estará sujeita a política de segurança que foi previamente implantada (ELMASRI; NAVATHE, 2011 pág. 584).

4.7.1.2 Oracle Label Security

O Oracle Label Security está embutido na tecnologia VPD e permite que as organizações governamentais ou de defesa, consolidem dados de diferentes tipos de classificações, no mesmo BD. O acesso aos dados é restrito com base na classificação dos dados e do certificado de segurança do usuário do aplicativo. Este recurso permite que requisitos de segurança multinível possam ser executados dentro do Oracle (ORACLE, 2013).

A figura 6 demonstra como ocorre a sequência de verificações DAC e a segurança de rótulo. No lado esquerdo da figura temos um usuário enviando uma requisição SQL através de uma aplicação. Primeiro o Oracle faz a verificação de privilégios do DAC deste usuário para se garantir que ele tem a permissões necessárias para executar a requisição. Depois, será verificado se existe alguma política de VPD associada à tabela, se houver, uma cláusula WHERE é acrescentada ao script SQL e só então a consulta será processada (ELSMARI; NAVATHE, 2011 pág. 585).

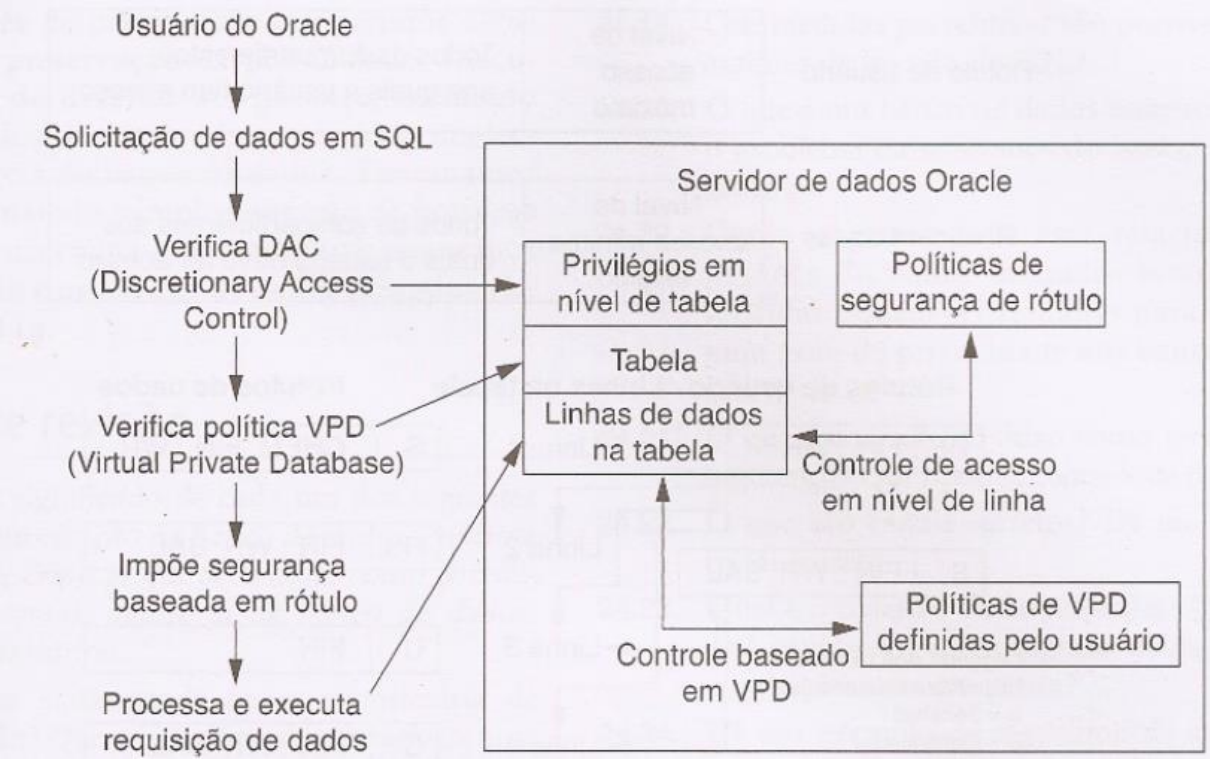

Figura 6 – Sequência de verificação DAC.
Fonte: ELSMARI e NAVATHE (2011)

O controle de acesso a informações sensíveis é motivo de preocupação para gestores, agentes de informação, DBAs, desenvolvedores de sistemas, e muitos outros. Controle de acesso seletivo com base no nível de segurança do usuário pode garantir confidencialidade sem limitações muito amplas. Este nível de controle de acesso garante que informações confidenciais não estarão disponíveis para pessoas não autorizadas, mesmo quando os usuários autorizados tenham acesso às informações necessárias, às vezes nas mesmas tabelas.

Dados sensíveis que permitam ser vistos por pessoas não autorizadas, podem ser embaraçoso, prejudicial ou perigoso para as pessoas, carreiras, organizações, agências, governos ou países. No entanto, muitas vezes, esses dados estão misturados com outras informações menos sensíveis, e que são legitimamente necessários para diversos usuários. Restringir o acesso a tabelas inteiras ou segregar dados confidenciais em bancos de dados separados, pode criar um ambiente de trabalho desajeitado, custoso em termos de *hardware, software* e administração.

O Oracle Label Security elimina a necessidade de tais medidas, permitindo o

controle de acesso em nível de linha, com base na tecnologia de banco de dados virtual do Oracle Database 11g 1 (11.1) Enterprise Edition. Ele controla o acesso ao conteúdo de uma linha comparando o seu rótulo com o rótulo de privilégio do usuário. Assim, os administradores podem facilmente adicionar políticas linha-restritiva seletivas para banco de dados existentes por meio de uma interface gráfica fornecida pelo Enterprise Manager (ORACLE HELP CENTER, p. 7-30).

4.7.1.3 Rótulos de Dados e Rótulos de Usuários Trabalhando Juntos

Um rótulo de usuário define quais são as informações e que tipo de acesso (leitura ou gravação) este usuário tem direito. Um rótulo de dado define, além da propriedade e sensibilidade da informação armazenada, quais são as políticas que um usuário deve atender para poder acessá-lo. Com base no resultado da comparação entre o rótulo de dados e do rótulo da sessão do usuário, o acesso será concedido ou negado.

Os rótulos relacionam os dados compartimentos, todos os dados de um mesmo projeto podem estar relacionados a um compartimento. Estes compartimentos são opcionais, de forma que um rótulo pode conter zero ou mais compartimentos.

Grupos hierárquicos são usados para identificar organizações como proprietárias dos dados de rótulos de grupos correspondentes. Um grupo pode, por exemplo, ser associado a um grupo pai.

Um usuário que possua o nível máximo de SENSITIVE terá possivelmente acesso aos dados com níveis de sensibilidade iguais ou menores que a dele, mas não terá acesso aos dados com nível HIGHLY_SENSITIVE. A figura 7 mostra como rótulos de dados e de usuários trabalham juntos.

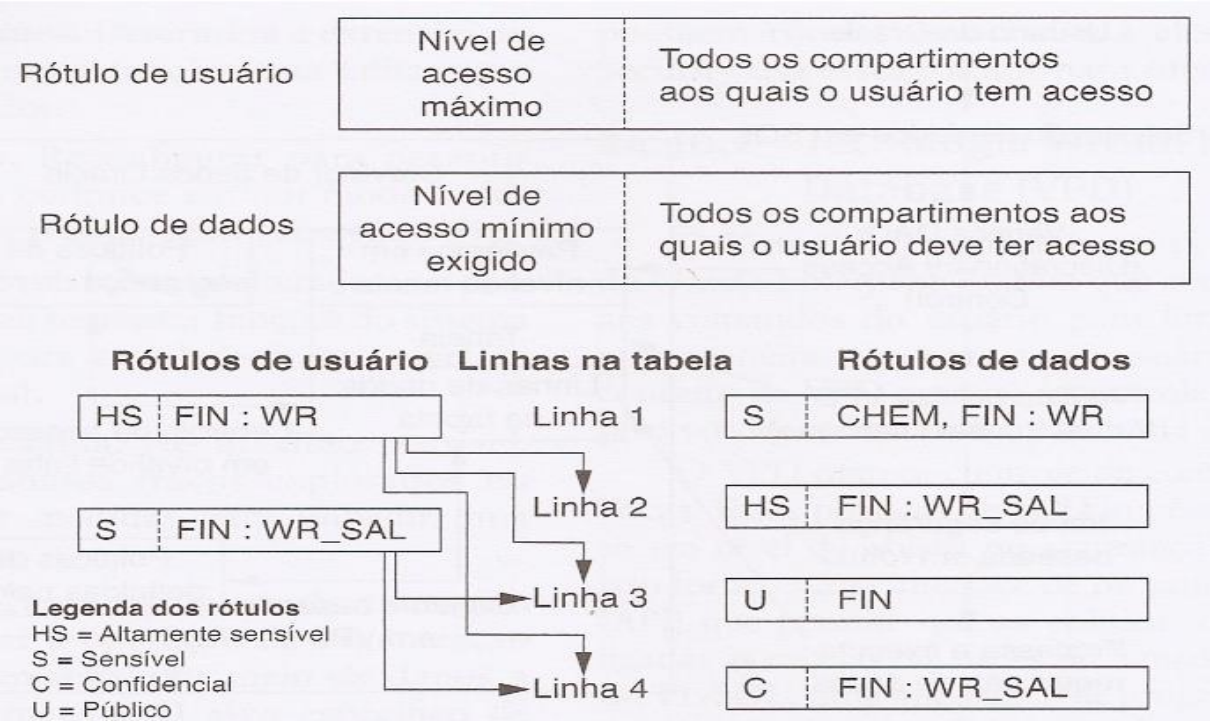

Figura 7 – Como rótulos de dados e usuários trabalham juntos.

Fonte: ELSMARI e NAVATHE (2011)

Podemos ver que o primeiro usuário tem nível de acesso HS (Highly Sensitive) nos compartimentos FIN (Financeiro) e WR (Western Region), que hierarquicamente inclui o grupo WR_SAL (WR Sales). Comparando este rótulo com os rótulos dos dados nas linhas da tabela, este usuário terá acesso às linhas 2, 3 e 4. O segundo usuário possui nível de acesso S (Sensitive) nos compartimentos FIN e WR_SAL, o eu lhe dará acesso apenas aos dados das linhas 3 e 4 (ELMASRI; NAVATHE, 2011 p. 585, 586).

5 CONSIDERAÇÕES FINAIS

Os sistemas gerenciadores de banco de dados estão em constante evolução, impulsionados pelas novas tecnologias, aplicações e normas. Sua principal função é garantir o controle das bases de dados, armazenando, protegendo e disponibilizando informações de todo o tipo a uma grande variedade de usuários. Neste contexto, um dos principais mecanismos dos SGBD, senão o principal é atender as políticas de segurança criadas pelas empresas, através do controle de acesso aos dados.

Este trabalho teve como objetivo principal, descrever como são aplicados os controles de acesso em SGBDs, avaliar as soluções disponíveis no mercado, suas vantagens e vulnerabilidades. Para cobrir esses objetivos, foram apresentados os conceitos básicos de segurança da informação, uma pesquisa sobre os principais controles de acesso disponíveis nos SGBDs, seguidos de um estudo de caso em um SGBD comercial específico, no caso o Oracle Database 11g Release (11.1)

Esta pesquisa trás como contribuição as seguintes conclusões: dentre os mecanismos de controle de acesso disponíveis no mercado e pesquisados neste trabalho, nenhum se mostrou suficiente para atender, sozinho, as necessidades de segurança. Porém, foi possível verificar que a utilização conjunta destas ferramentas aplicadas a uma política de segurança adequada, pode oferecer controle de acesso com granulação satisfatória para atender as principais necessidades das empresas.

O estudo de caso com o banco de dados Oracle mostrou que este faz controle de privilégios, tanto de sistema como de objetos, principalmente pela utilização de papéis de banco de dados, papéis globais, papéis de empreendimentos e papéis de aplicações seguras. Para garantir a segurança em nível de registro, o Oracle oferece um mecanismo diferenciado através da ferramenta de reescrita de consulta chamada VPD.

O assunto de segurança no controle de acesso a SGBDs é bastante vasto e para atender a proposta desta pesquisa, optou-se por apresentar, um resumo dos principais procedimentos de segurança em BDs com o melhor detalhamento possível para cada um dos tópicos abordados. Com isso, vários assuntos ficam abertos como opções para projetos futuros, como exemplo: a centralização dos controles de acesso, aperfeiçoamento dos mecanismos disponíveis e utilização de interfaces de controle para facilitar a administração de serviços.

REFERÊNCIAS

ACKERMANN, Marcelo A. **Aderência de Controles de Acesso em SGBDs Relacionais às Políticas de Segurança de Aplicações**. 2003. 117 f. Dissertação (Mestrado em Ciência da Computação) – Programa de Pós-graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2003. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/85913/203180.pdf?sequence=1>.

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.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados**. 6ª ed. São Paulo: Editora Pearson, 2011.

HAZEL, Lorraina. **An overview of oracle database security features.** CNE. May 13, 2001.

ORACLE. **Soluções transparentes para segurança e conformidade com o Oracle Database 11g.** Um artigo técnico da Oracle. Setembro 2008. Disponível em: <http://www.oracle.com/technetwork/pt/database/enterprise-edition/documentation/seguran%C3%A7a-conformidade-database-11g-432099-ptb.pdf> Acesso em: 28/09/2014.

ORACLE. **Oracle Press Release.** Redwood Shores, Califórnia 12-SEP-2008. Disponível em: <http://www.oracle.com/br/corporate/press/oracle-lider-banco-dados-345158-ptb.html> Acesso em: 28/09/2014.

ORACLE. **Oracle label security.** DATA SHEET. Disponível em: <http://www.oracle.com/technetwork/database/security/label-security-ds-12c-1898878.pdf?ssSourceSiteId=ocombr> Acesso em 28/09/2014.

ORACLE HELP CENTER. **Database SQL Reference.** p. 471. Disponível em: <https://docs.oracle.com/cd/B19306_01/server.102/b14200/statements_8004.htm> Acesso em 28/09/2014.

ORACLE HELP CENTER. **Database SQL Reference.** p. 387. Disponível em: <https://docs.oracle.com/cd/B19306_01/server.102/b14200/statements_6012.htm> Acesso em 28/09/2014.

ORACLE HELP CENTER. **Label Security Administrator's Guide.** Introduction to Oracle Label Security p. 7 – 30. Disponível em: <https://docs.oracle.com/cd/B28359_01/network.111/b28529/intro.htm> Acesso em 28/09/2014.

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

PISSINOU, Niki; MAKKI, Kia; PARK, E.K. **Towards a framework for integrating multilevel secure models and temporal data models**. ACM Computing Surveys, 1994.

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

RAMAKRISHNAN, Raghu; GEHRKE, Johannes. **Sistema de gerenciamento de banco de dados**. 3ª ed. São Paulo: Editora McGraw-Hill, 2008.

SANDHU, Ravi S. **Relational database access controls.** Handbook of information security management (1994-95 Yearbook), Auerbach Publishers, 1994. Disponível em: <http://www.profsandhu.com/articles/auerbach/a94dac.pdf> Acessado em: 27/07/2014.

SILBERSCHATZ, Abraham; KORTH, Henry F.; SUDARSHAN, S. **Sistemas de banco de dados.** 3ª ed. São Paulo: Editora Pearson Education do Brasil, 1999.

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

TANENBAUM, Andrew S. **Redes de computadores**. 4ª ed. Rio de Janeiro: Editora Campus (Elsevier), 2003.

VERIZON, **Relatório de investigações de violações de dados (relatório DBIR) de 2014**. Disponível em: <http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_pt-br_xg.pdf> Acesso em: 27/07/2014.