Volume 5, número 1, dezembro de 2021
REVISTA DE TECNOLOGIA INVEST

Artigo 6

Importância da Segurança em Banco de Dados

Gleice Ferreira Marques[1]
Rafael Cardoso Costa Cruz[2]

RESUMO

Um banco de dados possui algumas propriedades por meio das quais mostra que sua abrangência vai muito além de uma mera coleção de dados. Importante mencionar que um banco de dados pode conter informações de extrema valia tanto para uma empresa quanto para as pessoas. Assim, a divulgação de informações não autorizadas pode afetar a empresa de variadas maneiras, como levar a perda de clientes ou de mercado, ou até mesmo a ações judiciais. Para manter a segurança do bem mais valioso de uma pessoa ou empresa, existem alguns atributos significativos inerentes à segurança da informação que, se aplicados de forma correta, ajudam na proteção das informações, sendo estes: integridade; disponibilidade e confidencialidade. Desta forma, a fim de proteger contra ameaças, medidas de controle de acesso devem garantir a inviolabilidade dos atributos de segurança da informação supramencionados. Dada a relevância da temática, o presente artigo objetiva demonstrar a importância da segurança em banco de dados. Para tanto foram realizadas pesquisas bibliográficas baseadas em livros da área de banco de dados, segurança da informação e outras publicações correlatas. Face o exposto, ficou evidenciado que a segurança em banco de dados é de suma importância, pois é onde fica armazenada a maior parte das informações de uma empresa, e, portanto, necessita ter um cuidado especial. Não é trivial manter um banco de dados seguro, uma vez que se necessita criar uma rigorosa lista de métodos e práticas para manter a integridade das informações.

Palavras-chave: Banco de dados; Segurança; Integridade; Disponibilidade; Confidencialidade.

[1] Pós-graduada em Banco de Dados pela UFMT (2017), Pós-graduada MBA em Gestão de Projeto pelo IPOG - Instituto de Pós-Graduação - Cuiabá (2021), graduada em Análise e Desenvolvimento de Sistemas pelo Centro Universitário UNIVAG (2015). Docente do ensino superior nas turmas de computação da faculdade INVEST, já atuou como professora nos cursos técnicos em informática no Centro Universitário UNIVAG.
[2] Bacharel em Ciências da Computação pela Faculdade Invest de Ciências e Tecnologia.

ABSTRACT

A database has some properties through which it shows that its scope goes far beyond a mere collection of data. It is important to mention that a database can contain extremely valuable information for both a company and people. Thus, the disclosure of unauthorized information can affect the company in a variety of ways, such as leading to loss of customers or the market, or even legal action. To maintain the security of the most valuable asset of a person or company, there are some significant attributes inherent to information security that, if applied correctly, help to protect information, namely: integrity; availability and confidentiality. Thus, in order to protect the database against threats, access control measures must guarantee the inviolability of the aforementioned information security attributes. Given the relevance of the theme, this article aims to demonstrate the importance of database security. For this purpose, bibliographic searches were carried out based on books in the area of database, information security and other related publications. In view of the above, it became evident that database security is of paramount importance, as it is where most of a company's information is stored, and therefore needs to be especially careful. It is not trivial to maintain a secure database, since it is necessary to create a rigorous list of methods and practices to maintain the integrity of the information.

Keywords: *Database; Safety; Integrity; Availability; Confidentiality*.

1. INTRODUÇÃO

Este artigo consiste em dissertar acerca da importância da segurança em banco de dados, um ponto de extremo valor para qualquer empresa e pessoas que almejam manter a integridade, a disponibilidade e a confidencialidade de seus dados, uma vez que é a base para crescer no mercado que está cada vez mais competitivo.

Foi realizada uma pesquisa bibliográfica sobre a importância da temática, trazendo uma reflexão do conhecimento em segurança em banco de dados, difundir o conhecimento, apresentar os principais conceitos, dissertar a respeito das principais vantagens no qual oferece e compreender como se pode criar mecanismos que assegurem a qualidade dos dados, direitos de propriedade intelectual e sobrevivência do banco de dados.

O artigo busca esclarecer questões pertinentes à segurança em banco de dados, quais sejam: O que é segurança em banco de dados? Qual a relevância da segurança em banco de dados para uma empresa? Como garantir a confidencialidade, integridade e disponibilidade da informação de acordo com a política de segurança?

A utilização conjunta de ferramentas aplicadas a uma política de segurança adequada, pode propiciar controle de acesso com satisfação para atender às principais necessidades das empresas.

Com o uso de sistemas baseados em tecnologia, atualmente o Banco de Dados é uma importante ferramenta para as organizações. Com esse crescimento, surge uma grande preocupação em relação a questões de segurança dos dados. Assim, o presente artigo justifica-

se frente a relevância da temática, que 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. Assim, espera-se ao final desse artigo conseguir demonstrar a relevância e de que forma é viável manter o banco de dados seguro.

2. REFERENCIAL TEÓRICO

Nesta seção será abordada os conceitos sobre banco de dados, segurança em banco de dados, apresentar medidas de controle de acesso à informação e conceitos sobre o segurança em banco de dados em dispositivos móveis.

2.1. Banco de Dados

Tempos atrás, as empresas armazenavam as informações em arquivos físicos, o que gerava grande acúmulo de papel e ainda, dificultava a organização, atualização e o acesso a essas informações. Entretanto, o surgimento e evolução das tecnologias computacionais, fez com que as empresas passassem a investir na aquisição de computadores e assim, as informações passaram a ser armazenadas em bancos de dados digitais.

No entendimento de Date (2003, p. 10), “um banco de dados é uma coleção de dados persistentes, usada pelos sistemas de aplicação de uma determinada empresa”.

Segundo Korth, Silberschatz e Sudarshan (1999):

> Um banco de dados “é uma coleção de dados inter-relacionados, representando informações acerca de um domínio específico, isto é, sempre que for possível agrupar informações que se relacionam e tratam de um mesmo assunto, pode-se dizer que se tem um banco de dados”.

Possui algumas propriedades por meio das quais mostra que sua abrangência vai muito além de uma mera coleção de dados. A primeira propriedade faz menção a este ser um conjunto lógico e ordenado de dados que possui significado. Segundo Machado (2008), não será considerado banco de dados uma coleção de dados aleatória, isto é, sem uma finalidade ou objetivo. Um dos objetivos é representar um minimundo ou universo de discurso onde são consideradas as propriedades de objetos que interessam aos usuários para fins de processamento computacional (ELMASRI; NAVATHE, 2011).

Neste contexto, um banco de dados tem tamanho e complexidade diferentes. Como exemplo de dispositivo, pode-se citar o celular, o qual pode conter um ou mais banco de dados de pequeno porte e ainda, baixa complexidade. Já como exemplos maiores podem ser considerados os da Amazon.com e Alibaba.com, empresas multinacionais com atuação mundializada e que comercializam produtos, tais como: jogos, eletrônicos, livros, roupas, entre outras coisas, oriundas de vários pontos do planeta junto a consumidores igualmente distribuídos ao redor do globo terrestre.

Ademais, é possível tomar como exemplo situações comuns como uma lista telefônica, um catálogo de CDs ou um sistema de controle de RH de uma empresa, pode ser comparado a um armário de arquivamento, em outras palavras, ele é um recipiente para uma coleção de arquivos de dados computadorizados (DATE, 2003).

É possível colocar à disposição de usuários dados para uma consulta, uma introdução ou uma atualização, garantindo os direitos conferidos a esses últimos. Referido instrumento torna-se ainda mais útil quando os dados são cada vez mais numerosos. Face ao exposto, a vantagem primordial é a possibilidade de acesso aos dados poder ser efetuada por diversos usuários, de maneira simultânea, além de favorecer a busca de informações, eliminando os arquivos de papéis, integrando os dados de aplicações e, portanto, concedendo segurança.

Para Elmasri e Navathe (2011), um modelo de dados é um conjunto de conceitos empregados para descrever a estrutura e as operações. Neste sentido, busca sistematizar a compreensão que é desenvolvida acerca de objetos e fenômenos que serão representados por um sistema informatizado.

Todavia, os objetos e fenômenos reais são muito complexos e impossibilitam uma representação completa, assim, é imprescindível construir uma abstração dos objetos e fenômenos do mundo real, de forma a obter uma maneira de representação conveniente que seja apropriada às finalidades das aplicações do banco de dados. O êxito da implementação em computador de um sistema de informação depende da qualidade desta transposição de entidades do mundo real e suas interações para um banco de dados informatizado.

Foram criados diversos modelos de dados ao longo dos anos, apesar de pretenderem se configurar como ferramentas genéricas, refletem as condicionantes tecnológicas da época de sua criação.

De acordo com Elmasri e Navathe (2011), tais modelos podem ser classificados, como: modelos de dados conceituais, os quais são os mais apropriados para capturar a semântica dos dados e, consequentemente, para modelar e especificar as suas propriedades; Modelos de dados lógicos, cuja uma representação lógica das informações em sua área, não consiste em um banco de dados, sendo independente do modelo físico e ainda, da tecnologia a ser desenvolvida e, por fim, Modelos de dados físicos, que são empregados para descrever as estruturas físicas de armazenamento, sendo uma descrição no nível de abstração visto pelo usuário do sistema. Neste caso, referido modelo depende do sistema que está sendo utilizado.

2.2.. Segurança em Banco de Dados

A segurança em banco de dados engloba a proteção dos dados contra roubo, destruição mal-intencionada, atualização não autorizada, entre outros. Assim, tratando-se do mundo empresarial, torna-se expressiva, vide que a situação de uma empresa pode ser drasticamente comprometida por qualquer vulnerabilidade na segurança de um banco de dados.

Todo sistema de segurança deve prover mecanismos que não permitam a perda ou degradação da integridade, disponibilidade e confidencialidade. A perda da integridade ocorre quando existe uma modificação não autorizada nos dados ou ainda, por atos intencionais ou acidentais. No entendimento de Elmasri e Navathe (2005) a integridade do banco diz respeito à exigência que a informação esteja assegurada de modificações impróprias, incluindo a criação, a inclusão, a alteração e a exclusão. Caso ocorra a perda da integridade dos dados e esta não seja corrigida, pode ocasionar imprecisão e tomadas de decisões equivocadas.

A disponibilidade dos dados é primordial, pois se encarrega de tornar os objetos sempre disponíveis para o usuário ou para o *software* que tenha direito de acesso a eles. Advém a perda

da disponibilidade quando os dados se tornam indisponíveis para um usuário ou programa que tenha um direito legítimo em relação a eles.

Já a confiabilidade está ligada à proteção dos dados, algo de extrema importância, uma vez que a exposição de certas informações pode ter como consequências o constrangimento dos envolvidos, a perda da confiança ou em uma ação contra a instituição. Assim, a perda da confidencialidade, por sua vez, ocorre quando há uma violação da privacidade dos dados, ocasionando uma divulgação não autorizada dos mesmos.

A fim de proteger contra essas ameaças, quatro tipos de medidas podem ser implementados, sendo elas: controle de acesso, controle de inferência, controle de fluxo e criptografia. Tais medidas serão discutidas na próxima seção.

Os pesquisadores Elmasri e Navathe (2011, p. 564) relatam que o mecanismo de segurança de um Sistema Gerenciador de Banco de Dados (SGBD) precisa compreender provisões para restringir o acesso ao sistema de banco de dados como um todo. Tal função, intitulada de controle de acesso, é tratada criando-se contas do usuário e senhas para controlar o processo de login pelo SGBD. A partir do momento que uma pessoa ou um grupo de pessoas precisa acessar um banco de dados é indispensável que se faça a requisição de uma conta de usuário.

Portanto, o Administrador de Banco de Dados (DBA) decide se há necessidade de criação de conta para essa pessoa ou esse grupo de pessoas. Conforme aduzem Ramakrishnan e Gehrke (2008, p. 590), a criptografia de dados refere-se à aplicação de "[…] um algoritmo […], usando uma chave de criptografia especificada pelo usuário ou pelo administrador do banco de dados".

Diante disso, consiste em uma das melhores soluções para se armazenar ou transferir dados com segurança. Em caso de invasão ou acesso não autorizado e estando os dados criptografados, serão encontradas dificuldades para decifrar o real significado das informações, tendo em vista que a criptografia possibilita a sua compreensão tão somente por pessoas previamente autorizadas. No entendimento de Elmasri e Navathe (2011, p. 564), somente "[…] os usuários autorizados recebem algoritmos de codificação ou decodificação (ou chaves) para decifrar os dados". Visando ter acesso aos dados originais após a criptografia dos dados é imprescindível que se aplique um algoritmo de descriptografia. Conforme Ramakrishnan e Gehrke (2008, p. 590), "sem a chave de descriptografia correta, o algoritmo de descriptografia produz lixo".

Importante mencionar que a chave para tornar as informações compreensíveis depende da estratégia de criptografia empregada, sendo possível a utilização de criptografia com chave simétrica ou pública. Levando em consideração a importância e centralidade das informações para as empresas nos dias atuais, os bancos de dados, por armazenarem dados e informações cruciais ao negócio, tem sua potencialidade para ser alvo de ataques maximizada. Dentre os variados tipos de ataque possíveis, destaca-se o abuso de privilégio e a injeção de SQL (*SQL Injection*).

O abuso de privilégio caracteriza-se pelo fato do usuário tirar proveito das permissões que lhe foram concedidas com o intuito de realizar operações as quais não está autorizado. Tal fato é exemplificado por Elmasri e Navathe (2011, p. 575) em um caso hipotético onde "[...]

um administrador que tem permissão para alterar a informação do aluno pode usar esse privilégio para atualizar notas de alunos sem a permissão do instrutor".

A metodologia de ataque denominada injeção de SQL por sua vez, pode apresentar-se de duas maneiras, quais sejam: manipulação (modificação) de uma instrução SQL já existente ou injeção de uma nova instrução SQL. A injeção de SQL funciona com a inserção de comandos SQL por meio de formulários web, comandos que podem ser de manipulação de dados, tais como: *select*, *insert*, *update* e *delete*, ou então para definição de dados, como: *create*, *drop* e *alter*. Conforme aduzem Elmasri e Navathe (2011, p. 576) "em um ataque de Injeção de SQL, o atacante injeta uma entrada de cadeia de caracteres pela aplicação, que muda ou manipula a instrução SQL para o proveito do atacante.

No que concerne à segurança de banco de dados, são imprescindíveis algumas medidas para controle de acesso e ataques. Objetivando proteger os dados contra ameaças, medidas de controle de acesso devem assegurar a inviolabilidade de alguns atributos de segurança da informação, quais sejam: integridade, disponibilidade e confidencialidade, conforme supramencionado.

A esses devem ser adicionados o próprio controle de acesso em si e ainda, a criptografia de dados. O controle de acesso é uma das medidas precípuas para manter a segurança e fica sob a responsabilidade de um Administrador de Banco de Dados. Neste contexto, tornou-se um desafio a ser superado pelas empresas, impedir que pessoas não autorizadas tenham acesso aos sistemas.

2.2.1. Controle de acesso

Em um sistema de banco de dados multiusuário, o SGBD deve ser apropriado para prover aos usuários acessos a determinadas partes e ao mesmo tempo impedir que eles acessem dados não permitidos.

Além disso, é imprescindível evitar que usuários que não sejam autorizados tenham acesso aos dados, independente se for para obter informação, ou para realizar alterações mal-intencionadas em uma parte da base de dados. A função controladora desse fato é chamada de controle de acesso que é tratada por meio da criação de contas de usuários.

A autoridade principal responsável para conceder privilégios a usuários que precisam utilizar o sistema é o DBA, e cabe ainda a ela, classificá-los, assim como classificar os dados conforme a política da organização.

A concessão e a revogação de privilégios de uma conta de usuário, realizada pelo DBA, é empregada para controlar a autorização arbitrária. A atribuição de níveis de segurança adequados a cada conta de usuário é utilizada para controlar a autorização obrigatória. Referidos conceitos serão abordados a seguir.

2.2.1.1. Controle de acesso arbitrário (discricionário)

De acordo com Elmasri e Navathe (2005), o controle de acesso arbitrário é utilizado para conferir ou revogar privilégios a usuário, até mesmo a capacidade de acessar arquivos de dados, registros ou campos específicos de uma forma específica, como leitura, inclusão, exclusão ou atualização.

Existem dois níveis para a atribuição de privilégios para a utilização do sistema de banco de dados, sendo eles:

- **Nível de conta:** em que o DBA institui os privilégios específicos que cada conta tem, independente das relações no banco de dados. Aplica-se tal metodologia à criação de esquemas ou a criação de tabelas, bem como a adicionar e remover atributos das relações e, também, criar visões e recuperar informações. Cita-se como exemplo, caso uma conta não tenha o privilégio da criação de tabelas, assim nenhuma tabela poderá ser criada por intermédio desta conta.

- **Nível de relação (ou tabela):** neste, pode-se controlar o privilégio para acessar cada relação ou visão individual. Os privilégios no nível de relação explicitam para cada usuário as relações individuais na qual cada tipo de comando pode ser empregado. Importante frisar que determinados privilégios também se referem às colunas individuais (atributos) das relações.

2.2.1.2. Controle de acesso obrigatório

Para Elmasri e Navathe (2005) estes controles são utilizados para impor a segurança em diversos níveis por meio da classificação dos dados e dos usuários em variadas classes de segurança (ou níveis) e, posteriormente, pela implementação da política de segurança apropriada da organização.

Uma extensão disso é a segurança fundamentada em papéis (*role-based*), que confere políticas e privilégios baseando-se no conceito de papéis. Tal abordagem de controle de acesso obrigatório deveria ser combinada com os mecanismos de controle de acesso discricionário para que haja uma melhor efetividade. As classes de segurança típicas são: altamente secreta (*top secret*) (AS), secreta (*secret*) (S), confidencial (*confidential*) (C) e não confidencial (*unclassified*) (NC), em que AS é o nível mais alto e NC é o mais baixo.

2.2.2. Controle de fluxo

O controle de fluxo tem a função de prevenir que as informações fluam de tal modo que cheguem aos usuários não autorizados. Neste contexto, devem ser analisados os canais que são o caminho das informações. Assim, cabe ao controle de fluxo regular a distribuição ou fluxo de informações entre objetos acessíveis.

Um fluxo entre o objeto X e o objeto Y advém quando um programa lê valores em X e escrever valores em Y. Os controles de fluxo constatam se informações contidas em alguns objetos não fluem explícita ou implicitamente para objetos de menor proteção. Desta forma, um usuário não pode obter indiretamente em Y aquilo que ele ou ela não puder obter diretamente de X.

Elmasri e Navathe (2005) aduzem que a maioria dos controles de fluxo utiliza algum conceito de classe de segurança. A transferência de informação de um remetente para um destinatário apenas é consentida se a classe de segurança do receptor for pelo menos tão privilegiada quanto à classe do remetente. A política de fluxo mais simples especifica precisamente duas classes de informação, quais sejam: confidencial (C) e não confidencial (NC), e permite todos os fluxos, excetuando-se aqueles que saem de uma classe C e seguem para uma classe NC.

2.2.3. Controle de inferência

Um dos problemas de segurança consiste em controlar o acesso a um banco de dados estatístico, o qual é empregado para prover informações estatísticas ou resumos de valores com base em diversos critérios. De modo a exemplificar, supõe-se que um órgão do governo tenha efetuado uma pesquisa junto à população para gerar algumas estatísticas. Considerando que nessa pesquisa foram levantados dados como idade, sexo, renda e outras informações, e ainda, que tais dados foram armazenados em um banco de dados estatístico. Os estatísticos do governo só devem ter acesso às informações estatísticas da população, em outras palavras, não é possível o acesso às informações confidenciais detalhadas de um indivíduo em particular.

As medidas de controle correspondentes a esse tipo são denominadas controle de inferência, sendo este empregado em banco de dados estatísticos. O SGBD, só deve permitir consultas às informações estatísticas, tais como: médias, contagens, valores máximo e mínimo e desvio padrão de uma população, não sendo permitido o acesso a uma tupla em particular, que detenha informações de um indivíduo em específico.

O controle de inferência também deve prevenir acessos mal-intencionados de usuários que tentam por meio de uma sequência de consultas inferir os valores das tuplas. A proibição de consultas repetitivas para uma mesma população de tuplas é uma técnica para que isso não venha acontecer.

2.2.4. Criptografia

A criptografia é empregada para proteger dados sigilosos, como números de cartões de crédito, que podem ser transmitidos por alguma rede de comunicação.

Pode ser empregada também para prevenir que usuários não autorizados acessem as partes confidenciais do banco de dados, codificando os dados e fazendo com que haja dificuldades para serem decifrados. Os métodos supracitados podem não ser capazes de proteger os bancos de dados contra algumas ameaças, visto que, se por exemplo, algum usuário ilegítimo de algum modo tiver acesso às informações na hora da transmissão de dados e se a mensagem não estiver sido disfarçada (encriptada) então pode ocorrer perdas irreparáveis.

Segundo Martins e Candido Junior (2014, p. 11):

> A criptografia é uma das melhores soluções para se armazenar ou transferir dados, suponha que alguma informação caia em mãos erradas, se ela estiver cifrada, ou seja, que tenha sido usado um algoritmo de criptografia, a pessoa que a obteve terá dificuldades em conseguir encontrar o significado real, pois a criptografia mascara a informação trocando os caracteres por outros, disfarçando o sentido das palavras.

Assim, um sistema de banco de dados confiável mantém seus dados criptografados para não haver acessos indevidos, isto porque cifrar uma mensagem consiste em um meio de manter os dados seguros em ambientes inseguros (ALVES, 2007).

2.3. Segurança em Banco de Dados Móveis

O avanço da tecnologia na computação móvel nos dias atuais possui um crescimento de grande escala, onde a criação de novos computadores portáteis contém uma melhor capacidade

de processamento e também a facilidade de conectividade em redes de comunicação de dados e mais velozes e confiáveis. Nota-se em que a redução das dimensões desses computadores portáteis, economia de energia, fácil manuseio, vem contribuindo para que a computação móvel venha se tornar a cada dia mais presentes em nossas vidas.

A presença da computação móvel está em poderosos *notebooks*, *smartphones*, *smart TV* entre outros. Com essa presença a demanda de acesso à informação pode ser realizada em diversas localidades independentemente da localidade onde o usuário se encontra ou vice-versa. Além dessas facilidades é preciso realizar o gerenciamento dessas informações sempre visando garantir a segurança, a integridade, a disponibilidade, confidencialidade dessas informações, bem como a rapidez na resposta a essas consultas.

De acordo com ALVES (2007, p. 14):

> Um dispositivo móvel deve possuir determinadas características. Por exemplo, deve ser portátil e o usuário ser capaz de transportá-lo com relativa facilidade. Um dispositivo móvel também tem que ser altamente utilizável, funcional e permitir fácil conectividade e comunicação com outros dispositivos. Para o usuário, quanto maior a combinação dessas características disponíveis, melhor será o dispositivo móvel.

O desejo de estar conectado ao mundo digital torna a mobilidade mais presente em nossa vida pessoal, oferecendo agilidade, maneiras eficazes nas determinadas tarefas realizadas, com essa nova tendência de acesso a informação trouxe novos problemas de segurança da informação que as pessoas e empresas precisam ter um maior cuidado em sua utilização como: cuidado na transmissão de dados em redes sem fio, acesso a informações nos dispositivos, procurar ter atenção no meio de transporte devido ter a possibilidade maior de serem roubados ou perdidos sendo algo aborrecedor e caro ao seu proprietário.

A segurança dessas informações precisa sempre ser a prioridade e estar atualizada pois novos métodos de proteção surgirão e o tratando de forma correta pode trazer grandes ganhos e satisfação.

2.4. Ferramentas e banco de dados em nuvens

Surgimento de novas tecnologias vem ocorrendo ao passar dos anos, e a *cloud computing* (Computação em Nuvem) vem cada vez tornando um diferencial no mercado. A possibilidade de acessar arquivos pessoais, empresarias, aplicativos, servidores e muitas outras ferramentas de qualquer lugar, a partir de um computador que tenha acesso a internet é de grande benefício e eficiência.

De acordo com Piçarro (2018): “Empresas brasileiras enxergaram a computação em nuvem como um fator chave para o sucesso do negócio. Gigantes mundiais já “enxergaram” que a nuvem é o futuro”.

As flexibilidades nesta tecnologia fazem com que as empresas e pessoas consigam ter segurança e privacidade de seus dados com um custo benefício que vai de acordo com sua necessidade. Além disso, manutenções nos equipamentos servidores, *backups* são incluídos no pacote da empresa contratada gerando produtividade, ganho de tempo, redução de custos.

Conforme Piçarro (2018):

> Segurança é a maior das exigências das grandes empresas. Os sistemas baseados em computação na nuvem geralmente são certificados por padrões internacionais de segurança e permitem maior controle e privacidade. Dessa forma, é necessária autorização para acessar os dados armazenados e isso reduz riscos de invasões e perdas de informações. Além disso, se os dados não estão em equipamentos físicos não existe o risco de perdê-los por meio acidental (incêndio, por exemplo).

Possuem várias ferramentas no qual oferece essa tecnologia, como exemplo temos a AWS (*Amazon Web Services*), onde é um provedor de serviços de infraestrutura para aplicações online que permite hospedar os bancos de dados com segurança, servidores, hospedagem de sites, de forma escalonada e oferece o serviço conforme o uso, ou seja, você paga apenas por aquilo que irá utilizar, dessa forma trazendo a facilidade de acompanhamento e gerenciamento através do acesso à internet.

Uma grande empresa Netflix concluiu a sua migração 100% para a nuvem utilizando as ferramentas e recursos da *Amazon Web Services* (AWS) em 2016. A mudança fez que a empresa consiga executar um grande número de servidores de várias centro de dados melhorando a escalabilidade, disponibilidade e velocidade. Redução de custos nas transmissões e servidores físicos fez com que a empresa permita fazer muitas experimentações. (Macaulay, 2018).

3. VANTAGENS DA SEGURANÇA EM BANCO DE DADOS

Um banco de dados oferece a uma organização o controle centralizado dos dados, sendo de necessidade para uma empresa e ainda representa uma grande vantagem. Dentre as diversas vantagens do controle centralizado dos dados citam-se como exemplos a redução de redundância e o compartilhamento de dados.

Neste contexto, de acordo com Matioli (2010), um banco de dados deve:

- **Garantir a integridade:** Os dados armazenados devem satisfazer certos tipos de restrições, por exemplo, o salário de um funcionário não pode ser equivalente a zero reais.

- **Garantir a restrição de acesso não autorizado:** Os usuários só podem acessar o que realmente necessitam para auxiliar em seu trabalho.

- **Garantir a recuperação e backup:** Se ocorrer a falha, o SGBD deve efetuar a restauração até um ponto anterior assegurando os dados até este ponto.

- **Garantir o controle de concorrência:** Um dado deve ser atualizado tão somente por um usuário naquele momento. Pode ocorrer de vários usuários ao utilizarem o mesmo sistema ao mesmo tempo, tentar atualizar o mesmo dado, no entanto, isso não deve ser permitido.

- **Garantir o compartilhamento de dados**: os dados devem ser compartilhados e os departamentos devem interagir entre si, formando um sistema que se comunica e interage.

Acontecimentos recentes segundo ROHR (2020):

> Especialistas em segurança estão acompanhando um novo ataque cibernético que substitui as informações armazenadas em bancos de dados pela palavra “meow” (o “miau” dos gatos, em inglês). Esses bancos de dados estavam totalmente expostos, sem qualquer senha ou proteção. Bancos de dados desprotegidos muitas das vezes vazam informações pessoais ou confidências de empresas e são considerados um risco.

Identifica-se que as vantagens de utilizar a integridade, controles de restrições de acesso, controle de concorrência, neste acontecimento poderia ajudar a evitar que os ataques nestes bancos de dados não obtenham êxito.

Além de todas as vantagens citadas, fica evidente que uma organização depende de um banco de dados, visto que todos os dados deverão ser armazenados e mantidos em segurança e objetiva facilitar as transações e agilizar as operações.

4. RESULTADOS E DISCUSSÕES

O presente artigo aborda uma visão geral sobre o conceito de banco de dados e banco de dados em dispositivos móveis, sua importância nas empresas e nas vidas das pessoas, procurando mostrar a importância da segurança do mesmo e como utilizar medidas de controle de acesso aos dados. Durante a pesquisa realizada foi possível perceber que os avanços tecnológicos fizeram com que as empresas passassem a investir na aquisição de equipamentos computacionais e armazenamentos dos dados em banco de dados digitais, e também vem contribuindo para que a computação móvel venha se tornar a cada dia mais presentes em nossas vidas.

Com esses avanços, as tentativas de acesso indevido também aumentaram na mesma proporção e a segurança dos dados é um item de grande importância e todo sistema deve prover mecanismos para que não seja permitido o acesso indevido, perda de informação ou degradação da integridade, disponibilidade e confidencialidade.

Medidas que possuem a finalidade de proteger foram abordadas neste artigo sendo elas: controle de acesso que consiste em prover acessos em determinadas informações que contém no banco de dados, controle de inferência onde procura controlar os acessos em base de dados estatístico, controle de fluxo no qual possui a função de prevenir que as informações não chegam a usuários não autorizados e a criptografia que também é muito importante em que consiste em proteger dados sigilosos como exemplo: Número de cartão de crédito, senhas, criptografando essas informações, ou seja, codificando os dados fazendo que não sejam capazes de decifrar.

A utilização conjunta de ferramentas aplicadas a uma política de segurança adequada pode propiciar controle de acesso com qualidade satisfatória para atender as principais necessidades das empresas e das pessoas no que pertence, e os acontecimentos podem ser tomados como exemplo para obter um bom controle e prevenção dos dados.

5. CONSIDERAÇÕES FINAIS

Em virtude do que foi mencionado a importância da segurança em banco de dados consiste em apresentar medidas de prevenção a informações e com o crescente avanços tecnológicos tem se notado grande melhoras no gerenciamento de segurança da informação.

As informações são a maior riqueza das empresas e pessoas, e mantê-las de forma correta e segura é primordial. Os acontecimentos de invasões estão sujeitos a serem realizados a qualquer momento, empresas e pessoas precisam estar sempre atentos a esses tipos de ataques. A importância da segurança em banco de dados está para auxiliar e também direcionar de forma correta a como estar protegido.

Manter a segurança não é um trabalho fácil de ser feito, pois requer conhecimentos, altos investimentos, dedicação. O artigo teve como objetivo geral realizar a reflexão acerca do conhecimento em segurança em banco de dados e de certa forma mostrar o quanto essa área é importante para as nossas vidas e negócios, e foi possível identificar que utilizando os métodos corretamente, mantendo os dispositivos sempre atualizados, sempre procurar através de equipes qualificadas garantir os principais conceitos de integridade das informações, disponibilidade e a confidencialidade é possível obter resultados satisfatórios e prevenir das despesas com a percas de informações.

6. REFERÊNCIAS

ALVES, R. A. **Um estudo sobre Segurança em Banco de Dados Móveis**. 2007. 74f. Trabalho de Conclusão de Curso - Universidade Federal de Pernambuco, Recife, 2007.

PIÇARRO, C. **Por que as empresas de sucesso armazenam banco de dados na nuvem?**, www.ecommercebrasil.com.br, 16 de mar. 2018. Disponível em: <https://www.ecommercebrasil.com.br/artigos/armazenar-banco-de-dados-nanuvem/> Acesso em: 13 nov. 2020.

DATE, Christopher J. **Introdução a sistemas de banco de dados**. 8. ed. Rio de Janeiro: Elsevier, 2003.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados.** 4 ed. São Paulo: Pearson Addison Wesley, 2005.
ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados**. 6. ed. São Paulo: Pearson Addison Wesley, 2011.
KORTH, H. F.; SILBERSCHATZ, A.; SUDARSHAN, S. **Sistema de banco de Dados.** São Paulo: Makron Books, 1999.

MACHADO, Felipe N. R. **Banco de Dados:** projeto e implementação. 2. ed. São Paulo: Érica, 2008.

MARTINS, F. C. CANDIDO JUNIOR, E. **Segurança em Banco de Dados:** Conceitos e Aplicações. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/4412/4172>. Acesso em: 19 jun. 2020.

MATIOLI, D. C. **Importância da segurança em banco de dados**. 2010. 55f. Trabalho de Conclusão de Curso - Fundação Educacional do Município de Assis, Assis, 2010.

MACAULAY, T. **Como a Netflix concluiu uma migração histórica para nuvem AWS**, www.computerworld.com.br, 12 de set. de 2018. Disponível em: < https://computerworld.com.br/plataformas/como-a-netflix-concluiu-uma-migracaohistoricapara-nuvem-aws/> Acesso em: 14 nov. 2020

RAMAKRISHNAN, R.; GEHRKE, J. **Sistemas de gerenciamento de banco de dados**. 3. ed. São Paulo: McGraw-Hill, 2008.

ROHR, A. **Ataque cibernético 'misterioso' está destruindo bancos de dados expostos na web**, g1.globo.com.br, 2 de nov. de 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieresrohr/post/2020/07/29/ataqueciberneticomisterioso-esta-destruindo-bancos-dedados-expostos-na-web.ghtml> Acesso em: 08 nov. 2020.