Visão geral de Segurança em Bancos de Dados

Joaquim Vitor, Márcio Lucena Moraes, Rafaello Costa

Universidade Católica de Brasília, MBA Gestão de Sistemas de Informação

Resumo

Com a grande utilização de sistemas baseados em tecnologia, os Bancos de Dados são hoje uma ferramenta vital paras as organizações. Estas ferramentas são responsáveis por armazenar, recuperar e transformar um bem muito importante para qualquer empresa que queira ser ou continuar sendo competitiva no mercado, a informação. A informação e um fator competitivo e que muitas vezes diferencia uma empresa vencedora de uma fracassada. Tendo em vista tal importância, os Banco Bancos de Dados são tratados com bastante cuidado pela organização. Existem profissionais especialistas em administração de Bancos de Dados. Esses profissionais, junto com o Banco de Dados escolhido pela empresa, são responsáveis por manter a integridade, a confidencialidade e a acessibilidade dos dados e informações da organização. Em decorrência, os fabricantes de Bancos de Dados têm se preocupado em oferecer várias soluções de segurança, integradas as suas ferramentas. Vamos então mostrar de maneira geral como dois dos Bancos de Dados mais utilizados no mercado tratam a segurança. São eles: IBM DB2, e Oracle.

1. INTRODUÇÃO

Ao observar o comportamento de grandes organizações percebe-se que elas enfrentam diversos desafios para se destacarem e terem o reconhecimento do mercado. Muitos desses desafios advêm da própria natureza de atuação dessas organizações que, na maioria das vezes, têm que lidar com tecnologias para desenvolvimento de novos produtos e novas idéias num mercado cada vez mais exigente e competitivo.

Com a disseminação do uso da tecnologia, as organizações, se depararam com o problema da segurança. Atualmente é difícil encontrar uma empresa que não apresente preocupações relacionadas a segurança dos dados corporativos, sejam estes críticos ao negócio ou não. Todos os dias, os meio de informação divulgam novos ataques eletrônicos a várias empresas no mundo todo.

O preço que as organizações tem que pagar pela segurança possui dois componentes: o primeiro é o custo de se pesquisar e implementar uma solução de segurança conforme as necessidades da empresa, o segundo é o custo de se utilizar os sistemas de forma segura.

A segunda despesa não deve ser subestimada. Normalmente ela é maior que a primeira. Os usuários costumam esquecer suas senhas, sobrecarregando o suporte e outros ainda criam senhas fáceis e acessam a internet de maneira insegura.

Também cabe ressaltar que um sistema “seguro” pode apresentar um desempenho inferior ao de um sistema desprotegido pois a autenticação, troca de chaves, criptografia, tudo isso toma tempo de processamento e banda de rede. Quanto menos recursos do sistema forem usados na segurança, menor o custo operacional.

Além do investimento em tecnologia faz-se necessária uma mudança inclusive na forma de trabalho onde é fator critico de sucesso conseguir o comprometimento dos altos executivos e preparar as pessoas para uma mudança de cultura, investindo em seminários de conscientização que detalhem a importância da segurança e o papel das pessoas no cenário corporativo.

A busca pela segurança deve ser uma atividade constante pois quando uma nova tecnologia se incorpora ao ambiente corporativo, novas vulnerabilidades a acompanham. Vamos estudar o funcionamento das ferramentas de Banco de Dados quanto aos aspectos relacionados a segurança da informação. Iremos explorar os aspectos das três principais e mais utilizadas ferramentas do mercado.

Os sistemas gerenciadores de banco de dados (SGBD), são peças fundamentais em um ambiente de provimento de informações, estes sistemas conjuntamente com os sistemas operacionais e sistemas especialistas de segurança devem prover segurança às informações.

Atualmente os SGBDs mais utilizados são o SQL desenvolvido pela Microsoft, o Oracle DB desenvolvido pela Oracle e o DB2 desenvolvido pela IBM. Cada SGBD tem suas vantagens como também suas desvantagens no que diz respeito a vulnerabilidades, praticidade de utilização e falhas de segurança.

2. DB2

O DB2 UDB foi originalmente criado como um banco de dados relacional para atender missões críticas realizadas em mainframes. Suporta a exploração e o armazenamento de dados, possui alta tecnologia no processamento de suas transações. Permite desenvolver soluções de aplicativos rápidas, confiáveis e seguras.

De acordo com o fabricante, suporta mais de 20 plataformas distintas. São elas:

- WinNT;
- Win2000;
- Win98/95;
- AIX (Versão Unix da IBM);
- Linux
- HP-UX;
- SUN;
- OS/2;
- VM;
- MVS.

2.1 Característica de Segurança

Quando a base de dados encontra-se em sistemas inseguros, o próprio SGBD possui características de proteção aos dados. No caso do DB2, é possível prover autenticação dos usuários, definir níveis de autorização de acesso que podem ser definidas por usuários individualmente ou por grupos de usuários e oferece condições de controle de acesso aos dados, possui ainda auditoria de acesso para cada evento executado.

2.2 Opções de Autenticação

O processo de autenticação verifica a identidade do acesso, o qual pode ser por parte de um usuário ou de um aplicativo.

No DB2, assim como na maioria dos sistemas, esta autenticação é feita através de uma identificação de usuário e uma senha. Após a autenticação o DB2 grava a identidade do acesso (usuário) e qualquer outra informação relevante para segurança, como por exemplo, o grupo a qual o usuário faz parte.

O DB2 verifica a autenticidade do acesso e a partir do usuário autenticado, o DB2 verifica com a autorização SQL, se o usuário possui permissão para acessar algum valor do banco de dados. Estas informações serão utilizadas durante toda conexão.

O DB2 oferece diferentes opções de autenticação que podem ser ajustados no arquivo de configuração de gerenciamento (dbm.cfg), usando o parâmetro de AUTHENTICATION do arquivo. Este parâmetro é utilizado para determinar como e onde a autenticação deverá ocorrer.

O estabelecimento de ajustes no parâmetro de AUTHENTICATION do arquivo de configuração de gerenciamento pode ser organizado logicamente em quatro categorias distintas:

- Autenticação a partir do Servidor;
- Autenticação a partir do Cliente;
- Autenticação a partir do DCE ;
- Autenticação a partir do Kerberos.

2.2.1 Autenticação a partir do Servidor

SERVER: É o mecanismo de segurança padrão. Especifica que a autenticação deve ocorrer no servidor usando o sistema operacional que aloca o banco de dados. Se o login for especificado durante a conexão, o DB2 chama uma função de sistema para validar o usuário e a senha. No ambiente Windows, o ID do usuário é consultado freqüentemente com o username. O username e a senha são comparados freqüentemente com a conta de usuário validada no sistema.

SERVER_ENCRYPT: Basicamente, apresenta as mesmas características da opção SERVER, exceto porque a senha transmitida do cliente para o servidor está criptografada, ou seja, a senha chega ao servidor codificada. O DB2 utiliza um algoritmo *DES* de 56 bits para criptografar a senha e o algoritmo *Diffie-Hellman* é usado para gerar a chave de criptografia da conexão. O conjunto de ferramentas RSA Bsafe fornece este suporte.

2.2.2 Autenticação a partir do Cliente

Especifica que a autenticação deverá ocorrer no cliente. Se o cliente estiver alocado em um sistema operacional que tenha ferramentas próprias de segurança, por exemplo o *AIX*, este cliente é considerado confiável. De maneira geral todos os clientes são considerados confiáveis, exceto para os clientes Microsoft Windows 95/98.

Se um servidor recebe uma solicitação de um cliente confiável e uma solicitação de um cliente não confiável, as opções TRUST_ALLCLNTS e TRUST_CLNTAUTH permitem ao cliente confiável ganhar acesso de cliente autenticado, enquanto o cliente não confiável deverá prover uma senha para obter a autenticação de cliente com sucesso.

2.2.3 Autenticação a partir do DCE

Alguns administradores escolhem a implementação de segurança pelos serviços *DCE* por ele fornecer administração centralizada de usuários e senhas.

O *DCE* é um produto auxiliar de serviços de segurança, projetado para ambientes em três camadas. Este serviço oferece duas opções de implementação:

- **DCE**: Especifica que o usuário é autenticado pelo serviço de segurança. Um cliente DB2 registrado no DCE recebe uma espécie de ticket criptografado que pode ser utilizado direto no DB2. O DB2 já irá reconhecer este cliente como um usuário autenticado.

- **DCE SERVER_ENCRYPT**: Especifica que o servidor aceitará o ticket de serviço DCE ou o login do usuário DB2 juntamente com uma senha criptografada como prova de que o usuário é realmente autenticado como cliente DB2.

2.2.4 Autenticação a partir do Kerberos

Ao usar o *Kerberos*, o usuário poderá ser autenticado logo no início da sessão com o DB2. Uma vez autenticado, o usuário não será mais contestado por nenhum usuário que existir no sistema *Kerberos*. Este método somente poderá ser utilizado quando o cliente DB2 e o usuário DB2 estiverem no sistema operacional windows 2000.

O DCE e o *Kerberos* usam basicamente as mesmas tecnologias. Quando o cliente está registrado no ambiente de segurança *Kerberos*, o cliente DB2 pode obter uma licença criptografada *Kerberos* para utilizá-lo para autenticar-se ao servidor DB2 especificado. Pode-se escolher entre duas colocações:

- **KERBEROS**: Especifica que o cliente será autenticado apenas pelo ambiente de segurança Kerberos.

- **KRB_Server_Encrypt**: Especifica que o servidor estará aceitando também licença do Kerberos ou ID de usuário e senha criptografada como evidência da autenticação, selecionados pelo cliente.

2.3 Autorização

Após ser autenticado, o usuário acessa a segunda camada DB2 de segurança. A autorização é o processo com que o DB2 obtém as informações do usuário autenticado, incluindo as permissões de operações que o usuário poderá executar no banco de dados e os tipos de dados que o usuário poderá acessar.

O processo de Autorização do DB2 pode ser dividido em duas categorias: Autoridade e Privilégio.

2.3.1 Autoridade

As autoridades fornecem um método de agrupar privilégios e controlar o nível de acesso dos administradores e operadores da base de dados com relação à manutenção e operações permitidas.

As especificações da base de dados estão armazenadas em catálogos da própria base de dados. As autoridades do sistema estão associadas a membros de grupos e armazenados no arquivo de configuração administrativa do banco de dados. Este arquivo define as concessões de acesso e o que poderá ser executado de acordo com cada grupo.

O DB2 possui quatro níveis de autorização predefinidos hierarquicamente: SYSADM, SYSCTRL, SYSMAINT e DBADM.

O SYSADM, SYSCTRL e SYSMAINT operam em nível de arquivos e possuem ampla estrutura. Cada um pertence a grupos de regras de autorização e privilégios. Estas autoridades são definidas no arquivo de configuração administrativa do banco de dados para cada objeto.

O DBADM permite a administração do banco de dados. Um usuário com autorização DBADM tem controle sobre um banco de dados DB2 particular e pode efetuar qualquer função sobre os objetos do mesmo. No entanto, este nível de autorização não tem o privilégio de criar banco de dados, a não ser que a autorização tenha sido especificamente concedida.

Por padrão, a opção SYSADM tem agrupado todos os privilégios possíveis no sistema, incluindo a base de dados. Os usuários com privilégio de SYSADM podem conceder e cancelar qualquer um dos níveis de autorização administrativa ou podem conceder privilégios individuais. Implicitamente a opção DBADM está inclusa no SYSADM.

O DB2 possui várias opções de autorização. Para cada solicitação realizada pelo usuário, pode haver mais de uma verificação de autorização para a conexão, dependendo dos objetos e operação envolvidos. A autorização é executada de acordo com os grupos de privilégios definidos pelo DB2.

O DB2 possui um catálogo de registros de privilégios associados com cada tipo de autorização. O tipo de autorização de um usuário autenticado e os grupos que o usuário pertence são comparados com seus privilégios gravados. Baseado nesta comparação, o DB2 decide em permitir ou não o acesso solicitado pelo usuário.

2.3.2 Privilégio

Os privilégios são permissões únicas dadas a cada usuário ou grupo. Eles definem permissões para tipos de autorização. Pelos privilégios é possível autorizar o usuário a modificar ou alcançar determinado recurso do Banco de Dados.

Os privilégios também são armazenados em catálogos do próprio Banco de Dados, visto que os grupos de autoridade por já possuírem grupos predefinidos de privilégio concedem implicitamente privilégios a seus membros.

2.4 Métodos de Controle de Acesso

Os métodos de controle de acesso são usados para criar subconjuntos de informações dispostas, de modo que o usuário possa ver e alcançar somente os dados que são relevantes a suas necessidades.

O DB2 apresenta os seguintes métodos de controle de acesso:

- Controle de acesso usando pacotes;
- Controle de acesso usando views;
- Controle de acesso utilizando Triggers;
- Controle de acesso usando registro User.

2.4.1 Controle de acesso usando pacotes

O pacote é uma coleção de informações inclusas em um ou mais comandos SQL que são executadas dentro do próprio Banco de Dados. É reconhecido como o ponto de controle preliminar de acesso ao SQL dentro do DB2.

No pacote estão incluídas informações planejadas de acesso com objetivo de otimizar o modelo de autorização configurada no banco de dados. A maioria dos comandos emitidos pelo banco de dados estão relacionados a um pacote específico.

Quando um pacote é criado, o mesmo é limitado a privilégios de acesso específicos, os privilégios requeridos são executados estaticamente por comandos SQL dentro do pacote.

Para executar um pacote o usuário deve ter o privilégio EXECUTE, entretanto não deve possuir privilégio especial para executar nenhum comando estático incluído no pacote. Por exemplo, sem o privilégio de executar o comando CREATETAB o usuário não pode criar uma tabela no banco de dados, entretanto um usuário com privilégios de executar um pacote contendo o comando estático CREATE TABLE conseguirá criar a tabela no banco de dados.

2.4.2 Controle de acesso usando views

As *views* constituem um outro método de controle de acesso, normalmente utilizadas para restringir o acesso direto aos dados. Com a *view* é possível permitir acesso de usuário concedendo privilégios, ocultar linhas e colunas de informações confidenciais ou restritas residentes na tabela original das indicações do SQL.

Os privilégios e concessões são definidos somente na *view* e não afetam a tabela base sendo o acesso dos usuários delimitado pela view, a qual é gerada criando um subconjunto de dados na tabela referenciada.

A opção *With Verification* provê maior segurança porque não permite ao usuário modificar as linhas de tabela sem ter privilégios de leitura dentro da *view*.

2.4.3 Controle de acesso utilizando Triggers

Com a utilização das Triggers é possível criar mecanismos de segurança mais complexos que podem ser disparados cada vez que um evento é chamado. O comando *Insert* na tabela é exemplo de um evento que pode ser usado para disparar uma *Triggers*, além disso, as mesmas podem ser disparadas antes ou depois de comando especificado com o objetivo de prover maior rigor no controle de segurança.

Se o comando executado pelo usuário não for validado pela *Triggers*, um erro é sinalizado do corpo da própria *Triggers* para impedir que a tabela seja modificada indevidamente.

2.4.4 Controle de acesso usando registro User

O DB2 fornece um registro especial chamado *User*. Este registro contém o *User Id* usado para conectar-se ao banco de dados da sessão atual.

Neste registro podem ser armazenados valores de *view* tornando-o um cliente especial. A *view* pode ser criada com base em uma tabela com diferentes aspectos de usuário para usuário. Esta mesma técnica pode também ser usada com a utilização de *Triggers* e comandos SQL.

2.5 Auditoria

As opções de auditoria do DB2 permitem com facilidade o rastreamento dos eventos que ocorreram em suas instâncias. O monitoramento bem sucedido dos dados permite a visualização de tentativas e análises subseqüentes aos acessos realizados no banco e o que foi realizado.

As características de auditoria podem conduzir ao aprimoramento do controle de acesso e a prevenção contra acessos desautorizados, maliciosos ou descuidados aos dados.

Os eventos gravados podem ser extraídos em relatório para análise, estas informações serão extraídas diretamente das tabelas. No entanto, este recurso é pouco utilizado, pois gera uma sobrecarga desnecessária na base de dados.

Como alternativa, alguns administradores projetam *triggers* para execução de auditorias, quando a mesma faz-se necessária.

3. Oracle

A segurança do banco de dados pode ser classificada em duas categorias distintas: segurança de sistema e segurança de dados.

A segurança de sistema contém os mecanismos que controlam o acesso e o uso do banco de dados em um determinado nível do sistema. Os mecanismos de segurança do sistema verificam se um usuário está autorizado a se conectar ao banco de dados, se

a auditoria do banco de dados está ativa e quais operações de sistemas um usuário pode executar.

A segurança de sistema inclui combinações válidas de nome de usuários e senha, a quantidade de espaço em disco disponível para os objetos de esquema de um usuário e os limites de recurso de um usuário

A segurança de dados inclui os mecanismos que controlam o acesso e o uso do banco de dados no nível de objeto de esquema incluindo quais usuários têm acesso a um objeto e a tipos específicos de ações que cada um pode executar.

Além dos sistemas auxiliares para o banco de dados e seus aspectos de proteção, existem ferramentas adicionais que incrementam a segurança do Oracle Server, possibilitando um ambiente multiplataforma de maior escala.

Tais ferramentas dividem-se em dois grupos: as gratuitas e as pagas.

Entre as ferramentas gratuitas, existem dois produtos particulares que são vendidos juntamente com a versão básica do Oracle Server. Estes produtos são: Oracle Enterprise Manager (conhecido como OEM) e o Oracle Security Server Manager (conhecido como OSS).

O OEM é um conjunto de utilitários que são disponibilizados numa interface gráfica em modo usuário (GUI), que provêm meios para gerenciar uma ou mais bases de dados de um único computador. O OEM é composto por:

- Um conjunto de ferramentas administrativas;
- Um monitor de eventos que pode ser configurado para inspecionar situações específicas em sua base de dados;
- Um agendador de tarefas para executar tarefas de manutenção em horários definidos;
- Uma interface gráfica para o Recovery Manager Tools.

O OSS pode ser utilizado para implementar uma estrutura mais complexa de segurança para dados mais sensíveis, com os seguintes aspectos:

- Autenticação de usuário através de credenciais eletrônicas;
- Assinatura Digital;
- *Single Sign On (SSO)* .

Todas estas opções são implementadas em modo stand-alone. Em outras palavras, não é necessário que você tenha produtos de terceiros (por exemplo, Kerberos) ou qualquer outro produto da Oracle (por exemplo, o Advanced Networking Option) para fazer uso do OSS.

Entre as ferramentas não gratuitas da suíte do Oracle Server, podemos citar:

- ***Trusted Oracle***: provê segurança em diversos níveis (MLS - Multilevel Security);

- ***Advanced Networking Option***: utilizado para encriptar todos os dados trafegados no SQL*Net ou no Net8 entre cliente e servidor;
- ***Oracle Application Server*** (anteriormente chamado Web Application Server e agora Internet Application Server): utilizado para integração com aplicações baseadas na Web.

Segundo o fabricante, o Oracle é suportado por todas as plataformas, incluindo:

- WinNT;
- Win2000;
- Win98/95;
- AIX (Versão Unix da IBM);
- Linux
- HP-UX;
- SUN;
- OS/2.

3.1 Mecanismos de segurança

Por se tratar de um banco de dados multiplataforma, sua segurança não pode ser resguardada na segurança do sistema operacional em que foi instalado. Para isso, a instalação do Oracle segue uma política de depender o mínimo possível do sistema operacional, através da implementação de diversas medidas de segurança.

A primeira, e também mais básica, é a alteração das senhas dos usuários padrão do banco. Usuários como System (senha: manager), Sys (senha: change_on_install) e DBSNMP (senha: dbsnmp) são instalados com tais senhas padrão e têm um alto nível de acesso ao banco, o que pode comprometer por completo a segurança do mesmo.

O servidor Oracle fornece controle arbitrário de acesso, o que é um meio de restringir o acesso às informações privilegiadas. O privilégio apropriado deve ser atribuído por um usuário para que ele acesse um objeto de esquema. Os usuários com privilégios apropriados podem concedê-los a outros segundo o seu critério.

O Oracle8i introduz um controle detalhado de acesso e um modelo aprimorado de segurança para ambientes multicamadas. Esse controle usa um contexto de aplicações, extensível e orientado por parâmetros, para permitir que as aplicações controlem o acesso do usuário com base com base nos seus atributos, como o seu número e cliente. Por exemplo, para uma aplicação da Web, um administrador pode oferecer acesso a seus clientes externos, mas de modo que tenham acesso somente a seus próprios pedidos.

Atualmente, nas arquiteturas multicamadas, a camada intermediaria é normalmente insegura e pode realizar qualquer ação em nome de qualquer usuário. As camadas intermediarias, especialmente os servidores Web ou os servidores de aplicação, podem freqüentemente estar sobre ou atrás de uma proteção do tipo firewall, portanto, limitar seu acesso e auditar suas ações é importante.

O Oracle gerencia a segurança do banco de dados usando diversos recursos diferentes. Entre eles: usuários, domínio de segurança, privilégios, Papeis e auditoria.

3.2 Opções de Autenticação

Para acesso ao banco de dados, existem quatro formas de autenticação:

- Através de um arquivo de senhas;
- Autenticação herdada do sistema operacional (usuário autenticado previamente no sistema operacional);
- Arquivo de senhas e do sistema operacional;
- Autenticação nativa do banco de dados.

As três primeiras vão herdar confiabilidade do sistema operacional, o que pode vir a causar problemas. A política é sempre confiar no banco de dados, autenticando somente por ele e implementando uma boa política de senhas. Tal método de autenticação consta na view **V$SYSTEM_PARAMETER.**

Outra medida interessante seria alterar a porta de serviços padrão com o intuito de dificultar a identificação da funcionalidade dos ativos de banco de dados por meio de usuários maliciosos

3.3 Usuários

Abrange usuários e esquema do banco de dados onde cada banco de dados Oracle tem uma lista de nomes de usuários. Para acessar um banco de dados, um usuário deve usar um aplicativo desse tipo e tentar uma conexão com um nome de usuário valido. Cada nome tem uma senha associada para evitar o uso sem autorização.

Devem ser implementados ainda diferentes perfis de usuário para diferentes tarefas no Oracle, tendo em vista que cada aplicação/usuário tem a sua necessidade de acesso. Existe ainda a possibilidade de proteger os perfis com senha, o que é uma excelente medida. Além dessas medidas, o uso de cotas aumenta a restrição de espaço em disco a ser utilizado por usuários/aplicativos.

3.4 Domínio de Segurança

Onde cada usuário tem um domínio de segurança, um conjunto de propriedades que determinam coisas como ações (privilégios e papeis) disponíveis para o usuário; cota de tablespaces (espaço disponível em disco) do usuário; limites de recursos de sistema do usuário.

As tabelas (tablespaces) do sistema, como a system, devem ser protegidas de acessos de usuários diferentes dos usuários de sistema. A liberação de escrita e alteração de dados em tais tabelas é muito comum em ambientes de teste, onde os programadores e DBAs tomam tal atitude para evitar erros de aplicação por falta de privilégios. Porém, em ambientes de produção, tal medida é totalmente desaconselhável.

3.5 Privilégios

Um privilégio é um direito para executar um determinado tipo de declaração SQL. Alguns exemplos de privilégios incluem: Direito de conectar-se ao banco de dados; direito de criar uma tabela em seu esquema; direito de selecionar linhas da tabela de outra pessoa; direito de executar o procedimento armazenado de outra pessoa. Os privilégios são concedidos aos usuários para que eles possam acessar e modificar os dados do banco de dados. Os privilégios de um banco de dados Oracle podem se dividir em duas categorias distintas, descritas abaixo:

- Privilégios de sistema: Permitem que os usuários executem determinada ação no nível de sistema ou em determinado tipo de objeto de esquema. Alteração de qualquer linha de uma tabela por exemplo, são privilégios do sistema.

- Privilégios do objeto de esquema: Permitem que os usuários executem determinada ação em um objeto de esquema também especifico. O privilegio de exclusão de uma linha em uma tabela especifica por exemplo, é um privilegio de objeto.

3.6 Papéis

O Oracle fornece o gerenciamento fácil e controlado dos privilégios por meio dos papeis. Os papeis são grupos nomeados de privilégios relacionados que são concedidos aos usuários ou a outros papeis.

3.7 Auditoria

O Oracle permite a auditoria seletiva (monitoramento registrado) das ações do usuário para auxiliar na investigação de um suposto uso suspeito do banco de dados. A auditoria pode ser executada em três níveis diferentes: auditoria de declaração, auditoria de privilegio e auditoria de objeto de esquema. Para todos os tipos de auditoria, o Oracle permite a auditoria seletiva das execuções bem-sucedidas das declarações, das execuções que falharam ou de ambas. Isso permite o monitoramento de declarações suspeitas, independente do usuário que a emite ter os privilégios apropriados para produzi-la.

A auditoria do sistema aliada ao uso de *triggers* faz-se indispensável para manter o sistema sempre otimizado e resguardado de acessos indevidos. Outra medida importante, para qualquer implementação de banco de dados, é a implementação de uma política de backup que contemple a rotação dos arquivos de log e seu armazenamento off-site.

4.Conclusão

O DB2 pode apresentar vantagens em sustentar características de segurança para grupo de usuários onde a configuração com grupos ajuda a reduzir o custo total de posse

e reduz o trabalho manual do DBA permitindo que às autorizações e privilégios sejam atribuídas por grupo.

Por outro lado, o DB2 não obedece aos padrões de segurança propostos pelo Instituto Nacional de Padrões e Tecnologias (NIST) e a Agência de Segurança Nacional (NSA), enquanto isso os produtos Oracle participam de avaliações de critérios de FIPS-140 (Padrão de Processamento de Informação Federal 140-2) para módulos de criptografia.

O Banco de Dados Oracle 9i DataBase oferece proteção de dados conjuntamente com a característica de controle de acesso ao banco de dados, já a IBM constrói a segurança fora do banco de dados confiando em produtos como o SecureWay da Tivoli e o Sistema Operacional.

5.Referências Bibliográficas

ALMEIDA, Eduardo Brasil. **SEG – Segurança Lógica de Banco de Dados**. Ed.Campus. Aracajú, 2001.

GARCIA-MOLINA, Hector et alli. **Implementação de Sistemas de Banco de Dados**. Editora Campus. São Paulo, 2001.

AGIA, Rodrigo & ZEIDAN, Gustavo & BARROS, Augusto. **Banco de Dados.** Internet. http://www.modulo.com.br. Acessado em junho de 2005.