CENTRO UNIVERSITÁRIO BRASILEIRO-UNIBRA

CURSO DE GRADUAÇÃO TECNOLÓGO EM

REDES DE
COMPUTADORES

JOÃO MARCOS DE SANTANA VIEIRA

VULNERABILIDADES NA SEGURANÇA DO BANCO DE DADOS

RECIFE/2021

JOÃO MARCOS DE SANTANA VIEIRA

VULNERABILIDADES NA SEGURANÇA DO BANCO DE DADOS

Artigo apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor Orientador: Msc Ameliara Freire Santos de Miranda

RECIFE/2021

V658v Vieira, João Marcos de Santana

Vulnerabilidades na Segurança do Banco de Dados. / João Marcos de Santana Vieira - Recife: O Autor,2021.

27 p.

Orientador: Msc. Ameliara Freire Santos de Miranda

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Graduação Tecnológica em Redes de Computadores, 2021

1. Banco de Dados. 2. Segurança. 3. Falhas na Segurança da Informação. I. Centro Universitário Brasileiro - UNIBRA. Il. Título.

CDU: 004.7

JOÃO MARCOS DE SANTANA VIEIRA

VULNERABILIDADES NA SEGURANÇA DO BANCO DE DADOS

Artigo aprovado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores, pelo Centro Universitário Brasileiro – UNIBRA, por uma comissão examinadora formada pelos seguintes professores:

_____

Prof.º Msc Ameliara Freire Santos de Miranda

Professor(a) Orientador(a)

_____

Prof.º Msc Jheymesson A. Cavalcanti

Professor(a) Examinador(a)

_____

Prof.º Msc Adilson da Silva

Professor(a) Examinador(a)

Recife,____/___/____

NOTA:_____

À minha família, amigos e professores.

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus por me iluminar, sustentar e pastorear todos os dias. Agradeço a minha mãe, que sempre esteve ao meu lado me apoiando em cada momento e fase da minha vida. Também sou grato a todos os familiares e amigos que me apoiaram em diversos aspectos práticos desde o começo do curso, proporcionando que eu estudasse algo que sempre foi do meu interesse. Isso foi essencial em cada passo que percorri até aqui. Aos meus professores, obrigado por todo ensinamento e correções para meu melhor aprendizado. À todos vocês, meu mais profundo e sincero agradecimento.

“Se fosse tinta todo o mar, / E os céus infindos, os papéis, / Quais penas fosse todo hastil, / E os homens, escrivães fiéis; / Nem mesmo assim o amor seria / Descrito em todo fulgor; / Oh! deslumbrante maravilha / É esse eterno amor! / O amor de Deus, tão rico e puro, / Ninguém o pode explicar; / Jamais tem fim, é bem seguro, / Pra sempre o hei de louvar”.

(FREDERICK.M)

LISTA DE ABREVIATURAS E SIGLAS

DBA - Data Base Administrator

BD - Banco de Dados

SGBD- Sistema de Gestão de Base de Dados

IDS - Integrated Database System

IMS - Information Management System

SQL - Structured Query Language

TI - Tecnologia da Informação

LGPD- Lei Geral de Proteção de Dados Pessoais

SUS - Sistema Único de Saúde

SUMÁRIO

SEGURANÇA DE BANCO DE DADOS: ANALISE E APLICAÇÃO

João Marcos de Santana Vieira
Prof(a)Msc . Ameliara Freire Santos de Miranda

RESUMO

Por meio de pesquisa bibliográfica e a partir da análise do caso do vazamento de dados do Ministério da Saúde do Brasil em 2020, que expôs os dados de cerca de 243 milhões de brasileiros na internet, foram identificadas as possíveis causas da referida falha, uma vez que existe uma necessidade de maior segurança em relação aos dados e informações. Este trabalho apresenta conceitos referentes à garantia da segurança de uma base de banco de dados, identifica os tipos de sistema de proteção de dados mais seguros, aponta falhas mais comuns no vazamento de dados, e sugere correções ao sistema de segurança de dados.

Palavras-chave: Banco de dados; Segurança; Falhas na segurança da informação

SEGURANÇA DE BANCO DE DADOS: ANALISE E APLICAÇÃO

João Marcos de Santana Vieira
Prof(a)Msc. Ameliara Freire Santos de Miranda

ABSTRACT

Through bibliographic research and from the analysis of the case of data leakage from Brazil Department of Health in 2020, which exposed the data of about 243 million Brazilians on the internet, the possible causes of the referred failure were identified, since there is a need for greater security in relation to data and information. This final paper presents concepts related to the following: ensuring the security of a database, identifies the most secure types of data protection system, points out the most common flaws in data leakage, and suggests corrections to the data security system.

Keywords: Database; Security; Information security failures

1 INTRODUÇÃO

Registrar os principais eventos e informações relevantes que podem ser utilizados no futuro sempre foi uma necessidade humana. Ao falar de eventos ou informações reference a qualquer fato ou conhecimento do mundo real, e que pode ou não ser armazenado. A representação dessa informação é o que chamam de dados. Já um banco de dados é um agrupamento lógico e organizado desses dados, que possuem um significado definido (ALVES, 2004).

Hoje, a segurança dos bancos de dados é uma das maiores preocupações de organizações de todos os portes e segmentos. Para estas, deve ser constante a preocupação em garantir a integridade, confiabilidade e disponibilidade de suas informações, uma vez que à medida que o tempo passa é ainda mais difícil manter os dados seguros, pois como afirmou Edgar A. Poe “a habilidade humana não pode inventar código que a habilidade humana não possa decifrar”(TERADA, 2008).

Tendo como base estes conceitos, surge uma problemática de estudo com relação a como garantir a segurança de um banco de dados. Esse conceito foi abordado ao analisar o novo caso de vazamento de dados do Ministério da Saúde, que foi divulgado em dezembro, quando por falha na segurança do banco de dados do Sistema único de Saúde (SUS) as informações de mais de 240 milhões de brasileiros ficaram expostas durante seis meses (METRÓPOLES, 2021).

“Na prática, a eficácia de uma proteção depende muito do modo como ela é usada; o melhor cofre do mundo é inútil se ninguém se lembrar de fechar a sua porta”; Terada (2008).

1.1 MOTIVAÇÃO

Com o avanço exponencial da tecnologia, compreende-se a dificuldade cada vez maior de manter um banco de dados totalmente seguro, uma vez que esse avanço faz com que as formas de proteção já utilizadas se tornem obsoletas.

No entanto, hoje existem vários tipos de segurança de dados que podem oferecer uma maior garantia aos usuários a fim de prevenir que os dados sejam expostos, perdidos ou corrompidos. Diante disso, pode-se identificar a falta de conhecimento da aplicação de métodos mais seguros, bem como de capacitação dos técnicos de informática, o que pôs em risco a integridade e a autenticidade de dados dos usuários, ao utilizar uma forma inadequada de proteção de dados tais

como nome, telefone, endereço entre outros (NETSUPPORT, 2021).

1.2 PROBLEMÁTICAS

A partir do caso analisado foram identificadas algumas possíveis causas para a falha, as quais serão desenvolvidas ao longo da presente pesquisa. São elas:

- Vulnerabilidade de dados pessoais;
- Incapacitação dos funcionários de banco de dados;
- Desconhecimento da atualização na proteção de banco de dados;
- Ineficácia do sistema de proteção de dados utilizado.

1.3 OBJETIVOS GERAIS

Analisar e identificar possíveis falhas no sistema de proteção de dados, e apresentar sugestões que possam dirimir o problema em estudo.

1.3.1 Objetivos específicos

A fim de alcançar o objetivo geral, é visto os seguintes itens:

- Identificar os tipos de sistema de proteção de banco de dados mais seguros;
- Pontuar falhas mais comuns no vazamento de dados;
- Sugerir correções no sistema de segurança de banco de dados.

1.4 Organização do trabalho

Este trabalho está estruturado em cinco capítulos.

- No primeiro capítulo é apresentado a introdução, a qual descreve a relevância do assunto, bem como a análise deste. Ainda neste capítulo tem a motivação, problemática e objetivos do estudo, e a metodologia;
- No segundo capítulo está a definição de banco de dados, os principais SGBDs, algumas ferramentas de segurança, possíveis falhas, e as leis que regem a proteção dos dados;
- No terceiro capítulo há uma descrição do caso em análise;
- No quarto capítulo tem o resultado com a análise e sugestões;

- Por fim, no quinto capítulo a conclusão.

1.5 METODOLOGIA

A análise deste trabalho foi la utilizando as seguintes técnicas: pesquisa bibliográfica e estudo de caso. A pesquisa bibliográfica apresentada aqui relata os conceitos relacionados à segurança de bancos de dados, à lei que protege a informação de toda pessoa e, além disso, algumas sugestões de correção com relação à falha mencionada. Essas pesquisas foram feitas atravez de livros e sites desde que é banco de dados até tipos de segurança de dados, para uma melhor analise sobre o assunto. A presente análise é baseada no estudo de caso sobre o vazamento de dados do site do Ministério da Saúde do Brasil de dezembro de 2020, o qual é de conhecimento público, uma vez que foi divulgado por meios de comunicação. Aqui foram ultilizados varios sites de noticias onde estavam sendo divulgado as informações sobre o vazamento; usando varias fontes de informações, para que fosse colocado algo mais concreto e de uma formar mais clara a respeito do caso citado.

2 REFERENCIAL TEÓRICO

Neste capítulo está localizado a fundamentação teórica que envolve o campo de estudo da segurança dos bancos de dados, bem como suas possíveis falhas e consequências.

2.1 DEFINIÇÃO DE BANCO DE DADOS

Um banco de dados é um conjunto organizado de informações conectadas com a necessidade do mundo real. Essa estrutura regular de dados relacionam informações específicas de forma que criem sentido para quem a necessita. Hoje essa é a peça principal dos sistemas de informação (REGILAN, 2013).

Essa noção de banco de dados começou a ser desenvolvida em 1960 por Charles W. Bachman, significando uma coleção de informações organizadas de maneira que pudessem ser acessadas e recuperadas por meio de um sistema gerenciador de banco de dados (SGBD), (DEVMEDIA, 2021).

> O modelo desenvolvido por Bachman foi chamado de Integrated Database System (IDS) e utilizava o modelo de rede. Sem querer ficar para trás, na mesma época a IBM também começou a trabalhar no Information Management System (IMS), que se baseava em seu próprio modelo de banco de dados hierárquico. Pereira (2019).

Esse armazenamento de informações permite que os dados sejam compartilhados entre as diversas áreas de uma empresa, fazendo com que um determinado departamento possa receber um pedido e, a partir de um sistema integrado, poderá compartilhar essa informação em uma base de dados, e a solicitação pode ser enviada ao departamento responsável pela execução do pedido.

Em seu livro “Introdução a Bancos de Dados”, Pereira (2019) afirmou que prezar pela segurança dos dados é um dos motivos para se optar por um banco de dados, não somente para prevenir ataques cibernéticos, mas também pela possibilidade de se fazer backup e recuperação em caso de falhas ou perdas de dados de outra natureza.

2.2 PRINCIPAIS SGBDs

Os principais SGBDs do mercado são:

- Oracle

Esse é um dos tipos de banco de dados mais utilizados no mercado. A principal

característica do Oracle é a multiplicidade de suas funcionalidades. Ele pode ser instalado em diversos sistemas de operação e aumenta sua capacidade à medida que a demanda cresce (SÊMOLA, 2021).

- SQL Server

Esse Sistema Gerenciador de Banco de Dados (SGDB) foi desenvolvido pela Microsoft no final da década de 80, e utiliza-se do padrão de linguagem de pesquisa declarativa SQL para a administração dos dados. É comumente usado em meios corporativos e governamentais por trabalhar com informações criptografadas o garante uma maior segurança (SÊMOLA, 2021).

- MySQL

Trabalha de forma open source, ou seja, com o código aberto para a modificação de programadores. Atualmente é um dos bancos de dados mais populares, com mais de 10 milhões de instalações pelo mundo (SÊMOLA, 2021).

- PostgreSQL

É um gerenciador de banco de dados que otimiza muito o trabalho de quem precisa administrar informações, não á duvidas que banco de dados fazem parte de quem trabalha com criação, gerenciamento de site; e por meio dessa ferramenta facilita muito nos serviços, pois torna-se funcional e descomplica o trabalho na hora de sua ultilização (SOUZA, 2020).

2.3 SEGURANÇA DE BANCO DE DADOS

A segurança do banco de dados consiste em todas as ações tomadas, preventivas e reativas, para garantir a integridade, a disponibilidade e a confidencialidade dos dados. Manter os dados seguros é protegê-los contra roubos, modificações não autorizadas e acessos maliciosos de terceiros.

Com a rápida evolução da tecnologia, os sistemas de segurança se tornam rapidamente ultrapassados. Isso faz com que a garantia integral da segurança em banco de dados seja uma tarefa quase impossível. O que as empresas podem, e devem, fazer é retardar esse processo, o que com algumas medidas simples pode evitar que seu banco de dados seja prejudicado (TERADA, 2008).

A segurança de banco de dados se torna cada vez mais indispensável às empresas uma vez que sua situação pode ser afetada drasticamente por qualquer

vulnerabilidade na segurança destes.

Medidas de controle de acesso devem ser tomadas para proteger o banco de dados ao garantir a inviolabilidade de alguns atributos de segurança da informação citados anteriormente. Isso inclui o próprio controle de acesso em si, que é uma das principais medidas, e a criptografia de dados (NETSUPPORT,2021).

Hoje um dos desafios a serem superados pelas empresas é impedir que pessoas não autorizadas tenham acesso aos sistemas. Elmasri e Navathe (2011) afirmam que:

> 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.

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. Logo, o DBA decide se há necessidade de criação de conta para essa pessoa ou um grupo de pessoas (NAVATHE; ELMASRI, 2011).

2.3.1 CONTROLE DE ACESSO

Este mecanismo impõe regras de restrição por meio das contas dos usuários, sendo o administrador de banco de dados (DBA) o responsável por definir essas regras. Além disso, é ele quem pode conceder ou remover privilégios, criar ou excluir usuários, e atribuir um nível de segurança aos usuários do sistema, tendo em consideração a política da empresa (MACÊDO, 2021).

2.3.2 CONTROLE DE FLUXO

O controle de fluxo faz com que as informações sejam conduzidas por canais secretos, violando a política de segurança, e alcancem usuários não autorizados. Esta ferramenta tem a finalidade de verificar se as informações contidas em alguns objetos estão fluindo para objetos de menor proteção, seja implícita ou explicitamente (MACÊDO, 2021).

2.3.3 CRIPTOGRAFIA

Essa é uma medida de controle final utilizada para proteger dados sigilosos

que são transmitidos por meio de algum tipo de rede de comunicação. Pode-se dizer que este método é basicamente um conjunto de técnicas que transformam dados em códigos, os quais só podem ser decifrados por quem tenha a chave de acesso. Isso seria como um disfarce da mensagem para que, mesmo que haja algum desvio na transmissão, a mensagem não seja revelada (WYKES,2016).

Com esse método, os dados são codificados por meio de algum algoritmo de codificação, oferecendo, assim, uma proteção adicional às partes confidenciais de um banco de dados. Desta forma, aqueles que não possuem a chave secreta da criptografia não poderão acessar as informações codificadas (MACÊDO, 2021).

2.3.4 USUÁRIOS

Nesse método, cada banco de dados Oracle tem uma lista de nomes de usuários. E cada nome tem uma senha que lhe corresponde, evitando que pessoas sem autorização o utilizem. Neste caso, para acessar um banco de dados, o usuário deve usar um aplicativo desse tipo e tentar se conectar com um nome de usuário válido (MACÊDO, 2021).

2.3.5 DOMÍNIO DE SEGURANÇA

O domínio de segurança é um conjunto de contas de usuários e grupos no domínio informática, ou seja, um conjunto de propriedades que determinam coisas como ações disponíveis para o usuário, cota de espaço disponível em disco e limites de recursos de sistema do usuário (MACÊDO, 2021).

2.4 POSSÍVEIS FALHAS NO BANCO DE DADOS

Pessoas físicas e empresas de grande, médio ou pequeno porte estão suscetíveis a tornar-se alvos de ataques virtuais. As maiores e mais comuns falhas neste âmbito podem surgir desde problemas comuns, como a falta de um simples backup de arquivos a problemas mais complexos. Tais falhas podem ser resumidas nos seguintes itens: (1) falta de regras gerais; (2) pouca informação para os colaboradores; (3) pouca importância dada à segurança em TI; (4) evolução dos malwares e (5) falha na gestão (TELECOM, 2021).

Caracteriza-se como falta de regras gerais quando a empresa não possui um conjunto de regras para auxiliar os usuários a utilizarem as ferramentas e sistemas disponibilizados pela empresa de forma correta e segura. Tal comportamento faz

com que a empresa corra sérios riscos de vazamento de informações (TELECOM, 2021).

O segundo possível fator de falha está relacionado ao nível de informação dos colaboradores. Embora algumas empresas possuam um conjunto de regras de TI bem estabelecido, em muitos casos, nem todos os funcionários possuem suficiente familiaridade com a tecnologia. Sendo assim, são mais suscetíveis a ataques de hackers. Um exemplo recorrente são os ataques por meio de links reduzidos, como “migre.me”, “goo.gl”, “bit.ly”, etc (TELECOM, 2021).

O investimento em segurança de dados deve assumir considerável importância em empresas e órgãos públicos. O caso de vazamento de dados do Ministério da Saúde do Brasil em 2020 comprova isso. Muitas vezes o investimento em serviços de segurança em TI sai mais barato do que as possíveis perdas com ataques e vírus (TELECOM, 2021).

À medida que a tecnologia avança, os cibercriminosos[1] se aperfeiçoam, criando malwares cada vez melhores. Por isso é importante que as empresas possuam uma gestão adequada, de modo a configurar corretamente os ambientes para que não exista brecha onde os hackers possam atacar. É de crucial importância que os profissionais saibam como agir em situações problemáticas e saibam como eliminar possíveis ameaças (TELECOM, 2021).

2.5 LEIS QUE REGEM A SEGURANÇA DE DADOS

A Lei Geral de Proteção de Dados Pessoais é uma legislação que tem o objetivo de proteger a liberdade e a privacidade de consumidores e cidadãos. Criada em 2018 e prevista para entrar em vigor em maio de 2021, ela demanda que empresas e órgão públicos mudem a forma de coletar, armazenare usar os dados das pessoas. Ou seja, terá impactos significativo nas áreas judídica, administrativa e de segurança da informação das companhias. Baseando-se na Europa tem o General Data Protection Regulation que é o regulamento geral de proteção de dados europeu, é a lei que hoje em dia vale para todos os países europeus, devendo ter harmônica e conjunta com a legislação própria de cada país membro; essa lei por sua vez e aplicada a toda União Europeia (CAPEZ, 2021).

A segurança em banco de dados é legalmente garantida por meio da Lei nº 13.709/2018, a famigerada Lei Geral de Proteção de Dados (LGPD), sancionada pelo presidente Michel Temer em 14 de agosto de 2018 (BRASIL, 2018).

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018, Art. 1º).

A disciplina da proteção de dados pessoais tem como fundamentos:

I. O respeito à privacidade;

II. A autodeterminação informativa;

III. A liberdade de expressão, de informação, de comunicação e de opinião;

IV. A inviolabilidade da intimidade, da honra e da imagem;

V. O desenvolvimento econômico e tecnológico e a inovação (BRASIL, 2018, Art. 2º).

[1] Ciber + criminoso; relativo a cibercrime ou a crime cometido através da comunicação entre redes de computadores, nomeadamente através da Internet (DICIONARIO, 2021).

3 ESTUDO DE CASO

Neste trabalho será analisado o caso de vazamento de dados do Ministério da Saúde que expôs os dados pessoais de 243 milhões de brasileiros, o qual foi divulgado primeiramente pelo jornal Estadão no final de 2020. Essa falha de vazamento de dados foi a mais recente e mais grave do órgão, pela quantidade de pessoas afetadas (ECONOMIA, 2021).

Dados pessoais como nome completo, endereço, telefone e CPF ficaram vulneráveis durante seis meses, incluindo dados até mesmo de autoridades como o próprio presidente da República, Jair Bolsonaro, o presidente da Câmara, Rodrigo Maia, e o senador Davi Alcolumbre. O mais curioso é que o número do registro supera o próprio número de habitantes do Brasil, que atualmente está estimado em 210 milhões, isso porque os dados expostos contêm, inclusive, informações de pessoas já falecidas (RIENTE, 2021).

A falha resultou da exposição indevida de logins e senhas de acesso ao sistema, que armazena dados cadastrais de todos os brasileiros no Ministério da Saúde. Esses dados de acesso estavam em um trecho do código do site, que fica aberto para visualização de qualquer usuário por meio da simples função “Inspecionar, elemento”, disponível em qualquer navegador, que pode ser facilmenBRIe decodificado com a ajuda de uma simples ferramenta online (CAMBRICOLI, 2021).

O código utilizado, chamado de Base 64, é um método de codificação de dados, e não de segurança, ou seja, essa não é uma forma de criptografar informações. Ele é utilizado frequentemente para transferência de dados na internet, lidando apenas com textos, como, por exemplo, um email (RIENTE, 2021).

O Ministério da Saúde pode ser responsabilizado por dano individual ou coletivo, sendo condenado a pagar indenização, independente de quem tenha cometido o erro. A fundadora e diretora da Organização Coding Rights, Joana Varon, afirmou que “pela lei geral de proteção de dados quem é controlador de base de dados tem responsabilidades inclusive no que diz respeito à segurança dessas bases. Deixar que qualquer um tenha acesso a senhas de acesso à base de dados é um erro de segurança básica”. O Governo Federal afirmou que investigaria o caso (METRÓPOLES, 2021).

De acordo com o ministério da saúde, a falha reportada está sendo investigada para apurar a responsabilidade da exposição da base cadastral da pasta. Quanto ao problema identificado, este foi corrigido após a publicação da reportagem do Estadão. O órgão federal ainda garantiu que possui protocolos de segurança e proteção de dados, os quais são avaliados e aprimorados com frequência. No entanto, não explicou o motivo de não ter havido revisão do código fonte do site em junho, quando a primeira denúncia do problema foi realizada (METRÓPOLES, 2021).

4 RESULTADOS

Por meio do estudo de caso apresentado, foi analisado a notável falha na segurança do banco de dados do Ministério da Saúde, ao utilizar um código de escrita que não é específico para segurança e proteção de dados, e sim, apenas para codificar mensagens de texto como email, onde não se requer tanta segurança como quando se trata de banco de dados de armazenamento de dados pessoais dos usuários (METROPOLES, 2021).

Estes, por sua vez, exigem uma segurança rígida, como é visto na Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei 13. 709, de 14 de agosto de 2018, que diz que quem é controlador da base de dados tem responsabilidades inclusive no que diz respeito à segurança dessas bases. Deixar que qualquer pessoa obtenha senhas de acesso a bases de dados é um erro básico de segurança (RIENTE, 2021).

Por meio desta análise notar-se que não foram usados os tipos de segurança de dados disponiveis hoje em dia no mercado, estas não foram utilizadas corretamente, fazendo com que os dados pessoais de um sistema gigante ficassem vulneráveis e expostos a qualquer pessoa que tivesse um conhecimento básico de desenvolvimento de sites (CAMBRICOLI, 2021).

Como sugestão para evitar novas falhas da mesma natureza, além da capacitação aos profissionais que atuam no banco de dados, o órgão pode fazer uso da criptografia, por ser uma forma de segurança mais adequada para proteção e confidencialidade de informação, assim tornando os dados mais seguros, pois impede o acesso às informações por aqueles que não possuem a chave da criptografia (TELECOM, 2021).

5 CONCLUSÃO

A segurança de banco de dados hoje é primordial para as empresas, instituições e para os usuários, pois ali contém informações importantes para que uma empresa se destaque das demais, sendo útil para a melhoria e aprimoramento de quem a utiliza (NAVATHE; ELMASRI, 2011).

Na análise do caso, reconhecido publicamente, é visto que por uma falha no código fonte do site, o banco de dados do Ministério da Saúde se tornou vulnerável, deixando milhares de dados pessoais e s (RIENTE, 2021).

Nota-se que no site do Ministério da Saúde foi utilizado no seu código fonte algo inapropriado para segurança do banco de dados, o que o tornou acessível para terceiros, fazendo com que a segurança do banco de dados perdesse sua essência, que é proteger os arquivos contidos nele. Além da falha da escrita do código fonte, os dados também que ficaram expostos por cerca de seis meses (METRÓPOLES, 2021).

Sendo assim, é possivel ver a necessidade de uma capacitação adequada para os responsáveis pela segurança do banco de dados e os técnicos envolvidos. Pois como foi falado, a tecnologia está avançando muito rapido então os tecnicos tem que avançar juntos, para que haja um melhor conhecimento e assim ultilizar para uma melhor segurança e uma certa garantia, para que os dados não fiquem expostos, corrompidos ou perdidos. Também seria necessária a utilização de uma criptografia; que funciona como um cadeado e uma chave, pois o cadeado só abre com a sua chave em especifico, quando cada pino do cadeado esta nos lugares corretos, sendo assim, pessoas sem a devida autorização não teriam acesso às informações. Apenas possoas que contem a chave de acesso (pessoas autorizadas).

6 REFERÊNCIAS

ALVES, William Pereira. **Fundamentos de Bancos de Dados**. São Paulo: Erica, 2004.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD) 2018**. Disponível,em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 maio 2021.

CAMBRICOLI, Fabiana. **Nova falha d stério da saúde expõe dados pessoais de mais de 200 mi de brasileiros**. Disponível em: https://www.terra.com.br/vida-e-estilo/saude/nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes-de-brasileiros,b5ba3db11cebba15ad1717233d7ed2616dllihs9.html. Acesso em: 20 abr. 2021.

CAPEZ, Fernando. **Lei Geral de Proteção de Dados Pessoais: origem histórica**. Disponível em: https://economia.ig.com.br/colunas/defesa-do-consumidor/2020-06-01/lei-geral-de-protecao-de-dados-origem-historica.html. Acesso em: 15 jun. 2021.

DEVMEDIA. **A História dos Banco de Dados**. Disponível em: https://www.devmedia.com.br/a-historia-dos-banco-de-dados/1678. Acesso em: 24 abr. 2021.

DICIONÁRIO, Priberam. **Https://dicionario.priberam.org/cibercriminoso**. Disponível em: https://dicionario.priberam.org/cibercriminoso. Acesso em: 10 maio 2021.

ECONOMIA, G1. **Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal**. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 19 abr. 2021.

MACÊDO, Diego. **Conceitos sobre Segurança em Banco de Dados**. 2011. Disponível,em: https://www.diegomacedo.com.br/conceitos-sobre-seguranca-em-banco-de-dados/. Acesso em: 24 abr. 2021.

METRÓPOLES. **Nova falha da Saúde expõe dados de mais de 200 milhões de brasileiros**. Disponível em: https://www.metropoles.com/brasil/nova-falha-da-saude-expoe-dados-de-mais-de-2 00-milhoes-de-brasileiros. Acesso em: 15 abr. 2021.

NETSUPPORT. **Segurança de Banco de Dados: com o que se preocupar**. Disponível em: https://netsupport.com.br/blog/seguranca-em-banco-de-dados/. Acesso em: 27 abr. 2021.

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

PEREIRA, Paloma Cristina. **Introdução a Banco de Dados**. São Paulo: Senac, 2019.

REGILAN, Meira Silva. **Banco de Dados**. 2013. Disponível em: http://regilan.com.br/wp-content/uploads/2013/10/Apostila-Banco-de-Dados.pdf. Acesso em: 28 abr. 2021.

RIENTE, Leticia. **Novo vazamento de dados do Ministério da Saúde expõe 200 milhões de brasileiros**.. Disponível em: https://olhardigital.com.br/2020/12/02/noticias/novo-vazamento-de-dados-do-minis terio-da-saude-expoe-200-milhoes-de-brasileiros/. Acesso em: 18 abr. 2021.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. 2003. Disponível em: https://br.godaddy.com/blog/quais-os-principais-tipos-de-banco-de-dados. Acesso em: 30 abr. 2021.

SOUZA, Ivan de. **PostgreSQL: saiba o que é, para que serve e como instalar**. 2020. Disponível em: https://rockcontent.com/br/blog/postgresql/#:~:text=O%20PostgreSQL%20%C3%A9%20uma%20ferramenta%20que%20atua%20como,os%20padr%C3%B5es%20desse%20tipo%20de%20ordena%C3%A7%C3%A3o%20dos%20dados.. Acesso em: 27 abr. 2021.

TELECOM, Algar. **Quais são as maiores falhas na segurança de dados?** 2015. Disponível em: https://blog.algartelecom.com.br/gestao/quais-sao-as-maiores-falhas-na-seguranca- de-dados/. Acesso em: 03 abr. 2021.

TERADA, Routo. **Segurança de dados: Criptografia em rede de computador.** 2. ed. São Paulo: Edgard Blucher, 2008.

WYKES, Sean Michael. **Criptografia Essencial: a Jornada do Criptógrafo.** Rio de Janeiro: Elsevier Editora Ltda, 2016.