ANTONIO MARCOS BORCHERT

BANCO DE DADOS:

VULNERABILIDADE NA SEGURANÇA

Campo Grande
2019

ANTONIO MARCOS BORCHERT

BANCO DE DADOS:

VULNERABILIDADE NA SEGURANÇA

Trabalho de Conclusão de Curso apresentado à Instituição Anhanguera Uniderp, como requisito parcial para a obtenção do título de graduado em Ciência da Computação.

Orientador: Jessica Lopes

Campo Grande
2019

ANTONIO MARCOS BORCHERT

BANCO DE DADOS:

VULNERABILIDADE NA SEGURANÇA

Trabalho de Conclusão de Curso apresentado à Instituição Uniderp, como requisito parcial para a obtenção do título de graduado em Ciência da Computação.

BANCA EXAMINADORA

Prof(ª). Titulação

Prof(ª). Titulação

Prof(ª). Titulação

“Dedico este trabalho, em primeiro lugar, a Deus, porque Ele foi quem me deu força e coragem durante toda esta longa caminhada”.

E a todos os professores, que foram essenciais em minha trajetória e formação.

Somente um principiante que não sabe nada sobre ciência diria que a ciência descarta a fé, se você realmente estudar a ciência, ela certamente o levará para mais perto de Deus.

James Clerk Maxwell

BORCHERT, Antonio Marcos. **Banco de dados:** Vulnerabilidade na Segurança**.** 2019. 27 páginas. Ciência da Computação – UNIDERP, Campo Grande, 2019.

RESUMO

A presente pesquisa tem como foco abordar discutir apresentar a importância da segurança em banco de dados para as organizações uma vez que as empresas têm se tornado cada vez mais dependente desse tipo de tecnologia que tem um papel fundamental em razão do armazenamento de dados e informações fundamentais. A relevância das informações no contexto atual, pois representam uma fonte de vantagem competitiva para a organização e não deve ser mal gerida, protegidas, tornarem-se fontes de vulnerabilidades. O banco de dados representa propriedades através das quais indica a abrangência de informações e uma coleção de dados. A primeira propriedade de um banco de dados refere-se a este ser um conjunto lógico e ordenado de dados com significado. Banco de dados possui um determinado objetivo e simboliza um universo de discurso onde são consideradas as propriedades de objetos que interessam aos usuários para fins de processamento computacional. A divulgação de informações não autorizadas pode afetar a empresa de diversas formas, como levar a perda de clientes ou de mercado, ou até mesmo a ações judiciais. A segurança da informação visa proteger a informação de forma a garantir continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios. O estudo constitui-se em uma Revisão de literatura, qualitativa e descritiva que identificou os aspectos gerais, articulado com outras estratégias onde possibilitou o enriquecimento de novos conhecimentos.

Palavras-chave: Banco de Dados. Vulnerabilidade. Segurança. Informações.

BORCHERT, Antonio Marcos. **Banco de dados:** Vulnerabilidade na Segurança**.** 2019. 27 páginas. Ciência da Computação – UNIDERP, Campo Grande, 2019.

ABSTRACT

This research focuses on discussing the importance of database security for organizations as companies have become increasingly dependent on this kind of technology that plays a key role in storing critical data and information. The relevance of information in the current context, as it represents a source of competitive advantage for the organization and should not be mismanaged, poorly protected, become sources of vulnerability. The database represents properties through which it indicates the breadth of information and a data collection. The first property of a database refers to its being a logical and ordered set of meaningful data. Database has a certain purpose and symbolizes a universe of discourse where the properties of objects that interest users for computational processing purposes are considered. Disclosure of unauthorized information may affect the company in a number of ways, such as leading to loss of customers or the market, or even legal action. Information security aims to protect information to ensure business continuity, minimizing damage and maximizing return on investment and business opportunities. The study is a qualitative and descriptive literature review that identified the general aspects, articulated with other strategies where it allowed the enrichment of new knowledge.

***Key-words*:** Database. Vulnerability. Safety. Informations

LISTA DE ABREVIATURAS E SIGLAS

DBA	Database administrator
DDL	Data definition language
DML	Data manipulation language
ISO	International organization for standartization
SGBD	Sistema gerenciador de banco de dados
SO	Sistema operacional
SQL	Structure query language
VDL	View data language
C	Confidencial
NC	Não confidencial

SUMÁRIO

1 INTRODUÇÃO

Com o aumento dos números de informações contidas em vários setores diferentes do cotidiano do ser humano, seria impossível armazenar tudo no papel. Desta forma a informatização veio com o propósito de solucionar diversos problemas, principalmente nas grandes empresas, bancos, entre tantos outros estabelecimentos que utilizam o banco de dados, afim de armazenar informações. Com o crescimento das tecnologias e sistemas, as empresas investiram em computadores e descartaram os arquivos manuais, que além de ocuparem espaços físicos tornavam o serviço lento e ineficiente.

O banco de dados é um conjunto de dados ordenados e interligados para uma determinada finalidade. Considerado um departamento muito valioso para a funcionalidade e rapidez de vários serviços, desta forma torna-se imprescindível para o bom funcionamento e execução de serviços. Quando iniciou a utilização do banco de dados os *softwares* eram inferiores comparando com os da atualidade, mas desde o princípio, existe a preocupação com a segurança de informações.

O maior desafio relacionado ao banco de dados digitais é a segurança de informações, seja a ameaça lógica (*hardware*) ou externa, como operadores não autorizados, que podem fraudar “quebra de sigilo”, utilizando os dados para se beneficiar ou apenas para prejudicar a empresa. Desta forma compreende-se a importância do sigilo e da segurança dos dados tanto para a empresa, quanto para o cliente que tem informações pessoais armazenadas.

Sendo assim, é possível destacar a vulnerabilidade dos bancos de dados, pois é dele que a empresa depende para manter-se funcional e idônea, prestando um serviço de qualidade e segurança aos seus clientes. E os mesmos, terem garantias que os seus dados pessoais serão mantidos em confidência. O problema deste ´trabalho foi constatar se os bancos de dados utilizados hoje no mercado de trabalho estão preparados e bem estruturados afim de impedir ataques externos?

O objetivo geral deste trabalho foi demonstrar a vulnerabilidade dos bancos de dados utilizados atualmente. Enquanto que os objetivos específicos foram de definir o conceito de banco de dados e suas funcionalidades, demonstrar a importância da segurança de informações armazenadas em um banco de dados e descrever métodos para garantir a confidencialidade e segurança de um banco de dados.

Foi realizada uma revisão de literatura, fundamentada em pesquisas partindo de materiais disponíveis em livros, artigos, jornais e revistas cientificas.

Disponíveis na internet em sites como Scielo (Scientific Eletronic Library Online) e Google acadêmico de acesso gratuito. O material está disponível na língua portuguesa, publicados entre os anos de 1999 a 2011. Utilizando como descritores: Banco de Dados, Segurança da Informação, Vulnerabilidade.

2 BANCO DE DADOS E SUAS FUNCIONALIDADES

Durante muito tempo as pessoas trabalharam com papéis e arquivos, um serviço demorado e desgastante, retardava o funcionamento e agilidade dos locais comerciais. Conforme a demanda foi aumentando, a necessidade de um sistema diferente foi crescendo. No início dos anos 60, a revolução digital influenciou e tomou os grandes centros, descartando definitivamente o antigo sistema. Os computadores e os bancos de dados, forneceram processos mais rápidos e eficientes, facilitando o armazenamento e a busca das informações (DATE, 2004).

Banco de dados é um sistema operacional caracterizado por um conjunto de informações sobre um mesmo assunto, que se relacionam e que estejam interligadas, com o objetivo de criar um sistema de busca ágil. Facilitando e compactando dados de variáveis locais, como empresas, hospitais, escolas, entre outros (DATE, 2004).

O sistema de banco de dados foi desenvolvido para inúmeras finalidades e funcionalidades, dentre elas é registrar e armazenar informações num formato coerente, estar disponível quando solicitado, ter um compartilhamento eficiente e seguro desses dados, garantir a segurança das informações e de suas transações, a recuperação dos dados em situações de falhas operacionais (backup) e desenvolver departamentos que interagem, porém apenas para usuários autorizados (ELMASRI; NAVATHE, 2011).

Para formar um sistema de banco de dados é necessário um *hardware* (a parte física de um computador), um *software* (a parte lógica do computador), o sistema operacional que desenvolve as programações e o processamento dos dados armazenados e os usuários (SOFTWARE LIVRE, 2011).

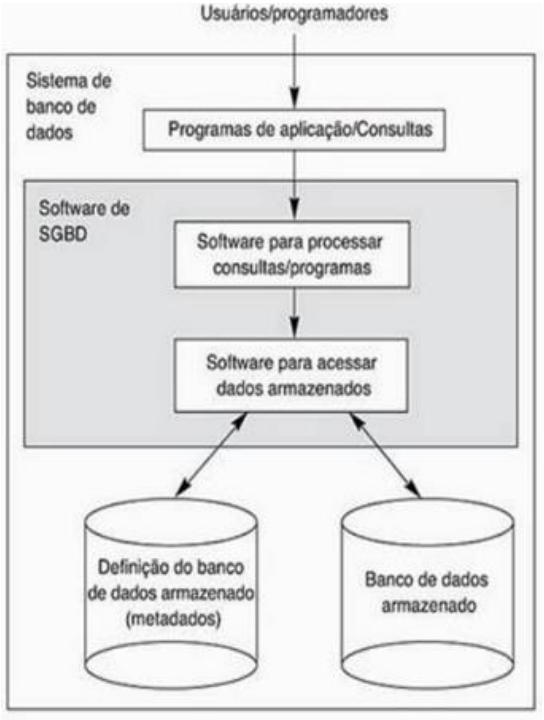
Os usuários são pessoas que tem permissões para acessar o banco de dados, podem ser aqueles que utilizam para executar funcionalidades respectivas da empresa, porém de uso restrito, eles não têm acesso em todos os dados, somente naqueles necessários para exercer sua função. Os usuários que utilizam banco de dados em terminais de autoatendimento, o programador responsável pelo desenvolvimento do banco de dados e por fim o administrador (DBA), um profissional qualificado e capacitado para a manutenção, controle e segurança do banco de dados (ELMASRI; NAVATHE, 2011).

Os usuários podem ser diferenciados em três categorias distintas, são diferenciados pela diferença na interação com o sistema de banco de dados, o programador de aplicações é o usuário que desenvolve programas, ou seja, ele é o responsável por desenvolver aplicações. O usuário final é aquele que atualiza o banco de dados, ou somente faz consultas, e o DBA o responsável por administrar o SGBD (SETZER; CORRÊA DA SILVA, 2005).

2.1 SISTEMA DE BANCO DE DADOS

Um banco de dados (FIGURA 1) tem a finalidade de armazenar várias informações, em grande quantia, facilitando a busca para os usuários, porém somente quando solicitadas. Desta forma compreende-se que um sistema de banco de dados além de armazenar as informações, ele também fornece ao usuário um controle centralizado, a redundância e o compartilhamen to dos dados armazenados. Facilitando diversas transações, agilizando várias tarefas, e o mais importante a segurança dos dados (DATE, 2004).

Figura 1. Banco de Dados



Fonte: Elmasri; Navathe (2010).

Sistema Gerenciador de Banco de Dados (SGBD) do inglês *DATA BASE MANAGEMENT SYSTEM* (DBMS) é um *software* composto por vários programas utilizado para armazenar e administrar uma coleção de dados que estão interligados, com uma programação facilitadora nas buscas e na confidencialidade. Pode ser utilizado por um único usuário ou multiusuários, acessando, adicionando e atualizando instantaneamente os mesmos dados, dependendo do critério de perfil de cada usuário configurado. Porém existe o DBA, cujo usuário é o administrador desse programa, ficando a ele particularidades para confidenciar os dados armazenados e autorizações de acesso (SOFTWARE LIVRE, 2011).

Os privilégios é considerado o fator predominante para o acesso dos dados armazenados, é desenvolvido pelo DBA, ele direciona e somente executa funções para os usuários que são permitidos. Com os privilégios formatados corretamente, o usuário só irá acessar e alterar dados autorizados, desta forma, protegendo e evitando alterações inadequadas pelos próprios usários permitidos, garantindo a segurança dos dados. Os privilégios podem ser autorizações individuais ou em grupos, isso será determinado pela DBA e a necessidade de cada local que exista um SGBD (MYSQL, 2011).

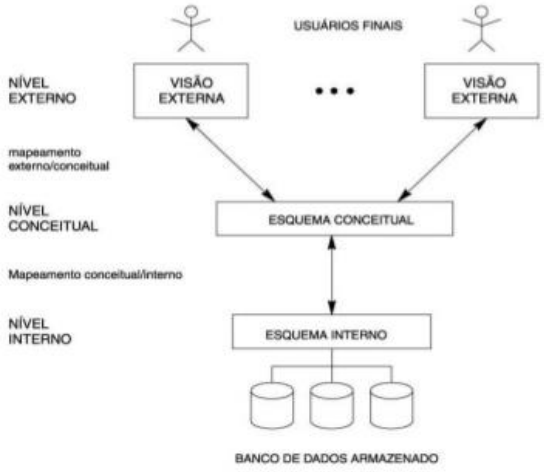
O SGBD pode ser constituído de uma interface gráfica que executam os comandos na linguagem SQL (*STRUCTURED QUERY LANGUAGE*), o sistema operacional (*SO*) é armazenado em disco, o acesso ao disco é controlado pelo SO responsável pelo escalonamento de leitura/escrita. Como características, utiliza a arquitetura cliente/servidor. De uma visão geral, *módulo cliente* rotineiramente é implementado para realizar trabalhos em uma estação pessoal. *Módulo servidor* será responsável por armazenar os dados, pelo acesso, é onde o SGDB fica alocado (MYSQL, 2011).

A arquitetura de um SGBD é a modelagem do banco de dados, aonde é possível verificar de uma forma gráfica a comunicação dos dados. Pode ser divido em alto nível, onde o usuário tem uma proximidade com a projeção dos dados armazenados e baixo nível, que está relacionado com o formato que os dados estão armazenados no computador (ELMASRI; NAVATHE, 2010).

Conforme a figura 2 pode compreender a Arquitetura de esquemas, que tem a objetividade de dividir os sistemas do usuário do banco de dados local. Neste

sentido de esquemas, a separação para o modelo acontece em três níveis: interno, conceitual, externo ou de visão. Esquema interno, está o modelo de dados e os caminhos para acesso ao banco de dados. Esquema conceitual, de um modo simplificado, possui a descrição total de um banco de dados e disponibiliza para a camada de aplicações de usuários. Esquema externo ou de visão, modelo de dados de alto nível, descreve e coleciona determinados interesses que cada aplicação/usuário precisa, ocultando outras partes do banco de dados (ELMASRI; NAVATHE, 2010).

Figura 2. Arquitetura de Três Esquemas



Fonte: Elmasri; Navathe (2010).

Linguagem de Consulta Estruturada ou SQL, é definida como a linguagem utilizada para desenvolver algumas funções no computador, como criar, altera e deletar os dados armazenados no SGBD. Existem algumas palavras chaves de linguagem como Consultas, Manipulação de Dados (responsável pela modificação dos dados armazenados na base), Controle de Transações (controlar as alterações), Definições de Dados (definir novas tabelas) e Controle de Dados (autorizações dos dados) (SETZER; CORRÊA DA SILVA, 2005).

A *DDL (DATA DEFINITION LANGUAGE)* coleção de comandos, de onde se origina a criação de bancos, tabelas, tipos e campos de dados, utilizado pelo DBA e

projetistas de banco de dados. Usado para descrever as funções tanto do esquema externo quanto o conceitual.

O DML (*DATA MANIPULATION LANGUAGE),* nesta camada é a forma como o usuário pode manipular essas informações, funções como: recuperar, inserir, modificar e excluir dados do banco.

O VDL (*VIEW DEFINITION LANGUAGE)* é o conjunto de comandos que especifica visões do usuário, mapeando seus objetivos de busca, nesta camada as instruções não modificam os dados, de uma forma simplista, apenas a busca e visualização (SILBERSCHATZ; KORTH; SUDARSHAN, 1999).

3 A IMPORTÂNCIA DA SEGURANÇA DE INFORMAÇÕES ARMAZENADAS EM UM BANCO DE DADOS

Tendo em vista que um banco de dados pode conter informações muito valiosas para a empresa ou até mesmo para as pessoas. A divulgação de informações não autorizadas pode afetar a empresa de diversas formas, como levar a perda de clientes ou de mercado, ou até mesmo a ações judiciais. A segurança da informação, segundo Alves (2006, p. 1), “[...] visa proteger a informação de forma a garantir continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios”.

Existem algumas características significativas relacionadas à segurança da informação que se aplicados de forma correta, ajudam na proteção das informações. É necessário que a empresa compreenda-os para preparar-se e fazer frente a eventuais problemas que possam ocorrer conhecer a origem, a extensão e a melhor maneira de tratar os riscos, de acordo com a situação e as possibilidades da empresa.

Sendo o primeiro destes atributos é a integridade, que tem intuito de garantir que a informação mantenha todas as características originais. A informação só é considerada integra quando não sofre nenhuma modificação – intencional ou acidental – ou quando essas modificações são autorizadas e realizadas de forma controlada (ELMASRI; NAVATHE, 2011).

O segundo atributo é a disponibilidade e objetiva garantir que as informações estejam disponíveis e acessíveis sempre que necessário. De acordo com Sêmola (2003, p. 45), “toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade”

O terceiro atributo é a confidencialidade e visa certificar que somente pessoas autorizadas terão acesso à determinada informação. A intenção é que somente o destinatário a receber a mensagem tenha acesso às informações que ela contém. Segundo Sêmola (2003, p. 45), “toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas”.

A característica do quarto atributo, a autenticidade, é *garantir* que a informação é autêntica, ou seja, verdadeira. De acordo com a Norma ISO/IEC 17799 apud Alves (2006, p. 2) refere-se a "'necessidade de verificar que uma comunicação, transação ou acesso a algum serviço é legítimo'". O quinto atributo é não-repúdio e tem como característica assegurar que uma pessoa não consiga negar a autoria de uma mensagem, informação, ato ou documento ISO/IEC 17799 (ALVES, 2006).

A segurança em banco de dados abrange a proteção dos dados contra roubo, destruição mal-intencionada, atualização não autorizada, entre outros. Portanto, torna-se significativa para a empresa, uma vez que sua situação pode ser drasticamente afetada por qualquer vulnerabilidade na segurança de um banco de dados. No que se refere a segurança de banco de dados, algumas medidas para controle de acesso e ataques aos bancos de dados são necessárias.

3.1 O CONTROLE DE ACESSO

O controle de acesso é uma das principais medidas para manter a segurança de um banco de dados e fica sob a responsabilidade de um DBA. Impedir que pessoas não autorizadas tenham acesso aos sistemas tornou-se um desafio a ser superado pelas empresas.

Elmasri e Navathe (2011, p. 564) afirmam:

> O mecanismo de segurança de um SGBD precisa incluir provisões para restringir o acesso ao sistema de banco de dados como um todo. Essa função, chamada de controle de acesso, é tratada criando-se contas do usuário e senhas para controlar o processo de login pelo SGBD.

É realizado da seguinte forma, quando uma pessoa ou um grupo de pessoas precisa acessar um banco de dados é necessário que se faça a requisição de uma conta de usuário. Sendo, o DBA decide se há necessidade de criação de conta para essa pessoa ou esse grupo de pessoas (ELMASRI; NAVATHE, 2011).

A criptografia de dados, segundo Ramakrishnan e Gehrke (2008, p. 590), refere-se à aplicação de "[…] um algoritmo […], usando uma chave de criptografia especificada pelo usuário ou pelo administrador do banco de dados".

É 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, haverá dificuldades para decifrar o real significado das informações, uma vez que a criptografia possibilita a sua compreensão apenas por pessoas previamente autorizadas. Segundo Elmasri e Navathe (2011, p. 564), apenas "[…] os usuários autorizados recebem algoritmos de codificação ou decodificação (ou chaves) para decifrar os dados".

Visto que para ter o acesso aos dados originais após a criptografia dos dados é necessário à aplicação de um algoritmo de descriptografia. De acordo com Ramakrishnan e Gehrke (2008, p. 590), "sem a chave de descriptografia correta, o algoritmo de descriptografia produz lixo". A chave para tornar as informações compreensíveis depende da estratégia de criptografia utilizada, sendo possível a utilização de criptografia com chave simétrica ou pública.

É muito importante que haja centralidade das informações para que as instituições na realidade contemporânea, os bancos de dados, por armazenarem dados e informações cruciais ao negócio, tem sua potencialidade para ser alvo de ataques maximizados.

Dentre os vários tipos de ataque possíveis, merecem destaque aqui o abuso de privilégio e a injeção de SQL (SQL Injection). O abuso de privilégio ocorre quando o usuário tira proveito das permissões que lhe foram concedidas para realizar operações as quais não está autorizado.

O artifício de ataque denominada injeção de SQL pode apresentar-se de duas formas: 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 através de formulários web, comandos que podem ser de manipulação de dados, tais como select, insert, update e delete, ou então para definição de dados, tais como create, drop e alter. Segundo o PHP Group a:

> Injeção direta de comandos SQL é uma técnica onde um atacante cria ou altera comandos SQL existentes para expor dados escondidos, ou sobrescrever dados valiosos, ou ainda executar comandos de sistema perigosos no servidor. Isso é possível se a aplicação pegar a entrada do usuário e combinar com parâmetros estáticos para montar uma consulta SQL (ELMASRI; NAVATHE, 2011, P. 575).

Quando o sujeito está com segundas intenções, pode tirar proveito de uma vulnerabilidade do código implementado no banco de dados para realizar o ataque. Para 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”. O método mais comum refere-se à manipulação de SQL, que funciona com à alteração de um comando SQL.

Sendo a alternativa certa para impossibilitar a injeção SQL, é a validação de todas as entradas. Com este pensamento ou autores relatam que “Todos os valores originados da coleta de dados externos devem ser validados e tratados a fim de impedir a execução de eventuais instruções destrutivas ou operações que não sejam as esperadas” (FILHO, CAVALCANTI e FILHO, s.d.; s.p.). Desta forma, tomando todas as medidas de precaução, dificilmente seu sistema sofrerá um ataque deste tipo.

3.1.1 Controle de Fluxo

O controle de fluxo controla o fluxo das informações entre objetos. Conforme afirmaram Elmasri e Navathe (2006, p. 538), “os controles de fluxo verificam se informações contidas em alguns objetos não fluem explicita ou implicitamente para objetos de menor proteção”.

Como sendo uma política de fluxo mais eficaz utiliza-se de duas classificações para as informações: confidencial (C) e não confidencial (NC). Esse método na maioria das situações resolve o problema, por exemplo, de quando se contém dados dos clientes, onde alguns deles são de caráter sigiloso. Segundo as técnicas de controle de fluxo devem garantir que só fluxos autorizados, explícitos e implícitos, sejam executados (HOTEK, 2010).

No passado, as empresas armazenavam as informações em arquivos físicos, o que causava grande acúmulo de papel e dificultava a organização, atualização e acesso a essas informações. Porém, com o surgimento e evolução das tecnologias computacionais, as empresas passaram a investir na aquisição de computadores e as informações passaram a ser armazenadas em bancos de dados digitais.

4 MÉTODOS PARA GARANTIR A CONFIDENCIALIDADE E SEGURANÇA DE UM BANCO DE DADOS

Conforme Peltier (2001) a segurança da informação está intimamente relacionada com as necessidades de negócio da organização. Determinar estas necessidades e identificar os riscos associados a estas, são fundamentais para manter a confidencialidade e a segurança.

Segundo o princípio de gerenciamento integrado de risco proposto por Alberts (2002), as questões de segurança devem estar incorporadas no negócio da organização e as estratégias e metas de negócio devem ser perseguidas pelas estratégias e políticas de segurança.

Como realizar o backup de dados é algo fundamental, considere o tamanho do transtorno caso uma empresa perca os seus dados, o que pode ocorrer por diversos motivos, queda de energia, vírus no servidor, falha humana, entre outros.

Uma das soluções é o uso de mídias (CD ou DVD) ou de um HD externo. podendo criar rotinas diárias ou semanais, para a cópia de arquivos do seu servidor ou computador. Existe outra bem utilizada que o uso de servidores espelhados, onde eles trabalham ao mesmo tempo. Os HDs são configurados para serem “espelhos” um do outro, ou seja, os arquivos gerados no HD principal são automaticamente gravados nos demais HDs espelhados (ELMASRI, 2006).

Outra forma de garantir a segurança das informações é criar um canal secreto que seria a permissão de uma transação de dados que infrinja as regras de segurança. Ele permite que uma informação de nível alto passe para um nível mais baixo, de maneira ilegal. Especialistas descrevem que a melhor forma de se evitar essa prática é bloquear o acesso dos programadores a informações pessoais de clientes, como salário ou saldo bancário e outras informações que expõe os dados da empresa e clientes.

Segundo Elgscreen, (2018) a criptografia de dados pode ser uma técnica ou estudo que tem como objetivo transformar uma informação em seu formato original para outra forma difícil de identificar. Ainda sobre a criptografia de dados, podemos ser entendidos como um conjunto de informações que podem passar por um processo de codificação que pode ser visto apenas a partir de agora decodificação.

4.1 CONTROLES DE PESSOAL E FÍSICO

De acordo com Atkinson (1999), com o desenvolvimento do controle gerencial no século XX, administrar e apresentar o retorno sobre o investimento é fundamental para as áreas que compõe a organização. Portanto trata-se de um direcionador importante para a área de segurança da informação.

De acordo com Elgscreen, (2018) a questão da segurança das informações em computadores praticamente é inexistente, pois é uma preocupação diária, minuto a minuto, daí a importância da prevenção de riscos, de forma que venha mitigar ao máximo as vulnerabilidades. Segurança 100% só existe se deixarmos os computadores desligados e desconectados, mas infelizmente, ele perderia sua utilidade.

É importante o funcionário conhecer seus deveres na empresa; um cuidado que o departamento de Recursos Humanos deve ter é em relação à contratação de um novo servidor, constatando os documentos e referências apresentados, propor treinamento adequado aos funcionários, deixando claras as diretrizes de segurança da empresa (VALLABHANENI, 2002).

A Norma ISO/IEC 17799 define perímetro de segurança como sendo uma coisa que constitui uma barreira, como uma parede, um portão de entrada controlado por cartão ou um balcão de recepção com atendentes. Há alguns controles que merecem cuidados especiais, tais como: identificar quem entra nas dependências da empresa, os trabalhadores da segurança também devem suas regras de trabalho, os locais de carga e descarga também merecem vigilância, para saber quem entrou e como entrou na empresa. Todos esses aspectos devem ser tratados individualmente e com muita cautela porque muitos crimes ocorrem em virtude da falta de segurança nas dependências da empresa (SÊMOLA, 2003).

Greenstein (2000) descreve que a implementação de um ambiente de controle para a instituição requer uma visão corporativa dos riscos envolvidos, sejam eles decorrentes da estratégia adotada ou dos processos existentes nas áreas operacionais e financeiras, sejam eles dos sistemas e das tecnologias aplicadas ou da regulamentação e da legislação vigentes.

Segundo Vaughan (1997), a avaliação e a revisão dos controles e dos riscos devem ser feitas por duas razões. Primeiro, o gerenciamento de riscos não é estático, ou seja, novos riscos aparecem, riscos antigos desaparecem, técnicas de controle ficam obsoletas e segundo, erros ocorrem continuamente.

Avaliar e revisar o gerenciamento dos riscos permite ao gestor revisar as decisões e corrigir os erros antes que estes se tornem onerosos. Para isto são necessários:

> Comunicação, aprendizado e aculturamento efetivos; Alinhamento contínuo entre os objetivos da instituição, gerenciamento de riscos; acompanhamento das ocorrências de sucesso e insucesso; monitoramento dos processos de gerenciamento de riscos e a revisão contínua do ambiente de controle (MCGEE, 1994, pág. 5).

Segundo Tapscott (1996), enquanto na velha economia o fluxo de informação era físico, como dinheiro, cheque, faturas, comprovantes, na nova economia digital a informação está armazenada digitalmente em computadores e fluindo na velocidade da luz através das redes.

Nakamura (2002), os benefícios trazidos pela tecnologia da informação resultam em uma maior produtividade e, consequentemente, em maiores lucros dentro da organização. A segurança da informação significa permitir que as empresas tenham mais lucros e segurança através das novas oportunidades de negócio implementadas através de soluções, utilizando-se os recursos de informática.

A segurança deve ser tratada não apenas como um mecanismo de proteção, mas sim como um elemento habilitador para que os negócios de uma empresa sejam executados.

Segundo Peltier (2002), a segurança existe para proteger os ativos contra as ameaças existentes contra estes. Identificar as ameaças contra os ativos, que necessitam ser protegidos, é o primeiro passo para a segurança destes ativos.

Define-se a ameaça como: “Prenúncio ou indício de coisa desagradável ou terrível (...)” (FERREIRA, 1999, pág. 118).

> (...) as ameaças no mundo digital espelham as ameaças no mundo físico. Se bancos físicos são roubados, então bancos digitais serão roubados, a

> segurança deve ser tratada não apenas como um mecanismo de proteção (SCHNEIR, 2002, pág. 27).

De acordo com Peltier (2001) baseados nestes elementos, as ameaças existentes à segurança da informação podem ser divididas em três grandes grupos: humana, acidental, e de desastre natural.

Ameaças de intencionais são amplamente exploradas na literatura para Mcclure (2000) e Spyman (2000) são dois exemplos de autores que exploram tecnicamente as formas de ataque à sistemas computacionais. Eles ensinam sobre ameaças intencionais e suas contramedidas, como muitos outros autores técnicos em segurança de redes.

4.1.1 Confidencialidade, Integridade e Disponibilidade

De acordo com kKutz e Vines(2001), a tríade que compõe os princípios básicos da segurança da informação são: integridade, confidencialidade e disponibilidade. Quando aplicados, esses princípios permitem adotar controles e medidas em relação a segurança da informação, reduzindo, dentre outros, os riscos de vazamento e divulgação não autorizada da informação, fraudes financeiras, apropriação indevida de informações, reputação da imagem da instituição:

A integridade: Principio que trata sobre a proteção da informação ou dos bens de informação contra a criação ou a modificação não autorizada. Perda de integridade pode estar relacionada com erro humano, ações intencionais ou contingência (VALLABHANENI, 2002).

Confidencialidade: Princípio que trata sobre a disponibilidade de informações à apenas pessoas autorizadas. Controles devem ser implementados para garantir que o acesso à informação seja sempre restrito àquelas pessoas que necessitam efetivamente tê-los (VALLABHANENI, 2002).

Disponibilidade: Princípio que trata sobre prevenir que a informação ou o recurso de informação esteja indisponível, quando requerida pelo cliente, pelo órgão regulador ou mesmo pela própria instituição. Aplica-se não só à informação, mas, também, aos canais eletrônicos, equipamentos de uma rede e outros elementos da infraestrutura tecnológica (VALLABHANENI, 2002).

Oliveira (2012) relata que o método usado para manter a consistência dos dados, impedindo a entrada de valores duplicados ou até o mesmo fazer referência a uma chave inválida para uma entidade.

Segundo Wadlow (2001), a administração da segurança, seja como função, ou seja, como responsabilidade de uma área específica dentro da instituição, é requisito fundamental dentro do processo de estabelecimento da arquitetura da segurança corporativa.

5 CONSIDERAÇÕES FINAIS

Constata-se que é fundamental que se adote um posicionamento no que se refere ao tratamento com Bancos de Dados, conferindo periodicamente seus pontos frágeis e buscando aperfeiçoamento de suas técnicas de proteção.

Os benefícios trazidos pela tecnologia da informação resultam em uma maior produtividade e consequentemente, em maiores lucros dentro da organização. A segurança da informação significa permitir que as empresas tenham mais lucros e segurança através das novas oportunidades de negócio implementadas através de soluções, utilizando-se os recursos da tecnologia. A segurança deve ser tratada não apenas como um mecanismo de proteção, mas sim como um elemento habilitador para que os negócios de uma empresa sejam executados. A segurança existe para proteger os ativos contra as ameaças existentes contra estes. Saber, identificar as ameaças contra os ativos, que necessitam ser protegidos, é o primeiro passo para a segurança destes ativos.

Sendo assim, concluiu-se ao final do presente trabalho que o problema apresentado no início deste trabalho foi respondido adequadamente, porquanto, se pode observar que a informação é um ativo de fundamental importância em qualquer organização. Por ser valiosa, é também ameaçada e deve ser protegida, a segurança da informação pode ser entendida como um conjunto de ações que assegura a conservação da confidencialidade, integridade e disponibilidade de informação. Estudos futuros como em bancos de dados de código aberto com o objetivo de entender como a comunidade trata essa tríade de segurança, se esses softwares apresentam brechas para essas ameaças, pois nem todo negócio se dispõe de softwares licenciados de bancos de dados com grande ênfase na busca por segurança, tampouco, dispõe-se de funcionários habilitados para este fim.

REFERÊNCIAS

ALBERTS, C. **Managing Information Security Risks; Addison- Wesley,** 2002; ISBN 0-321-11886-3; p.10-25; 81-11.

ALVES, Gustavo A. **Segurança da informação: uma visão inovadora da gestão**. Rio de Janeiro: Ciência Moderna, 2006.

ALVES, William P. **Banco de dados: teoria e desenvolvimento.** 1. ed. São Paulo: Érica, 2009.

ATKINSON, A. **Contabilidade Gerencial**. Atlas, 1999.

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

ELGSCREEN. W. **O que é criptografia de dados? Curso Prático de SQL** /Renata Miyagusku.São Paulo, 2018.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados.** 4 ed. São Paulo: Pearson Addison Wesley, 2006. 527p.

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

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados**. 6. ed. São Paulo: Addison Wesley, 2011.

FERREIRA, A. B. H.; **Novo Aurélio – O dicionário da Língua Portuguesa.** Nova Fronteira, 1999, 3a ed.; ISBN 85-209-1010-6; p. 1772.

FILHO, Clóvis Luiz de Amorim; CAVALCANTI, Paulo Diego de Oliveira Bezerra e FILHO, Marcello Benigno de Barros Borges, SQL **Injection em ambientes Web.** Disponível em: < http://www.devmedia.com.br/sql-injection-em-ambientesweb/9733#ixzz32CidD8Xc > acesso em: 19 de outubro de 2019.

GREENSTEIN, M.**Security, Risk Management and Control; McGraw-Hill Higher Edu**cation, 2000.

HOTEK, Mike. SQL Server 2008: **Passo a passo.** Porto Alegre: Bookman, 2010. p.287.

KRUTZ, R.; VINES, R.; **The CISSP Prep Guide: Mastering the Ten Domains of Computer Security;** Wiley Press, 2001.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G.; **Hackers Expostos. Makron Books**, 2000; ISBN 85-346-1194-7.

MCGEE, J. **Gerenciamento Estratégico da Informação**. Editora Campus, 1994. ISBN 85-7001-924-6; p. 5, 23-24.

MySQL. MySQL 5.5 **Reference Manual**. 04 de abril de 2011. MySQL. Disponível em: http://dev.mysql.com/doc/refman/5.5/en/index/.html (Acessado em 10 de Setembro de 2019, às 07h00min.).

NAKAMURA, E. **Segurança de Redes em Ambientes Cooperativos.** Berkeley Brasil, 2002; ISBN 85-7251-609-3; p. 28-29; 165-215.

OLIVEIRA, CH. SQL **Curso Prático.** São Paulo: Novatec Editora Ltda, 2012.

PELTIER, T.; **Information Security Risk Analysis**. Auerbach, 2001; ISBN 0- 8493-0880-1; p. 3-47.

PHIFER, L.. **Best practices for securing enterprise networks; Business Communications Review**, Hinsdale, Dec, 2002.
RAMAKRISHNAN, Raghu; GEHRKE, Johannes. **Sistemas de gerenciamento de banco de dados**. 3. ed. São Paulo: McGraw-Hill, 2008.

SCHNEIER, B.; **Segurança.** Campus, 2001; ISBN 85-352-0755-4; p. 22-59; 303-314
SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva.** Rio de Janeiro: Elsevier, 2003.

SETZER, Valdemar W.; SILVA, Flávio Soares Corrêa da. **Bancos de Dados:** Aprenda o que são, melhore seu conhecimento, construa os seus. São Paulo: Edgard Blücher, 2005.

SILBERSCHATZ, Abraham; KORTH, Henry F.; SUDARSHAN, S. **Sistema de banco de dados**. 3. ed. São Paulo: Makron Books, 1999.

SOFTWARE LIVRE. **Comitê técnico de implantação de software livre no Governo Federal**. Disponível em: http://www.softwarelivre.gov.br. (Acessado em em 8 de Setembro de 2019, às 13h00min.).

TAPSCOTT, D. **Geração Digital; Makron Books**, 2001. ISBN 85-346-0726- 5; p. 176.

VALLABHANENI, S.; **CISSP Textbook; SRV Professional Publications**, 2002; ISBN 0-9715216-5-4; p. 154-161; 2-14; 53-116; 169-235; 238-285; 300- 475.

VAUGHAN, E. **New Baskerville:** John Wiley & Sons. 1997; ISBN 0-471-10759; p. 3-67.