**BANCO DE DADOS SEGURO: COMO ESTRUTURAR E PROTEGER SUAS INFORMAÇÕES**

*SECURE DATABASE: HOW TO STRUCTURE AND PROTECT YOUR INFORMATION*

*BASE DE DATOS SEGURA: CÓMO ESTRUCTURAR Y PROTEGER SU INFORMACIÓN*

André Dias Martins**[[1]](#footnote-0)**

Fernanda Reis Veregue[[2]](#footnote-1)

**Resumo.** A informação é um dos bens mais preciosos da humanidade desde seus primórdios. No entanto, com a competitividade do mercado e os mais variados produtos e serviços, a informação se tornou chave para a prosperidade de todas as companhias, mas que para saber utilizá-la corretamente, precisa de uma ferramenta fundamental que são os bancos de dados, que gerenciam e guardam as preciosas informações das companhias, que por sua vez investem cada vez mais em segurança para que não tenham seus segredos revelados, desta forma o artigo trata sobre a medidas e precauções tomadas para a segurança dos banco de dados.

**Palavras-chave:** Informação. Banco de dados. Segurança.

**Abstract.** Information is one of the most precious possessions of mankind since its inception. However, with the competitiveness of the market and the most varied products and services, information has become key to the prosperity of all companies, but that to know it use correctly, needs a fundamental tool that are the databases, Who manage and store the precious information of the companies, who in turn invest more and more in security so that they do not have their secrets revealed, in this way the article deals with the measures and precautions taken for the security of the database.

**Keywords:** Information. Database. Security.

**Resumen:** La información ha sido uno de los bienes más preciados de la humanidad desde sus inicios. Sin embargo, con la competitividad del mercado y los más variados productos y servicios, la información se ha convertido en clave para la prosperidad de todas las empresas, pero para saber utilizarla correctamente se necesita una herramienta fundamental, que es la base de datos, la cual administra y almacena la preciada información de las empresas, que a su vez invierten cada vez más en seguridad para que sus secretos no sean revelados, por lo que el artículo trata sobre las medidas y precauciones que se toman para la seguridad de las bases de datos.

**Palabras clave:** Información. Base de datos. Seguridad.

**1 - Introdução**

O artigo refere-se à segurança dos bancos de dados, com os tópicos de banco de dados e suas variações em sistema de gerenciamento, métodos de segurança atual e soluções de problemas mais comuns de segurança. Mas primeiramente iremos conceituar o que é um banco de dados e para que ele serve.

Um banco de dados (ou em inglês: database) é uma entidade composta de uma coleção de tabelas que armazena um conjunto específico de dados estruturados e com a menor redundância possível. Pois antigamente as empresas utilizavam arquivos físicos para armazenar suas informações, algo muito custos e falho, mas com o surgimento dos computadores e suas constantes evoluções com as mais diversas aplicabilidades, possibilitou o armazenamento desses dados em uma forma digital, dando assim a evolução os bancos de dados ao longo do tempo, para o que conhecemos atualmente, o qual se tornou o coração dos diversos sistemas de informação (DEVELOPER NETWORK, 2016).

Um banco de dados permite a consulta, incluir ou até mesmo editar os dados disponíveis ao usuário, dependendo do nível de acesso que ele possui, mantendo um registro das atividades realizadas. Isso se tornou muito útil, pois os dados informáticos são cada vez mais numerosos. Um banco de dados pode ser local, utilizado por um usuário em sua máquina local, ou remoto, utilizado por vários usuários através de internet, intranet ou extranet, a qual possui um servidor que compartilha os dados com os demais. Uma das vantagens mais essenciais da utilização dos bancos de dados é a possibilidade de poder ser acessado por vários usuários simultaneamente.

Os sistemas de gerenciamento de banco de dados (conhecidos como SGBDs), são responsáveis pela manipulação dos dados no banco e a interação dos usuários com os dados, atualmente existe vários tipos de SGBDs: Oracle, SQL Server, DB2, PostgreSQL, MySQL, o próprio Access ou Paradox, entre outros (REZENDE, 2016).

Os dados nada mais são que fatos brutos, em sua forma primária. E muitas vezes o um dado sozinho ou fragmentado pode não fazer nenhum sentido, mas depois de sua inserção e manipulação em um banco de dados, torna-se uma informação que consiste no agrupamento dos dados coletado e organizada para fazer sentido, gerando o conhecimento, o é um dos maiores bens de uma empresa ou organização (FURTADO, 2016).

Os dados são tão valiosos quanto a nossa capacidade de acessar e extrair o significado dele, e não podemos extrair o significado se eles não tem organização, armazenamento, e não podemos analisá-lo de forma eficaz.

**Metodologia**

O presente artigo caracteriza-se como uma pesquisa bibliográfica sobre a segurança dos bancos de dados, por meio do estudo e análise de material relacionado e experiências encontradas no meio digital e literal.

As informações levantadas durante a pesquisa vão ser detalhadas em tópicos nos quais, apresentaram necessidade da segurança, maneiras de deixar seu banco de dados seguro, e vantagens de um banco de dados seguro.

A pesquisa se dará através da informação sobre os métodos de segurança nos banco de dados.

## **Instrumentos e materiais de pesquisa:**

Utilizamos os seguintes materiais e instrumentos para coleta de dados:

a) Sites: Ferramenta utilizada na busca de informações e experiências de diversas formas, auxiliando no esclarecimento de dúvidas.

b) Artigos: Auxilado na pesquisa e contribuindo na base legal das informações.

**Tipos de bancos de dados**

Existe vários gerenciadores de banco de dados alguns dos mais conhecidos são: Oracle, Microsoft Access, IBM DB2, Microsoft SQL Server, MySQL, SQL Lite, Paradox, Access e dBASE, entro outros mais, o banco de dados pode ser pequeno a ponto de ser instalado e gerenciados em um computador comum (Desktop) que pode ser utilizados por Microempresas que gerencia poucas tabelas e funções, mas já outros podem ser tão grandes a ponto de serem armazenados em servidores de rede, onde gerencia milhares de tabelas e funções complexas, estes por sua vez são utilizados por: países, estados, grande empresa e entre outros que precisam armazenar muita informação.

## **A necessidade de um banco de dados seguro**

Tratando de banco de dados, muitas companhias recorrem a certos formulários que não condizem com a forma correta sobre a segurança de seus dados, o problema é que em muitas das vezes a empresas preza a desempenho do banco de dados, deixado de lado as prioridade sobre a segurança, embora o ideal a se fazer é sempre tentar manter equilíbrio entre desempenho e segurança, mas isso nem sempre é aplicado na prática (CHICKOWSKI, 2016).

Os DBAs (administrador de banco de dados) e desenvolvedores de aplicativos simplesmente não disponham de tempo ou não querem tratar da segurança, deixando-a de lado, porque isso aumenta o custo do desenvolvimento de produtos, pois eles são cobrados para adicionar mais aplicações e funcionalidades, que por sua vez aumentará o volume de dados a ser processado, com isso um aumento circunstancial nos ciclos de testes. Assim o programador ou desenvolvedor precisa fazer ciclos extras para amarrar e adicionar camadas de segurança em volta das aplicações, caso contrário alguns hackers e vírus podem tirar proveito dessas brechas que são deixadas, por conta de uma falta de prioridades dos departamentos de TI. Através das brechas são acessados dados que não deveriam ser acessados, atacando o SQL e tirando proveito da vulnerabilidade encontrada nos links de aplicativos do banco de dados e liberando problemas para o sistema, levando assim, acessar dados estratégicos restritos da empresa ou organização (CHICKOWSKI, 2016).

Para Elmasri e Navathe (2011), a segurança de banco de dados é implementada para resolver as seguintes questões:

* Questões legais e éticas relacionadas ao direito de acessar determinadas informações;
* Questões políticas em nível governamental, institucional ou corporativo relativas a informações que devem ter sua confidencialidade mantida.
* Questões de sistema, envolvidos com níveis de sistema, como a definição da forma de tratamento da segurança, se esta será tratada no nível de hardware, no nível de sistema operacional ou no nível de SGBD.
* A necessidade de identificar níveis de segurança para classificação dos dados.

**Maneiras de deixa seu banco de dados seguro:**

A maneira de conseguir proteger o banco de dados é priorizar a segurança de dados críticos como primeira preocupação. Definindo três princípios fundamentais de proteção de base de dados.

**Conhecendo o banco:**

Atualmente muitas companhias, não conseguem proteger seus dados críticos, por não entender como funciona o ambientes externo (ambiente dos usuários finais) do seu próprio banco de dados, para o desenvolvedor e DBAs controlar essas informações, ele precisa conhecer e entender com máxima clareza onde estão localizadas, como estão e quem as utiliza, desconhecendo essas informações, você pode não saber quem usa os sistemas caso tenha concedido muitos privilégios, ou nem ao menos sabem onde os dados críticos estão ou se foram feitas cópias do sistema. Para que não ocorra as situações citadas acima, a equipe de desenvolvimento deve documentar seus esquemas de autorização e a sua classificação dos banco de dados para que a possa analisar os riscos para a companhia.

Uma vez que o banco de dados está bem localizado e seguro, os DBAs pode avaliar sua vulnerabilidade, para que possam decidir o nível de proteção que necessitam configurar e ferramentas que precisam utilizar, para que possam conseguindo controlar os acesso, identificar o'que foi e onde foi acessado e por quem foi acessado, mas tais ferramentas de monitoramento e auditoria em sua premissa, tiveram algumas deficiências, que por sua vez acabaram tendo uma má reputação em os DBAs, deficiências essa as quais traziam lentidão e algumas falhas de segurança, com o passar do tempo foram se corrigindo essa deficiências, mas o medo ainda persiste, pois quando se trata de banco de dados desempenho é um ponto chave, tanto para a companhia quanto para seus utilizadores (CHICKOWSKI, 2016).

**Banco de dados limpo:**

Uma vez que a empresas não alteram as suas senhas do banco de dados, concedem privilégios para os usuários sem a sua real necessidade, deixam dados críticos sem suas devidas correção ou falham em seu gerenciamento das configurações de banco de dados, isso tudo pode chamar atenção de hackers e vírus, muitos vez DBAs e desenvolvedores deixam não alteram as senha padrões dos bancos, na intenção de agilizar a sua administração e integração com as aplicações, isso também facilita a invasão e exposição das informações contidas no sistema. Todos os bancos de dados vêm com um pré-configuração de usuário e senha padrão, isso é feito para facilitar as instalação e integração muito utilizada no meio acadêmico, por essa facilidade, mas quando se trata de um banco de dados de empresas onde se encontra informações valiosas e sigilosas, esse padrão deve ser quebrado.

Pois os invasores podem se utilizar desses padrões, para que de uma forma maliciosa acesse os bancos, fazendo downloads de informações ou até mesmo deletando e alterando elas, dessa forma ao eliminar os padrões, melhora em muitos aspectos a postura mediante a segurança. Isso ocorre, em algum caso, por ser óbvio demais, acabam que deixando passar. Muitas empresas acabam distribuindo muitas credenciais, não removendo elas depois que a um desligamento de usuários, isso também criar algumas vulnerabilidades internas, isso ocorre quando o tempo e recursos estão no limite, pois as companhias muitas vezes, não gastam tempo definindo quem é o quê acessar ou até mesmo qual banco acessar.

Dessa forma eles concedem privilégios a grupos inteiros de usuários, por motivos que os usuários utilizam se do mesmo banco de dados para realizar sua função na empresa. Isso ocorre naturalmente, pois é da mesma forma que as companhias contestam as atualizações e os gerenciamentos de vulnerabilidades, pois isso requer tempo, deixando o sistema ocioso durante a transição. As atualizações em tese são feitas para melhorar e otimizar o desempenho do sistema ou banco de dados, mas nem sempre os resultados são satisfatórios, risco de perder desempenho é real, pois como já citado acima o desempenho de um banco é o ponto chave para algumas empresas, mesmo com os riscos as companhias não podem deixar de pensar nas correções de suas bases de dados críticas, pois isso afetaria diretamente a sua segurança. Segundo Rothacker (2017), assim, os invasores vão ter que fazer engenharia reversa das atualizações com as correções para conseguir realizar uma invasão bem sucedida, isso requer muito tempo e disposição, pois até conseguir, uma nova atualização já terá sido lançada, inviabilizando esse processo (CHICKOWSKI, 2016).

**Conexão com o banco**

As infra estruturas dos bancos de dados tem que ser tão bem segura quanto os próprios bancos de dados, pois os hackers constantemente acessam os bancos através da camada de aplicação, utilizando se SQL para atacar. Desta forma engana os bancos de dados expondo mais informações do que o desenvolvedor pretendia, as equipes de segurança, os DBAs e os gerentes de aplicações devem realizar análises em conjunto para corrigir as exposições, inserindo validações no banco de dados para evitar essas vulnerabilidades.

Dessa forma as equipes devem observar todas as formas de ataque ao banco, quando forem planejar a segurança do mesmo, ressaltando que os bancos devem ser acessados somente por usuários autorizados a ver tais informações, funções e entre outros contidos no banco de dados indicado. Pois isso tudo ao redor de um banco de dados deve ser seguro, desde o nível de hospedagem da rede e até as aplicações. Tudo isso advertindo faz parte da base de uma boa estratégia para proteção crítica de banco de dados.

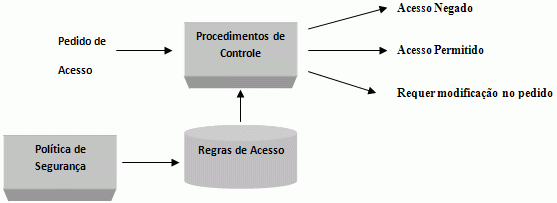
Esses esforços são constantes, pois não podem parar com as configurações e monitoramento dos bancos de dados, sempre que aplicado às correções cabíveis e verificações das aplicações, mantendo os bancos de dados críticos em sua parte mais segura da rede.

**Conceitos sobre segurança em banco de dados**

A segurança do banco de dados enfrenta as mesmas dificuldades passadas pela segurança de informação, que são: garantir a integridade, disponibilidade e a confidencialidade das mesmas. Abaixo estão os conceitos sobre a segurança dos bancos de dados.

**Controle de acesso:**

São todos controles feitos quando é realizado um acesso ao banco de dados, controle esse que impõem regras de restrição aos usuários. O DBAs é por sua vez o responsável com o mais alto nível de acesso, declarando assim as regras existentes dentro de um SGBD, ele é quem conceder ou remover privilégios, criar ou excluir usuários, de acordo com a necessidade e a política da empresa onde ele opera as sua função, exemplificada na figura 1 abaixo (MACÊDO, 2017).



**Figura 1 - Exemplo de sistema de controle de acesso**

**Controle de Inferência:**

Banco de dados estatístico possui esse mecanismo de segurança para poder proteger suas informações estatísticas de um cliente ou de um grupo de clientes, esses bancos são muito utilizados para a geração de dados estatísticos sobre vários grupos de clientes, quando configurado o mecanismo o usuário terá acesso à informação estatística dos diversos grupos, não tendo acesso os dados de apenas uma pessoa em específico, protegendo assim os dados pessoais do indivíduo (MACÊDO, 2017).

**Controle de fluxo:**

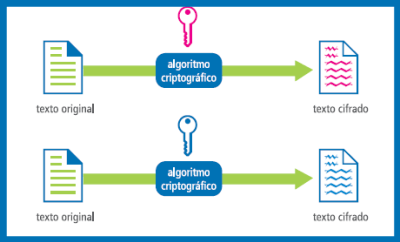
Mecanismo que previne que as informações trafeguem por meios secretos ou que violem a política de segurança instanciadas pelo DBAs, para que não chegasse em usuários não autorizados. Ele regula a distribuição ou tráfego das informações entre objetos acessíveis, esse monitoramento ocorre para que mesmo que de maneira indireta os dados caiam diretamente aos usuários não autorizados (MACÊDO, 2017).

**Criptografia**

Essa uma medida de controle final, utilizada para realizar a proteção de dados sigilosos que ao serem transmitidos por meio de comunicação, seja ela via internet ou intranet, também podendo ser utilizada como uma proteção adicional no banco de dados, assegurando a partes confidenciais para que usuários não autorizados acessem essas partes do banco. Isso é realizado através de um algoritmo de codificação que codifica os dados, tornando-os inúteis para os usuários não autorizados, mas pra quem tiver o acesso autorizado aos dados é conferida uma chave para decifrar os mesmo, abaixo estão dois modelos de criptografias por chaves Simétricas e Assimétricas (MACÊDO, 2017).

**Chaves simétricas:**

A esse sistema de criptografia e a decriptografia se utilizam apenas de uma chave para ambos os processos, conhecida também como criptografia convencional. A criptografia basicamente é a transformação de um texto original em texto criptografado, que se utiliza apenas uma chave secreta todo o seu processo, no qual utiliza um algoritmo que faz encriptar dados, e para reverter esse processo é necessário a chave e um algoritmo de decriptografia, exemplificar na figura 1 abaixo (MACÊDO, 2017).



**Figura 2 - Chave Simétrica sendo criptografada e descriptografada**

**Chaves assimétricas:**

Segundo Galvão (2017) a criptografia de chave pública ou criptografia assimétrica é um método de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada.

A chave pública pode ser distribuída livremente para todos os usuários, através de e-mail ou outras formas de comunicação, enquanto que a chave privada deve ser mantida sobre a posse de seu legítimo dono.

Utilizando um algoritmo de criptografia assimétrica, a mensagem ou dado encriptado com a chave pública, pode somente ser desencriptado pela sua chave privada correspondente.

Os algoritmos de criptografia assimétrica podem ser utilizados para realizar autenticidade e confidencialidade das informações. Para utilizar como confidencialidade, a chave pública é usada para encriptar mensagens, com isso apenas o possuidor da chave privada pode desencriptar-la conseguindo saber o conteúdo da mesma, já para o método autenticidade, a chave privada é usada para cifrar mensagens, garantindo que apenas o detentor da chave privada corresponde poderia ter cifrado a mensagem que foi decifrada com a “chave pública”, como mostra a figura 2 (PINTO, 2017).



**Figura 3 - Exemplo de chaves assimétricas**

**Usuários:**

São implementados diferentes perfis de usuário para que realizem tarefas e possuem privilégios diferentes, tendo em vista que cada aplicação/usuário tem a sua necessidade de acesso, a também existe também a possibilidade do uso de senha que protege os usuários de realizar acessos não autorizados em perfis diferentes (SILVA, 2017). Segundo Cabrera (2017) existem basicamente quatro categorias de usuários finais de banco de dados, as quais são.

* Usuários Casuais: Que acessam o banco de dados casualmente, mas que em cada acesso venha a necessitar de diferentes informações, fazendo o uso de uma linguagem mais complexa para atender às suas necessidades no momento da utilização.
* Usuários Iniciais: Que se utiliza de consultas no banco de dados já pré-estabelecidas, que foram testadas, esse tipo de usuário é também chamado de comum, que faz sua interação através de definições pré-estabelecidas a ele.
* Usuários Intermediários: São aqueles tipo de usuários que já detêm uma experiência maior com utilizem os banco de dados, realizando consultas mais complexas e elaboradas.
* Usuários Avançados: Este por sua vez tem total domínio dos banco de dados, pode até escrever aplicações especializadas.

**Domínio de segurança:**

É um conjunto de propriedades definidas pelo DBAs que determinam as ações, os privilégios e os papeis em que cada usuário se encaixa de acordo com a sua função ou determinação da empresa, o domínio de segurança também regulamenta espaço em disco disponível para cada usuário (cota de tablespaces) e recursos computacionais (MACÊDO, 2017).

As tabelas do sistema, como a system, são restritas e protegidas para que o usuário do sistema não tenha acesso, pois o acesso deve ser feito pelos DBAs exclusivamente. A liberação ao acesso destas tabelas é muito comum em ambientes de teste, onde os desenvolvedores e DBAs tomam as atitudes que evitam erros na aplicação pela falta de privilégios que restringem os usuários, evitando assim falhas no ambiente para o usuário final (SILVA, 2017).

**Autoridade:**

Segundo Macedo (2017) através da autoridade é feito métodos para agrupar privilégios e conceder os níveis de acesso dos administradores, operadores dos bancos de dados com relação à manutenção e operações permitidas. Essas especificações iriam ficar armazenadas em catálogos na própria base de dados. As autoridades do sistema estão associadas a membros de grupos e ficam mantidas essas configurações administrativas no próprio banco de dados. Estas configurações por sua vez irão conceder os acessos que cada grupo poderá fazer (OLIVEIRA; SPINOLA, 2016).

**Privilégios:**

Os privilégios são as permissões dadas aos usuários ou grupo de usuários, para que possam acessar os dados, são elas que definem as autorizações de visualização ou modificação, que o usuário pode acessar em um banco de dados (MACÊDO, 2017).

Os privilégios por sua vez também são mantidos em catálogos no próprio banco de dados, como nas autoridades que por já possuírem grupos pré-definidos de privilégio, concedendo implicitamente privilégios a seus usuários (MACÊDO, 2017).

**Tipos de privilégios:**

Os Sistemas Gerenciadores de banco de dados oferecem um acesso seletivo com relação ao banco de dados, pois cada conta específica tem seus privilégios e banco nos quais o usuário pode sim ou não acessar, desta forma o controle é eficiente, pois ao possuir um conta no sistema, não quer dizer que irá ter acesso total ao SGBD (ROCHA, 2013). Segundo Macedo (2017) informalmente existe dois níveis para poder atribuir privilégios fazer o uso do sistema de banco de dados:

* O nível de conta: Nesse nível, o DBA estabelecerá os privilégios específicos que cada conta irá possuir sobre o banco, independente das relações no mesmo, podem incluir privilégios como: CREATE TABLE, CREATE VIEW, ALTER, DROP, MODIFY e SELECT.
* O nível de relação: O DBA pode controlar o privilégio para acessar cada relação ou visão individual no banco de dados, são especificados para cada conta de usuário e sobre quais tipos de comandos podem ser aplicados nas relações individuais.

Abaixo estão alguns exemplos de concessão de privilégios a grupos e usuários:

* Concede a todos os usuários, o privilégio de realizar inserções na tabela finanças:

(GRANT INSERT ON finanças TO PUBLIC;)

* Concede um usuário especifico “joao” todos os privilégios disponíveis na visão “vis\_tipos”:

(GRANT ALL PRIVILEGES ON vis\_tipos TO joao;)

* Concede ao usuário márcio, todos os privilégios no banco contabilidade e estende ainda a ele a possibilidade de conceder privilégios a outros usuários:

GRANT ALL ON DATABASE contabilidade TO márcio WITH GRANT OPTION

**Revogação de privilégios:**

A revogação de privilégios é muito útil, uma vez que um determinado usuário precisar acessar temporariamente um informação, isso faz com que o proprietário de uma relação conceda o acesso ao usuária, que uma vez concluída a tarefa essa autorização será revogada facilitando para ambos, dessa forma esse mecanismo se faz muito necessário para a revogação de privilégios, que no SQL, o comando é “REVOKE”, quando introduzido no contexto correto exemplificado abaixo, revoga a autorização ao privilégios que lhe foi concedida (ROCHA, 2013).

* REVOKE [ GRANT OPTION FOR ]

{ { SELECT | INSERT | UPDATE | DELETE | RULE | REFERENCES | TRIGGER }

[,...] | ALL [ PRIVILEGES ] }

ON [ TABLE ] nome\_da\_tabela [, ...]

FROM { nome\_do\_usuário | GROUP nome\_do\_grupo | PUBLIC } [, ...]

[ CASCADE | RESTRICT ]

**Controle de acesso obrigatório e para segurança multinível:**

Ao utilizar este método, não existe um meio termo para o usuário, pois o lhe foi concedido os privilégios necessários e ou ele não terá acesso aos dados, método este utilizado normalmente em bancos de dados que classificam dados de usuários, por ser exigido um nível superior de segurança. Em sua grande maioria os SGBDs não oferecem esse tipo de controle de acesso como sendo obrigatório, normalmente são utilizados os métodos de controle descritos nos tópicos anteriores. Por serem mais complexos, normalmente são utilizados em sistemas governamentais ou de inteligência, também utilizados em corporação multinacional, pelo seu alto poder de segurança (MACÊDO, 2017).

As classes de segurança típicas são altamente sigilosas: (top secret, TS), secreta (secret, S), confidenciais (confidential) (C) e não Classificada (unclassified, U), em que TS é o nível mais alto e U é o mais baixo.

Em resumo, para Macedo (2017) os mecanismos de controle de acesso obrigatório impõem segurança multinível, pois exigem a classificação de usuários e de valores de dados em classes de segurança e impõem as regras que proíbem o fluxo de informação a partir dos níveis de segurança mais altos para os mais baixos (OLIVEIRA; SPINOLA, 2016).

**Controle de acesso baseado em papeis:**

Trata sobre o assunto de restringir o acesso a usuários autorizados é uma alternativa para os sistemas de controles de acesso do tipo MAC (controle de acesso obrigatório) e DAC (controle de acesso discricionário). O primeiro conceito de controle de acesso baseado em papeis foi criado juntamente com os primeiros sistemas computacionais multiusuários interativos. De acordo com o RBAC (controle de acesso baseado em funções) é que permissões de acesso são associadas a papeis, e eles são associados aos usuários. Os papeis são criados de acordo com os vários cargos que existem em uma organização, já os usuários são associados a papeis de acordo com as suas principais responsabilidades, qualificações e determinações pela empresa, sendo que vários usuários podem ser designados para cada papel. Os privilégios de segurança comuns a um papel são atrelados ao nome dele, e qualquer usuário destinado a este papel automaticamente receberia os privilégios concedidos (MACEDO, 2017).

Esse método de controle facilita a realocação de usuários de um papel para outro, dessa forma as mudanças no ambiente computacional, instalação de novos sistemas e remoção de aplicações antigas, modificam apenas o conjunto de permissões atribuídas aos diferentes papeis, sem o envolvimento direto de um conjunto de usuários, não afetado as estrutura deles (MACEDO, 2017).

A separação entre as tarefas é um requisito muito importante em diversos SGDBs, impedindo o usuário de realizar sozinho o trabalho que necessariamente requer o envolvimento de outros indivíduos, essa exclusão mútua de papeis é um método que pode ser implementado com sucesso (MACEDO, 2017).

Outro aspecto bem relevante sobre o sistemas RBAC são as restrições temporais possíveis, pode vir a existir nos papeis se implementadas, com tempo e duração da ativação nos papéis, isso pode ser disparado com implementação temporária em um papel que requer temporariamente a ativação de outro. O uso deste modelo RBAC é um objetivo altamente desejado como principal métodos de requisição na segurança de aplicações baseadas na web (OLIVEIRA; SPINOLA, 2016).

**Conclusão:**

Diante do exposto as bases de dados atuais precisam ser minuciosamente construídas, constantemente verificado e corretamente limpa, pois as vezes por falha ou vícios de programação, deixamos brechas vitais que podem causar a ruina de uma base de dados, fazendo com que a confidencialidade e confiabilidade dos dados fique duvidosa e comprometida, pois o principio de um banco de dados e garantir as qualidades acima citadas.

As etapas acima expõem os métodos que são utilizados em uma construção mais segura de um banco de dados, usando corretamente de acordo com as necessidade e normas de uma empresa. Essa construção pode ser bem sucedida, pois não bastante guardar bem os o seus servidores, isso requer a junção de todos os requisitos bem como: infraestrutura, uma base bem estruturada, com todos os seus controles configurados e criptografias.

Conclui-se que para uma base ser segura a constância em manutenção e reorganização se faz necessária, pois um base grande pode conter vários registro e privilégios concedidos que não estão sendo mais utilizado ou que foram disponibilidade de formar errado comprometendo a sua estrutura, bem como também ao acesso a área externa da base, pois la o acesso deve ser liberado apenas para pessoas autorizadas e com um alto nível de conhecimento.

###### **REFERÊNCIAS:**

CABRERA, Antonio Parron. **Quem são os usuários de um SGBD?**: Usuários Finais. Disponível em: <https://programandoesalvando.wordpress.com/2014/11/18/quem-sao-os-usuarios-de-um-sgbd/>. Acesso em: 26 fev. 2017.

CHICKOWSKI, Ericka. **3 passos para tornar seu banco de dados mais seguro:** Frequentemente eles pecam nas questões de desempenho e segurança. Disponível em: <http://www.itforum365.com.br/noticias/detalhe/2335/3-passos-para-tornar-seu-banco-de-dados-mais-seguro>. Acesso em: 29 jul. 2016.

DEVELOPER NETWORK, Microsoft. **Bancos de dados**. Disponível em: <https://msdn.microsoft.com/pt-br/library/ms179422(v=sql.120).aspx>. Acesso em: 15 jul. 2016.

ELMASRI, Ramez e NAVATHE, Shamkant B. **SISTEMAS DE BANCO DE DADOS**. 6. Ed. São Paulo: Pearson Addison Wesley, 2011.

FURTADO, Gustavo. **O que é um Banco de Dados?**. Disponível em: <http://www.dicasdeprogramacao.com.br/o-que-e-um-banco-de-dados/>. Acesso em: 24 jul. 2016.

GALVÃO, Junior . **Diferenças entre chaves simétrica e assimétrica para criptografia**. Disponível em: <http://Diferenças entre chaves simétrica e assimétrica para criptografia>. Acesso em: 25 fev. 2017.

MACÊDO, Diego. **Um pouco de tudo sobre T.I.**: Conceitos sobre Segurança em Banco de Dados. Disponível em: <http://www.diegomacedo.com.br/conceitos-sobre-seguranca-em-banco-de-dados/>. Acesso em: 25 fev. 2017.

MACÊDO, Diego. **Chaves Simétricas e Assimétricas**. Disponível em: <http://www.diegomacedo.com.br/chaves-simetricas-assimetricas/>. Acesso em: 26 fev. 2017.

OLIVEIRA, Viliane de Souza; SPINOLA, Rodrigo Oliveira . Obtendo bancos de dados seguros: Conteúdo sobre boas práticas. **Windows Azure Seu banco de dados na nuvem**, Revista SQL Magazine, v. 108, p. 27-28, mar. 2016.

PINTO, Pedro. **Criptografia simétrica e assimétrica**. Sabe a diferença?. Disponível em: <https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/>. Acesso em: 25 fev. 2017.

SILVA, Alana Van Der Vinne da. **Conceitos sobre Segurança em Banco de Dados**. Disponível em: <http://docplayer.com.br/17992042-Conceitos-sobre-seguranca-em-banco-de-dados.html>. Acesso em: 27 fev. 2017.

REZENDE, Ricardo. **Conceitos Fundamentais de Banco de Dados**: Conheça nesta matéria os conceitos fundamentais sobre banco de dados. Disponível em: <http://www.devmedia.com.br/conceitos-fundamentais-de-banco-de-dados/1649>. Acesso em: 25 jul. 2016.

ROCHA, Luciano Roberto. **BANCO DE DADOS WEB**: concessão e revogação de privilégios. Curitiba: Www.lrocha.com, 2013. 18 p. Disponível em: <http://www.lrocha.com.br/arquivos/arquivos/BdWeb (PostgreSQL)/AULAS/bd\_a9.pdf>. Acesso em: 31 ago. 2013.

ROTHACKER, Alex . **TeamSHATTER**. Disponível em: <http://www.teamshatter.com/>. Acesso em: 07 jan. 2017.

1. André Dias Martins: Bacharel em Administração; Bacharel em Sistemas de Informação; Licenciado em Sistemas de Informação; Licenciado em Pedagogia; Licenciado em Matemática; Mestre em Ensino e Tecnologia e Doutor em Educação Ciência e Matemática. E-mail: andre.dias@fatecie.edu.br [↑](#footnote-ref-0)
2. Fernanda Reis Veregue: Bacharel em Química; Licenciada em Química; Especialista em Didática e Metodologia do Ensino Básico e Superior; Mestre em Química e Doutora em Química; Doutorado sanduíche na Colorado State University (CSU), nos Estados Unidos. [↑](#footnote-ref-1)