CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA

CURSO DE GRADUAÇÃO TECNÓLOGO EM REDES DE COMPUTADORES

CHRYSLAYNY THAYS DOS SANTOS SILVA

CLEYTON FAUSTO ALVES JÚNIOR

MARCOS ALEXANDRE MELO ALVES SANTANA

SEGURANÇA DE REDES NOS BANCOS DE DADOS

RECIFE/2022

CHRYSLAYNY THAYS DOS SANTOS SILVA
CLEYTON FAUSTO ALVES JÚNIOR
MARCOS ALEXANDRE MELO ALVES SANTANA

SEGURANÇA DE REDES NOS BANCOS DE DADOS

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

Professor(a) Orientador(a): Valfrido Furtado Leite Filho

Professor(a) Co Orientador(a): Ameliara Freire Santos de Miranda

RECIFE/2022

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 1745.

S586s Silva, Chryslayny Thays Dos Santos
Segurança de redes nos bancos de dados / Chryslayny Thays Dos Santos Silva, Cleyton Fausto Alves Júnior, Marcos Alexandre Melo Alves Santana. Recife: O Autor, 2022.
34 p.

Orientador(a): Valfrido Furtado Leite Filho.
Coorientador(a): Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2022.

Inclui Referências.

1. Dados. 2. Bancos. 3. Segurança. 4. Empresas. 5. Disponibilidade. I. Alves Júnior, Cleyton Fausto. II. Santana, Marcos Alexandre Melo Alves. III. Centro Universitário Brasileiro - UNIBRA. IV. Título.

CDU: 004

DEDICATÓRIA

Dedico este trabalho aos meus pais, Cleyton e Anne.
(Cleyton Fausto)

Dedico este trabalho aos meus pais, Christina e Reginaldo,
e aos meus irmãos, Alyson e Eduarda.
(Chryslayny Thays)

Dedico este trabalho aos meus pais, Geanne e Paulo, e minha
tia Maria, e minha irmãs Kawany e Carla
(Marcos Melo)

AGRADECIMENTOS

Agradeço principalmente aquele que fez e faz, Deus, que em vários momentos me deu força para alcançar meus objetivos, fé sempre foi alimente pra enfrentar as dificuldades e solidão durante algumas madrugadas de estudo. Aos meus pais e irmãos, que me incentivaram nos momentos difíceis, que me mostraram que eu deveria enfrentar a vida com sabedoria, obrigado a esses guerreiros que compreenderam a minha ausência enquanto eu me dedicava à realização deste sonho. Aos mestres, professores que sempre ouvi, obrigado por todos os conselhos, ajuda e pela paciência, vocês me conduziram, me ensinaram que eu podia mais. (Marcos)

Gostaria de agradecer primeiramente a Deus, por toda a força e coragem que tem me dado durante o curso

Agradeço aos meus pais, Christina e Reginaldo por todo apoio que me deram

Agradeço aos meus irmãos, Eduarda e Alyson, por todo amor, apoio e força durante esses dois anos e meio

Agradeço também aos meus amigos, Thalia, Lavínia, Karolayne e Elton por toda força dada e por toda cumplicidade

Agradeço à minha coorientadora Ameliara, por toda a jornada e dedicação.

Por fim, agradeço a todas as pessoas que me ajudaram diretamente e indiretamente, meu muito obrigada. (Chryslayny)

Agradeço primeiramente à Deus, que me deu o dom da vida e me abençoa todos os dias com o seu amor infinito.

Sou grato aos meus pais Cleyton e Anne, que me apoiaram muito com palavras de incentivo. (Cleyton)

“Ninguém ignora tudo. Ninguém sabe tudo. Todos nós sabemos alguma coisa. Todos nós ignoramos alguma coisa. Por isso aprendemos sempre.”

(Paulo Freire)

Sumário

SEGURANÇA DE REDES NOS BANCOS DE DADOS

Chryslayny Thays dos Santos Silva

Cleyton Fausto Alves Junior

Marcos Alexandre Melo Alves Santana

Professor (a) Orientador (a): Valfrido Furtado Leite Filho

Professor (a) Co- Orientador (a): Ameliara Freire Santos de Miranda

Resumo:

Os bancos de dados são importantes porque toda a informação é armazenada neles e é importante entender sua segurança, pois por falta de segurança, os bancos de dados de pequenas e médias empresas são frequentemente atacados. Hoje, para as empresas, um sistema de gerenciamento de banco de dados eficaz é fundamental para suas operações, pois suas informações são organizadas e armazenadas em seus bancos de dados. Muitas pessoas utilizam redes sociais como Instagram e WhatsApp, em cada uma dessas redes sociais existe uma forma de proteger os dados de seus respectivos usuários, por exemplo no WhatsApp temos criptografia de ponta a ponta, além da disponibilidade de fator de autenticação. A segurança no Instagram não é completa quando se trata da disponibilidade de fatores de autenticação porque a criptografia não é de ponta a ponta, mas também fornece autenticação de dois fatores. Lidamos com vazamentos de big data e ataques a sistemas de segurança. Nosso objetivo é apontar a importância dos bancos de dados, mostrar seus usos e identificar diversos bancos de dados. Vamos falar sobre ransomware, malware de ataque de dados orientado por senha que assume os arquivos pessoais da vítima e

cobra por eles. Os bancos de dados são essenciais para as empresas porque centralizam grandes quantidades de informações e aplicativos e devem operar com segurança adequada, desempenho eficiente e alta disponibilidade. O papel de um especialista em TI é essencial para garantir a inovação e a transformação digital de uma empresa. Um bom profissional nesta área também deve ter conhecimento de organização, gestão e estratégia. Eles trabalham para reduzir o risco de incidentes que podem afetar a disponibilidade, integridade e confidencialidade das informações. Sem ele, as empresas não dispõem dos recursos técnicos necessários para se manterem competitivas em um mercado cada vez mais competitivo.

Palavras-Chaves: Dados. Bancos. Segurança. Empresas. Disponibilidade.

Abstract

Databases are important because all the information is stored in them and it is important to understand their security, because due to lack of security, databases of small and medium-sized companies are often attacked. Today, for companies, an effective database management system is critical to their operations as their information is organized and stored in their databases. Many people use social networks such as Instagram and WhatsApp, in each of these social networks there is a way to protect the data of their respective users, for example in WhatsApp we have end-to-end encryption, in addition to the availability of an authentication factor. Security on Instagram is not complete when it comes to the availability of authentication factors because the encryption is not end-to-end, but it also provides two-factor authentication. We handle big data leaks and security system attacks. Our goal is to point out the importance of databases, show their uses and identify different databases. Let's talk about ransomware, password-driven data attack malware that takes over victim's personal files and charges for them. Databases are essential for businesses because they centralize vast amounts of information and applications and must operate with adequate security, efficient performance, and high availability. The role of an IT specialist is essential to ensure a company's innovation and digital transformation. A good professional in this area should also have knowledge of organization, management and strategy. They work to reduce the risk of incidents that could affect the availability, integrity and confidentiality of information. Without it, companies do not have the necessary technical resources to remain competitive in an increasingly competitive market.

Keywords: Data. banks. Safety. Companies. Availability.

1. INTRODUÇÃO

A importância da segurança dos dados é enorme, mas nem sempre foi assim. No começo dos bancos de dados, as soluções de segurança para dados confidenciais limitavam-se a salas trancadas contendo os sistemas de computador que os abrigavam e os programas. A crescente exposição desses sistemas ao público levou ao desenvolvimento de hardware e software para fornecer proteção ao acesso, transmissão e manipulação de dados. (BOROVINA; MONTEIRO, 2013)

A segurança dos bancos de dados significa manter as informações confidenciais seguras e evitar a perda de dados. A segurança do banco de dados é controlada pelo administrador do banco de dados (DBA). (LIMA, ACERVO, 2022)

Os administradores de bancos de dados, também conhecidos como DBAs, garantem que as empresas possam encontrar facilmente as informações de que precisam no banco de dados e que tudo esteja funcionando corretamente. Inicialmente, os administradores se reúnem com a equipe de gestão para entender quais dados a empresa precisa para definir os objetivos de seu banco de dados. Os DBAs também são responsáveis por implementar medidas de segurança para impedir o acesso não autorizado ao banco de dados. Isso é importante porque os bancos de dados geralmente contêm informações pessoais e/ou financeiras confidenciais. (MENDES, 2020)

O Banco de Dados SQL impõe mecanismos para permitir ou não o acesso aos dados com base nas funções fornecidas pelo administrador. Porém, o comando GRANT permite permissões específicas em Objetos. (Bancos de Dados, Tabelas, Sequências, etc.) Não possui restrições de pessoas, podendo ser uma ou mais, e também permite um grupo de usuários. Os administradores de banco de dados e de rede do sistema operacional têm se preocupado muito em criar e manter um ambiente mais seguro. (MACÊDO,2012)

O Microsoft Azure criou um serviço de banco de dados relacional para manter os dados de seus clientes protegidos, aumentando a segurança que eles esperam dos bancos de dados relacionais. O SQL tem seu próprio conjunto de recursos de segurança criados com base nos controles herdados do Azure. A Base de Dados Azure SQL suporta apenas ao protocolo de fluxo de dados tabulares (TDS), exigindo assim que a base de dados seja acessível apenas através do porta padrão TCP/1433. (LANFEAR, 2022*)*

Além disso, garantir a segurança geral do banco de dados contra acesso não autorizado é uma tarefa muito difícil. Especialmente porque a tecnologia está em constante evolução e os sistemas de segurança estão se tornando rapidamente desatualizados, para evitar que seu banco de dados seja completamente comprometido, as empresas adotaram alguns princípios de segurança para evitar a perda completa de seus dados. Alguns desses princípios incluem: backup de dados, criptografia, criação de políticas de senha forte, tecnologia de nuvem, treinamento de funcionários e políticas de relatórios. (NETSUPPORT,2021)

Hoje, para as empresas, um sistema de gerenciamento de banco de dados eficaz é fundamental para suas operações. Todas as informações da empresa são organizadas e armazenadas em um banco de dados. Portanto, proteger esses dados é muito importante, pois é um dos alvos mais visados pelos cibercriminosos. (MAIA,2021)

É fundamental que as empresas entendam todos os riscos que enfrentam e as vulnerabilidades que existem. Só assim será possível tomar as medidas adequadas para corrigir essas falhas e evitar que se tornem problemas mais graves. (FLOWTI, 2021)

Dentre as várias formas de manter a segurança, é importante minimizar o número de pessoas que podem acessar o banco de dados, permitir apenas os responsáveis pelo gerenciamento dos dados e aumentar a segurança para que haja mais confidencialidade. Outra prática recomendada de segurança é criar backups na nuvem de arquivos importantes para proteger o gerenciamento do banco de dados. Armazene seus dados brutos ou de versão criptografados no servidor de banco de dados. (1TECH, 2020)

1.1 PROBLEMATIZAÇÃO

A infraestrutura de TI em cibersegurança é extremamente importante no risco de vazamento de dados de ataques cibernéticos.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Apresentar as vantagens sobre bancos de dados e sua segurança.

1.2.2 OBJETIVOS ESPECÍFICOS

. Demonstrar a importância da segurança do banco de dados.

. Mostrar como usar a segurança em um determinado banco de dados.

. Indicar que alguns bancos de dados requerem segurança.

1.3 HIPÓTESE

A área de TI envolve a análise de proteção de vários tipos de vulnerabilidades, evitando que as informações armazenadas em bancos de dados sejam acessadas por usuários não autorizados.

1.4 JUSTIFICATIVA

Segundo William Bezerra, para ter os dados seguros é preciso garantir a segurança do conjunto de hardware, software e rede onde os bancos de dados será implementado, tanto virtualmente como na nuvem. Sendo assim necessário a configuração dentre outras coisas, como; a alta disponibilidade, os planos de contingência, backup e restores de dados, preferencialmente com a criptografia.

1.4.1 METODOLOGIA

O presente estudo trata- se de uma revisão de literatura sobre a segurança nos bancos de dados, utilizando as seguintes palavras chaves: Segurança, bancos de dados, informações, gerenciamento, backup, no idioma português, fazendo- se o uso dos bancos de dados, como: Infranewstelecom, Santodigital, Internationalit, Securitymagazine, Stefanini, netsupport, Scholar, Zendesk, Devmedia, Flowti, Itforum,

Grancursoonline, Google acadêmico. Para o método de exclusão a base foi retirar artigos com informações duplicadas. Foi feito isto pela leitura dos resumos e de artigos que não se encaixavam com as palavras chaves citadas acima.

E levando em conta os métodos de inclusão foram utilizados artigos entre os anos de 2003 até 2022, com as palavras chaves citadas acima sendo os mesmos revistas, teses, sites e artigo publicados em bancos de pesquisas já referenciados. No total foram encontrados 44 artigos, revistas, sites e teses onde se foi descartado 15 por serem fora do tema proposto ou por não se enquadrarem no objetivo do presente artigo, restando 29 para o desenvolvimento.

2. REFERENCIAL TEÓRICO

2.1 Demonstrar a importância da segurança do banco de dados

A segurança do banco de dados é fundamental para o entendimento das medidas destinadas a proteger ambos os aspectos dos bancos de dados, desta forma, além de as empresas terem maior controle sobre as informações que serão compartilhadas entre seus usuários, pode-se evitar a proliferação de informações privadas. (NETSUPPORT, 2021)

Em outro plano, percebe-se que a confidencialidade comprova que apenas pessoas autorizadas podem acessar determinadas informações, pois o objetivo é que somente o destinatário possa acessar as informações. Afinal, um dos projetos de criptografia de dados refere-se à aplicação de “[…] um algoritmo […] que utiliza uma chave de criptografia especificada pelo usuário ou administrador do banco de dados”, que é uma camada extra de proteção, que impede o hacking invadir redes de banco de dados e acessar informações que podem levar a uma violação de dados. (RAMAKRISSHNAN, GEHRKE, 2008)

Apenas "[...] usuários autorizados recebem algoritmos de codificação ou decodificação (ou chaves) para descriptografar dados". Além disso, outra política que pode ter em vigor são as senhas fortes, que se atualiza regularmente. Vale ressaltar também que é utilizado tecnologias em nuvem que investem em ferramentas de proteção e não gastam tanto em contratos de infraestrutura de sistema, pois podem

ser usadas para backups e reduzir a chance de perda de dados. (ELMASRI, NAVATHE,2011)

Assim, "toda a informação deve ser protegida de acordo com o grau de confidencialidade do seu conteúdo, com o objetivo de limitar o seu acesso e utilização apenas àqueles a quem se destina", para além disso, no que respeita aos sistemas de base de dados, que são habitualmente utilizados pelas maiores empresas como: Oracle e DB2. (SÊMOLA,2003)

Os servidores Oracle fornecem controle de acesso arbitrário, que é um método de restringir o acesso a informações privilegiadas. Os usuários devem receber as permissões apropriadas para acessar objetos de esquema. Os usuários com as permissões apropriadas podem concedê-las a outros a seu critério. (VITOR, JOAQUIM, *et al*; MORAES, MÁRCIO, *et al*; COSTA, RAFAELLO, *et al*;)

2.2 Mostrar como usar a segurança em um determinado banco de dados

Na maioria das empresas hoje, os bancos de dados são onde quase todos os nossos segredos são armazenados. Portanto, protegê-lo de todas as invasões é uma das tarefas mais importantes para administradores de banco de dados, programadores e equipes de DevOps que dependem dele. No entanto, o trabalho não é fácil. Afinal, embora os criadores nos forneçam todas as ferramentas e empreguem boas medidas de segurança, além de documentá-las. No entanto, dezenas de erros, omissões e erros em potencial compreensivelmente bobos tornam o desafio de manter a segurança do banco de dados uma tarefa sem fim. (GAIDARGI, 2021)

Para acabar com esses tipos de ataques, existem métodos como o SGBDs, que é a sigla para Sistema Gerenciador de Banco de Dados - em inglês, Data Base Management System. Com este recurso rodando como software, sua empresa pode utilizar seus dados como referência para realizar diversas tarefas e atividades. Isso é fundamental para controlar o acesso e demarcar as permissões do perfil do usuário. Exemplos de SGBD: MySQL, PostgreSQL, Oracle, SQL Server, Access, etc. (RICARDO, 2006)

A segurança em SGBD (Sistema de Gerenciamento de Banco de Dados) é feita através do controle de acesso onde os perfis dos usuários precisam ser definidos para

delimitar suas permissões. A mitigação de possíveis ataques é outra medida, avaliando e planejando formas de conter e prevenir esses ataques, como o uso de certificados digitais e/ou criptografia. A privacidade das informações é outro aspecto que também precisa ser considerado na lista de ações para beneficiar a segurança do banco de dados. (OCTAVIO, 2021)

Dois tipos de mecanismos de segurança de banco de dados são geralmente mencionados: Mecanismos de segurança discricionários - utilizados para conceder permissões aos usuários, como acesso a arquivos ou registros de dados (ler, inserir, excluir ou atualizar); Mecanismos de segurança obrigatórios - Usados para reforçar a segurança com base no nível de classificação de determinados dados e usuários. (ANA, 2015)

A consideração cuidadosa de como conceder privilégios administrativos aos usuários do banco de dados pode evitar grandes problemas para a organização, incluindo a redução do risco de violações de dados dispendiosas. Embora você possa confiar em um DBA, os cibercriminosos costumam usar ataques de spear phishing e outras táticas para atingir usuários privilegiados de uma organização, explorando suas contas para uso malicioso, incluindo a extração de dados confidenciais. Por exemplo, se um hacker conseguir invadir a conta de um DBA com permissão de execução para o comando "SELECT ANY TABLE", ele poderá acessar quase todos os dados do banco de dados, incluindo números de identificação social, números de cartão de crédito. propriedade. (WILLIAMS; CAHILL, 2019)

A maioria dos fabricantes de SGBDs inclui um subsistema de segurança e autorização de banco de dados para proteger certas partes do banco de dados contra acesso não autorizado. (OCTAVIO, 2021)

Os mecanismos de segurança referem-se às regras impostas pelo subsistema de segurança do SGBD, que examina todas as solicitações de acesso e as compara com as restrições de segurança armazenadas no catálogo do sistema. No entanto, existem vulnerabilidades do sistema e ameaças externas que podem levar a servidores de banco de dados comprometidos ou à destruição ou roubo de dados confidenciais. (MACÊDO, 2011)

Para evitar ataques, é melhor escolher um bom banco de dados, como o PostgreSQL, que é um sistema de banco de dados muito poderoso, capaz de suportar

grandes quantidades de dados. Além disso, possui baixo custo de manutenção e alta estabilidade. (BAIADOCONHECIMENTO, 2022)

Outra questão que se deve estar atento é a forma como os comandos SQL são utilizados em nossas aplicações, principalmente para protegê-las de ataques de injeção de SQL. A injeção de SQL é uma maneira de ignorar logins. Onde invasores enviam comandos por meio de comandos existentes na tentativa de penetrar no software torna-se um risco iminente, pois a partir deste momento, os invasores terão acesso aos dados corporativos para manipulá-los ou copiá-los. (TRENTIN, 2011)

Foi visto que a segurança do banco de dados inclui medidas destinadas a proteger os dados em duas áreas. Ela teve o cuidado de evitar que o sistema caísse nas mãos de pessoas não autorizadas, e também se preocupava com quem poderia realmente acessá-lo. A importância de ter todo esse controle é a sobrevivência da empresa. Sabendo que a coleta de dados é fundamental para orientar as empresas no mercado, descobrir perfis de consumidores, traçar estratégias de vendas e manter-se competitivo no mercado. (NETSUPPORT, 2022)

2.3 Indicar que alguns bancos de dados requerem segurança

Com o avanço da tecnologia, a segurança de dados está se tornando cada vez mais importante nas empresas, principalmente na área de TI. Estratégias contra ataques digitais são necessárias para garantir os conjuntos de dados mais seguros. No entanto, um dos problemas mais comuns com um sistema é que qualquer falha encontrada nele tem o potencial de descobrir um problema maior, como um ataque cibernético, de modo que pequenas e médias empresas podem correr o risco de perder dados para criminosos cibernéticos. (STEFANINIGROUP, 2021)

Todos os dias os ataques cibernéticos atacam redes de outros usuários afim de buscar algum tipo de benefício ao ter acesso a rede da vítima, diante disso existem dois tipos de empresas; as que foram hackeadas e as que não sabem que foram hackeadas. (INTERNATIONALE, 2021)

Alguns tipos de ataques cibernéticos são DDoS Attack, Port Scanning Attack, Ransomware, Phishing, Injeção de SQL, Ameaça persistente avançada (APT) (INTERNATIONALLT, 2021)

Os criminosos podem lucrar bastante conseguindo ter a pose de dados financeiros, propriedade intelectual e segredos corporativo, considerando que, tudo que se faz hoje é online. Vazamentos, roubos de identidade e vendas de dados tornou sua fonte de renda. (SANTODIGITAL, 2022)

Segundo uma entrevista realizada pela opinion box, 57% das pessoas afirmaram que suas preocupações com a segurança de seus dados aumentaram nos últimos anos, por isso é de suma importância assegurar que seus dados estão protegidos. Diante disso existem alguns tipos de plugins para garantir a segurança de um site, por exemplo: Security, Jetpack e VaultPress. (SILVA, 2021)

Como Cuckier disse, nossos dados fornecem evidências quantificáveis de que ataques estão ocorrendo em computadores com conexões de Internet. (SECURITYMAGAZINE,2022)

3. Segurança da Informação

A segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes integridade, disponibilidade e confidencialidade. (SILVA, 2004).

Conhecer os conceitos sobre segurança da informação não significa necessariamente saber garantir essa segurança. Muitos têm experimentado esta sensação quando elaboram seus planos de segurança e acabam não atingindo os resultados desejados. (CAMPOS, 2007)

Segurança da informação refere-se à preservação da integridade e do sigilo, quando a informação é armazenada ou transmitida. Violações de segurança da informação ocorrem quando as informações são acessadas por pessoas não autorizadas ou festas. Violações podem ser o resultado de ações de hackers, as agências de inteligência, os criminosos, concorrentes, funcionários ou outros. Além disso, pessoas que valorizam e desejam preservar a sua privacidade estão interessado em segurança da informação. (BROOK, 2010)

Tecnologias da Informação e Comunicação, tem uma abordagem referente as políticas de segurança da informação, sob o ponto de vista da gestão. Não se pode pensar nas TICs apenas como uma unidade tecnológica responsável pelas aplicações de informática dentro da organização, o objetivo principal desse setor é desenvolver

conhecimentos, gerando melhorias nos sistemas de informação, melhorando processos, auxiliando nas atividades e consequentemente otimizando os negócios. 23 “Tecnologia da Informação pode ser conceituada como recursos tecnológicos e computacionais para geração e uso da informação [..]” (REZENDE, 2005).

A vulnerabilidade em segurança da informação pode ser considerada como a fragilidade onde uma ameaça pode atacar de alguma forma, nesse caso é necessário identificar essas vulnerabilidades e saber como elas estão abertas, ou seja, vulneráveis. (COELHO; *et al*., 2014)

3.1 Segurança de banco de dados corporativo

As novas tecnologias estão realmente forçando empresas de todos os portes e segmentos de mercado a modernizar e integrar a cultura digital no dia a dia das empresas. Essas mudanças podem variar desde pequenas mudanças nos serviços, como conectar-se a sites e redes sociais para se comunicar com os clientes, até automação em larga escala e virtualização de tarefas, como portfólios online para gerenciamento de contas e finanças. No entanto, esse ambiente moderno exige os cuidados necessários para garantir que a empresa sobreviva em uma situação que antes não era preocupante. Por exemplo, podendo lembrar do ataque cibernético em Atlanta, EUA, em março do ano de 2017. A segurança da informação trata de garantir a proteção de informações confidenciais que circulam em um ambiente de negócios. Além disso, garante que as mesmas informações estejam totalmente disponíveis quando necessário e fornecidas apenas por pessoal autorizado. No entanto, essa prática deve estar alinhada com outras estratégias para eliminar completamente os erros na segurança dos dados. (ETH, 2018)

A integridade dos dados também é importante devido à acessibilidade, confiabilidade e consistência das informações ao longo de seu ciclo de vida. Ele é projetado para preservar o conhecimento para que nada seja danificado ou perdido. Assim, atrapalhando o planejamento de toda a organização. Devido à sua importância, a integridade dos dados é uma grande preocupação para muitas soluções de segurança. Isso porque várias ferramentas de proteção foram criadas para preservar ao máximo o que está disponível no sistema. (GUERRA, 2020)

A segurança do banco de dados é direcionada para garantir a integridade, disponibilidade e confidencialidade das informações. Portanto, é necessário utilizar diferentes mecanismos para restringir o acesso das pessoas aos dados e distribuir o fluxo de informações. Profissionais experientes em gerenciamento de banco de dados já conhecem as principais vulnerabilidades do ambiente e podem identificar rapidamente as principais tentativas de intrusão. Por meio do monitoramento contínuo, eles criam barreiras ao acesso aos dados e agem em qualquer situação de ameaça. (SAPHIR, 2020)

Os bancos de dados são estratégicos para as empresas porque centralizam grandes quantidades de informações e aplicativos e precisam operar com segurança adequada, desempenho eficiente e alta disponibilidade. Proteger todos esses aspectos do banco de dados da melhor maneira possível requer uma tremenda dedicação e muito trabalho dos DBAs, administradores de banco de dados e toda a equipe de TI. Como geralmente tudo é feito manualmente, não há automação de banco de dados. Você precisa lidar com segurança, proteção de dados, custo, disponibilidade, conformidade e atualizações e migrações. Assim, automatizando determinadas tarefas, os profissionais podem liberar seu tempo para focar em assuntos mais estratégicos e também tornar toda a operação mais eficiente. (MICROSERVICE, 2022)

Bancos de dados autônomos já são uma realidade. Com essa tecnologia, otimização, reparo, escalabilidade e tarefas relacionadas são realizadas pelo próprio banco de dados. Em um banco de dados autônomo, algumas tarefas executadas manualmente, como otimização, reparo ou até mesmo instalação de patches de segurança, não existem mais para o DBA porque isso é feito pelo próprio banco de dados. Humanos cometem erros, não importa quão bons profissionais sejam. Na operação autônoma, com a ajuda de inteligência artificial e aprendizado de máquina, o erro humano é bastante reduzido. (HIGA, 2018)

Além de aplicar segurança em camadas a todo o ambiente de rede, a segurança do banco de dados requer o estabelecimento dos controles e políticas corretos para acesso ao banco. Essas políticas de segurança de banco de dados devem ser integradas para dar suporte aos objetivos gerais de negócios da organização e às políticas de segurança de rede e nuvem. As responsabilidades pela manutenção e revisão de tais controles de segurança precisam ser definidas. Medidas

adicionais podem ser estabelecidas para apoiar mecanismos formais de segurança, como treinamento de conscientização, programas educacionais, testes de penetração e estratégias de avaliação de vulnerabilidade. (GIFFONI, ERICK, 2022)

3.2 Proteção dos Dados no SQL Azure

O Banco de Dados SQL do Azure fornece serviços de banco de dados relacional no Azure. Para proteger os dados do cliente e fornecer os recursos de segurança robustos que os clientes esperam dos serviços de banco de dados relacional, o Banco de Dados SQL tem seu próprio conjunto de recursos de segurança. Essas funções são baseadas em controles herdados do Azure. O principal princípio de segurança de rede para produtos do Banco de Dados SQL do Azure é permitir apenas as conexões e comunicações necessárias para permitir que o serviço funcione. Todas as outras portas, protocolos e conexões são bloqueadas por padrão. LANs virtuais e ACLs são usadas para restringir o tráfego de rede por redes de origem e destino, protocolos e números de porta. (LANFEAR; *et al*., 2022)

Uma das exigências da LGPD é a confidencialidade de dados como números de cartão de crédito, CPF, etc. No SQL Azure, você pode mascarar ou modificar determinados dados para que não possam ser vistos por usuários sem privilégios. Com o comando T-SQL, você pode aplicar máscaras a colunas. (COUTINHO, 2020)

Lida com o gerenciamento de identidade e autenticação com eficiência. Há duas maneiras de fazer isso: Autenticação SQL (nome de usuário e senha) e Azure Active Directory (Azure AD). Todos os servidores têm o nome de usuário root e a senha de usuário mestre que foi criado durante a configuração. Mas então podemos habilitar o Azure Active Directory. Precisa habilitar a ID raiz para isso e, em seguida, pode-se criar usuários do Azure Active Directory que também podem receber acesso. Assim, depois de configurar um usuário administrador, você abre a porta para que outros usuários se autentiquem por meio do Azure Active Directory em vez da autenticação do SQL Server. Ele permite que você gerencie sua segurança a partir de um local centralizado, em vez de o SQL Server ter seu próprio banco de dados de autenticação. (LIMA, 2022)

Para ajudar a proteger os dados do cliente, o Banco de Dados SQL do Azure inclui um recurso de firewall que bloqueia todo o acesso ao Banco de Dados SQL por padrão. Os firewalls de gateway podem restringir endereços, permitindo um controle refinado sobre os clientes para especificar intervalos de endereços IP aceitáveis. O firewall concede acesso com base no endereço IP original de cada solicitação. (RABELER; *et al*., 2022)

O recurso Microsoft Defender para SQL detecta possíveis ameaças à medida que ocorrem e fornece alertas de segurança para atividades incomuns. Os usuários podem usar recursos de auditoria para explorar esses eventos suspeitos e determinar se o evento se destina a acessar, adulterar ou explorar dados no banco de dados. Os usuários também obtêm uma visão geral da segurança, que inclui avaliações de vulnerabilidade e ferramentas de descoberta e classificação de dados. (JACKSON; *et al*., 2022)

O SQL Azure também possui recursos avançados de proteção contra ameaças que detectam atividades incomuns e indicam tentativas potencialmente prejudiciais de acessar ou explorar bancos de dados. A Proteção Avançada contra Ameaças identifica potencial injeção de SQL, acesso de data centers ou locais anômalos, acesso de entidades desconhecidas ou aplicativos potencialmente indesejados e credenciais SQL de força bruta. (BUCKGIT; *et al*., 2022)

4. Ameaças à Segurança na Internet

Segurança da Internet é um termo que descreve a segurança de atividades e transações feitas pela Internet. Trata-se de um componente particular de ideias maiores, como segurança virtual e segurança do computador, envolvendo tópicos que incluem segurança do navegador, comportamento on-line e segurança de rede. (KASPERSKY, 2022)

Os softwares maliciosos, conhecidos como malwares, surgiram em 1971, são programas criados para executar ações danosas e atividades maliciosas em um computador. É importante conhecer seu tipo. (FRANÇA, 2020)

Malware - O malware eles não representam uma ameaça apenas para um computador, rede ou sistema, porque também são capazes de assumir controle dos equipamentos diretamente conectados a eles. Vírus são um tipo de malware, mas nem todo malware é um vírus. (MOURA, 2022).

Espionagem industrial - É a prática de obter informações secretas ou confidenciais sobre organização, empresa ou mesmo de pessoas que não tem autorização. (RODRIGUES, 2017).

Ransomware -O ransomware é um dos malwares mais temidos pelos usuários, pela maneira que afeta suas vítimas. Em suas primeiras ocorrências, esse malware bloqueava a tela do computador deixando exposta uma mensagem exigindo pagamento para que o computador fosse liberado. Com o seu sucesso, surgiram diversas novas variantes e, consequentemente, mais perigosas. As novas versões são capazes de criptografar os arquivos do seu dispositivo exibindo informações de como proceder para receber a chave de desbloqueio. O pagamento geralmente é solicitado através de Bitcoins, uma moeda eletrônica independente de qualquer autoridade central. É bom lembrar que o pagamento não garante que seus arquivos sejam desbloqueados, afinal como dificilmente é possível identificar o criminoso, também não há como cobrá-lo. (TREND MICRO, 2015).

O livro Guia do Hacker Brasileiro (2002), do autor Marcos Flávio Assunção se inicia com a pergunta: “Estamos seguros?”. Ao final do tópico, após discorrer um pouco sobre segurança em informática, o próprio autor responde à pergunta: “com certeza que não”.

O tema segurança da informação desperta um pouco a curiosidade e a preocupação dos usuários de um modo geral. Curiosidade, pois intriga um pouco quando é visto notícias de crackers que invadem sistemas, tiram sites do ar, roubam informações, etc. E, preocupação porque fica no meio desse fogo cruzado: de um lado o desenvolvimento promovido por empresas e entidades de ensino a serviço da utilidade pública com técnicas e novos serviços do campo da segurança da informação; e do outro, o bandido que de algum modo consegue ter acesso a essas ferramentas e utilizá-las de certa forma antiética. (RASMO, 2017)

a vulnerabilidade é uma condição existente num software ou hardware, e que pode resultar em perda de uma ou mais propriedades da segurança da informação, conforme citadas anteriormente. Uma vulnerabilidade pode deixar um sistema propenso a um ataque. Aplicações web utilizam-se de sistemas gerenciadores de banco de dados (SGBD) para armazenar informações de usuários. Para aplicar segurança nesses SGBDs, é preciso pensar na proteção das informações contidas

ali. Exemplos de ataques de grande proporção ocorreram com o site do Yahoo quando teve milhões de contas de usuários roubadas, e os criminosos tentaram negociar essas informações no mercado negro da internet. Portanto, um desenvolvedor precisa estar atento à forma de armazenamento de informações sensíveis nos bancos de dados, como senhas, números de cartões, CPFs, etc. Se essas informações são guardadas em texto puro, um ataque como o do Yahoo pode expor totalmente os usuários. (LENTO, 2014)

É importante que as organizações definam uma estrutura adequada para a proteção – e gestão – de suas informações, de acordo com seu porte e tipo de negócios, de modo a conscientizar todos os colaboradores de que a informação é um bem, isto é, tem valor para a empresa e deve ser protegida (FONTES, 2006).

A segurança da informação prioriza não apenas as ferramentas de prevenção anti-ataque, mas também os dados gerados e coletados dentro da empresa. De acordo com um estudo realizado pelo Instituto Ponemon em parceria com a Varonis, constatou-se que 62% dos funcionários afirmaram ter acesso a dados que não precisavam para realizar tarefas cotidianas. Ainda assim, menos de 30% das empresas documentam o que os funcionários fazem com essas informações (COMPUTERWORLD, 2016).

Em agosto de 2013, o Yahoo teve a maior violação de dados de sua história, alegando que dados associados a mais de 1 bilhão de contas de usuários foram roubados, incluindo nomes, endereços de e-mail, números de telefone, datas de nascimento e senhas criptografadas (COMPUTERWORLD, 2016).

Também em 2013, mais de 4,6 milhões de usuários do aplicativo Snapchat foram notificados de que seu número de celular e localização foram comprometidos sem sua permissão (LANDIM, 2014).

4.1 Segurança nas redes sociais

Nos dias de hoje a segurança nas redes sociais é de grande importância para a proteção de dados de seus usuários, é muito difícil encontrar empresas ou alguém que não tenha acesso a este tipo de comunicação, as redes sociais se tornou

essencial para milhares de pessoas , quanto maior a popularidade dentro delas , maior é o perigo de cair em golpes onlines praticados pelos cibercriminosos. (ID5,2022)

Segundo levantamento do IBGE , sete a cada dez brasileiros estão conectados nas redes sociais , sendo considerado , 181,1 milhões de brasileiros com 10 anos ou mais , sendo assim , a tendência é crescer cada vez mais. (CETIC, 2022)

Facebook e Instagram permite o compartilhamento de atividades , sendo elas , fotos , vídeos , localização, por conta das diversas possibilidades que existem em diferentes serviços que também são ultilizados por crianças e adolescente , é de suma importância explicar para eles sobre como ultilizar estes serviços com responsabilidade e segurança. (DIALOGANDO, 2015)

Um aplicativo de mensagens seguro usa criptografia completa para a proteção de dados de seus usuários ao longo de toda a jornada, ao remetente e o destinatário. Sendo assim, os dados são enviados criptografados e descriptografadas quando chegam ao destino, nesse tempo de envio e entrega, ninguém em hipótese alguma pode ter acesso. Ainda assim, a criptografia completa evita que os aplicativos de mensagens seguros armazenem cópias de suas comunicações nos servidores deles no caso de uma violação de dados. (BELCIC; CORRIGAN, 2022)

Segurança no Whatsapp

A criptografia ponta a ponta do WhatsApp protege as chamadas e mensagens dos usuários , garantindo assim que as conversas e ligações fique somente entre você e a pessoa discada, nem mesmo o whatsapp tem a possibilidade de ouvir e ler as mensagens, com a nova atualização do aplicativo de mensagem, existe a possibilidade de enviar e receber dinheiro através da opção PAGAMENTOS, contudo , as informações de cartões de créditos são armazenadas e criptografadas em um lugar seguro. (WHATSAPP LLC, 2022)

Para a proteção de mensagens antigas é necessário que o usuário desabilite o backup do aplicativo de mensagem, fazendo com que isso impeça que as conversas sejam acessadas pelo backup salvo em serviço de nuvem, contudo, por outro lado, as mensagens não poderiam serem vistas caso o usuário mudasse de aparelho. (PERALLIS, 2019)

Segurança no Instagram

Com os ataques cibernéticos , como a invasão nos servidores e hackeamento em perfis nas redes sociais , estão se tornando cada vez mais comum, por isso , proteger a sua conta é de extrema importância. Dentro das seguranças do Instagram, existem as seguintes formas de proteger seus dados, sendo uma delas , autenticação de dois fatores , SMS. Ambos para poder logar a sua conta no aplicativo de mensagem vai gerar um código para informar dentro do Instagram , esse código é de forma mutável , sempre que a pessoa logar e deslogar vai pedir um código diferente. (PIPEMARKETING,2020)

Algumas ações que podem ser tomadas para evitar armadilhas nas redes sociais segundo o site Id5.

a) Senhas fortes com no mínimo 8 números incluindo letras maiúsculas e minúsculas e caracteres.

b) Evitar clicar em links desconhecidos

c) Não adicionar pessoas desconhecidas

d) Prestar atenção ao que compartilha

Existem duas formas diferentes de nossas informações pessoais ficarem gravadas na internet. São eles de maneira voluntária ou involuntária, sendo assim, os dados voluntários são aqueles que as pessoas publicam diretamente nas suas redes, sejam elas, e-mails, Instagram, Facebook, compartilhando fotos, vídeos e até mesmo comentando. Já os dados involuntários são um conjunto de dados e metadados pessoais que são gerados e armazenados pelos equipamentos e serviços que fazem a mediação com os ambientes digitais, sendo eles, cookies, histórico de navegação e buscas, dados de acessos a arquivos e serviços, senhas, logins. (SaferNet, 2018)

Segundo Gonçalves (2013), um estudo realizado em 2009 pela AT&T Labs e Worcester Polytechnic Institute, constatou que o código de identificação atribuído aos usuários pode ser associado com o comportamento monitorado pelos cookies.

Informações que também podem ser obtidas através de “cookies”:

a) Rastreamento dos sites que o usuário visite

b) Armazenar informações a sites específicos

c) Acompanhamento de movimento de visita de um site para outro

d) Construção de um perfil em torno de um usuário

4.2 Profissionais de Segurança de TI

É difícil imaginar um mundo sem internet. Seja profissionalmente ou pessoalmente, a tecnologia está presente no dia a dia da maioria das pessoas. Com a popularização da navegação na web, a área de segurança da informação também tem recebido cada vez mais atenção no ambiente virtual da área técnica. Conhecido como segurança cibernética ou cibersegurança, visa proteger os dados de usuários e empresas de más práticas ou uso indevido. (MENDES, 2020)

Os profissionais de segurança da informação trabalham para reduzir o risco de incidentes que possam comprometer a disponibilidade, integridade e confidencialidade das informações. Ele precisa de algum conhecimento específico na área para entender como proteger os dados. Por exemplo: esse analista deve entender a teoria das redes de computadores, seus protocolos e suas melhores práticas; além de aprender constantemente novas maneiras de destruir informações e como evitá-las, você também deve entender os sistemas operacionais e como eles funcionam. (DUARTE, 2018)

As responsabilidades de um profissional de segurança da informação estão relacionadas à proteção de todas as informações e dados de uma empresa, seja online ou não. Hoje, com a maioria das informações concentradas em bancos de dados e na nuvem, a segurança cibernética tornou-se extremamente importante para as empresas, pois não é incomum que hackers tentem obter acesso a informações confidenciais. Este profissional é obrigado a tomar medidas para proteger dados e informações de qualquer tipo de ameaça que possa surgir. O objetivo é sempre garantir a continuidade operacional e minimizar o risco do negócio. (INFOTECBLOG, 2021)

O campo da segurança da informação é muito amplo e atraente financeiramente. Além disso, seu mercado está se expandindo como parte do setor de tecnologia. Nesse Ramo existem algumas áreas de atuação como: Segurança Empresarial: O profissional deve desenvolver um plano estratégico para proteger os dados da empresa, realizar auditorias de sistema e monitorar a política de segurança da organização; Desenvolvimento de software de segurança: Este profissional

desenvolve produtos e serviços e analisa códigos maliciosos (malware); Segurança forense: é o profissional que pesquisa, coleta e reporta provas digitais em investigações policiais, especialmente crimes cibernéticos; Inteligência Nacional: Este profissional também pode atuar em órgãos de segurança do governo, como a Agência Brasileira de Inteligência. (CARREIRA, 2022)

Para ter sucesso na área de segurança da informação, os profissionais precisam ter pelo menos um diploma de bacharel em cursos relacionados à informática, como: Ciência da Computação, Análise de sistemas, Programação, Tecnologia da informação e Sistema de informação. No entanto, algumas empresas preferem que seus especialistas em segurança de TI tenham um Master of Business Administration (MBA) com ênfase em tecnologia da informação ou sistemas, que é orientado à segurança da informação. (SINCE, 2020)

Não é fácil resumir a área de TI em poucas frases, principalmente considerando quantas carreiras existem nessa área. Existem as especializadas em infraestrutura (ou seja, mantêm dispositivos de hardware em operação), redes (fornece conectividade local ou remota entre dispositivos e recursos da empresa de forma segura), bancos de dados (com servidores e repositórios de gerenciamento), etc. Independentemente disso, a importância dos profissionais de TI é inquestionável. Sem ele, as empresas não têm os recursos técnicos necessários para se manterem competitivas em um mercado cada vez mais competitivo, nem conseguem acompanhar as tecnologias mais recentes para garantir a produtividade dos funcionários. (PERALLIS, 2022)

5. Internet das coisas

A Internet das coisas do termo em inglês - internet of things (IoT) é uma referência á tendência de diferentes tipos de objetos de conseguirem estabelecer conexão com a internet, sendo eles do eletrodomésticos ao carro , sendo assim , estes objetos conseguem coletar e transmitir dados a partir da nuvem. Já é possível encontrar dispositivos IoT como na vida diária ou no âmbito de trabalho. (TECMUNDO, 2022)

A internet das coisas se refere a uma revolução tecnológica,a ideia é que cada vez mais o mundo físico e digital se torne um só , através de dispositivos que se comuniquem com os outros , os datas centers e suas nuvens , smartwatch , Google

Glass. O surgimento dessa ideia foi discutida desde 1991, quando a conexão TCP/IP e a internet que é conhecida começou a popularizar , Bill joy que foi o cofundador da sun microsystem pensou sobre a conexão de device para device. (TECHTUDO, 2022)

Em 2005 a internet das coisas entrou em discussão onde foi generalizada , começou a ganhar atenção dos governos e apareceu em questões sobre privacidade e segurança de dados, foi a partir daí que a internet das coisas tornou- se pauta do Internacional Elecommunication Union. (CHICARINO; et al., 2017)

Tudo que está conectado a internet está vulnerável. As pessoas tem o pensamento de que não precisam de segurança, que não correm riscos pois os equipamentos estão seguros em casa ou até mesmo que seus dados não são importantes. Os dados dos usuários são o maior bem do futuro. Nos últimos anos, os maiores ataques cibernéticos foram disparados através de vulnerabilidades encontradas em dispositivos eletroeletrônicos. Dispositivos vulneráveis conectados à internet podem ser sequestrados com facilidade e transformados em uma grande botnet para ser utilizada em ataques de negação de serviço distribuído. (BORGES, 2021)

A internet das coisas promete comodidade incomparável, ainda assim, para que a IoT atinja seu esperado potencial, será necessário conquistar e manter a confiança dos consumidores sobre questões como privacidade e segurança. Os dados serão transmitidos pela IoT e formarão uma representação gráfica de cada pessoa, o maior desafio será de proteger essas informações. (THALES,2022)

SOLUÇÕES DE CIBERSERGURANÇA PARA CONSTRUIR CONFIANÇA

Para desenvolver um dispositivo IoT que oferece uma conexão segura e confiável é um grande desafio para os especialistas em cibersegurança. a segurança digital deve fazer parte de todo o ciclo de vida do dispositivo: projeto, fabricação e durante o uso das pessoas. o software para esses dispositivos IoT deve ser proativo, preventivo e corretivo, segurança, privacidade, disponibilidade e integridade de dados. (PINHEIRO,2022)

Os invasores tem muitos meios de acessar os recursos ou dados em um dispositivo conectado, os três alvos sãos: o dispositivo, a infraestrutura de nuvem e a rede. (THALES,2022)

IoT: RELAÇAO DE CONFIANÇA

Para a internet das coisas funcionar com efetividade, as empresas precisam trabalhar na auto confiança dos seus clientes por meio do fornecimento de uma tecnologia cada vez melhor e segura. (PINHEIRO, 2022)

Segurança e privacidade na internet das coisas

A implementação da tecnologia associadas à internet das coisas é fundamental para o desenvolvimento social e econômico do país, principalmente para o uso da tecnologia da informação e comunicação. Contudo, a IoT também traz uma série de riscos em relação a segurança, privacidade e a proteção de dados. ainda assim, ao considerar seus aspectos sociais e econômicos, essa estratégia identifica os riscos de três tecnologia que sustentam esse modelo: dispositivos e sensores, sistemas de inteligência artificial e computação em nuvem. Explorando ainda aspectos regulatórios e técnicos importantes para o desenvolvimento de tecnologias para uma IoT mais segura. (HUREL; LOBATO, 2018)

6. CONSIDERAÇÕES FINAIS

Esta pesquisa mostra que deve ter como objetivo a proteção de dados, evitando que um sistema caia em mãos não autorizadas, ao mesmo tempo em que causa preocupação com quem realmente tem acesso a ele.

Portanto, é necessário entender que os dados são muito valiosos e várias medidas de segurança devem ser implementadas nos sistemas de segurança de dados para garantir sua integridade, disponibilidade e confidencialidade.

Por isso, as ameaças que estão sempre ativas na internet também são mostradas para capturar e roubar dados de usuários para extorsão e venda para outras empresas ou terceiros.

Em conclusão, mostra- se também a importância da segurança nas redes sociais, diante do comportamento dos usuários em compartilharem seus respectivos dados, como fotos e vídeos, visando a importância da criptografia em cada aplicativos de mensagens.

REFERÊNCIAS

ACERVO LIMA: O QUE SÃO RECURSOS DE SEGURANÇA DE DADOS DO AZURE?, 2022. Disponível em: (https://acervolima.com/o-que-sao-recursos-de-seguranca-de-dados-do-azure/). Acesso em: (16/05/2022)

ADMINISTRADOR. Segurança em Banco de Dados: Cuidando do bem mais valioso da empresa, MICREIROS, 2011. Disponível em: (https://micreiros.com/seguranca-em-banco-de-dados-cuidando-do-bem-mais-valioso-da-empresa/). Acesso em: (28 de maio de 2022)

As 4 principais ameaças à segurança de rede e os seus impactos no negócio. Copyritht, 2022. Disponível em : (https://www.upx.com/post/principais-ameacas-rede/#:~:text=1.-,Malware,software%20de%20risco%20seja%20instalado). Acesso em: (24/05/2022).

BAIA DO CONHECIMENTO: O que é restrição de segurança banco de dados?, 2022. Disponível em: (https://baiadoconhecimento.com/biblioteca/conhecimento/read/419549-o-que-e-restricao-de-seguranca-banco-de-dados). Acesso em: (24/05/2022)

BELCIC, Corrigan. Os aplicativos de mensagem mais seguros, AVG, 2022. Disponível em: (https://www.avg.com/pt/signal/secure-message-apps). Acesso em: (05 de junho de 2022).

BUCKGIT, Alex. Configurar a Proteção Avançada contra Ameaças para o Banco de Dados SQL do Azure, 2022. MICROSOFT.

BURNETT, Steven. Criptografia e segurança: o guia oficial RSA, Gulf Professional Publishing, 2002. Google Books.

CETIC, TIC Domicílios, 2022. Disponível em: (https://cetic.br/pesquisa/domicilios/). Acesso em: (29/05/2022).

Ciberataques: O que são e quais são os principais tipos? International IT, 2021. Disponível em: (https://www.internationalit.com/post/ciberataques-o-que-s%C3%A3o-e-quais-s%C3%A3o-os-principais-tipos) . Acesso em: (24/03/2022).

DIALOGANDO, Segurança nas redes sociais, 2015. Disponível em: (https://www.dialogando.com.br/seguranca/seguranca-nas-redes-sociais). Acesso em: (13/05/2022).

França, Bruna. Principais programas maliciosos. Disponível em: (https://br.ccm.net/faq/9841-os-diferentes-tipos-de-programas-maliciosos) . Acesso em: 20 de maio. de 2022.

GAIDARGI. Juliana. Erros que comprometem a segurança do seu banco de dados, INFONOVA, 2021. Disponível em: (https://www.infonova.com.br/seguranca/erros-seguranca-banco-dados/). Acesso em: (20 de maio de 2022)

Hackers atacaram os dados da sua empresa? Explicamos como proceder. Flowti, 2021. Disponível em: (https://flowti.com.br/blog/hackers-atacaram-os-dados-da-sua-empresa-explicamos-como-proceder) . Acesso em: (21/03/2022).

ID5, Segurança nas Redes Sociais: Dicas importantes de proteção, 2022. Disponível em: (https://www.id5.com.br/blog/seguranca-nas-redes-

sociais/#:~:text=Configura%C3%A7%C3%B5es%20da%20seguran%C3%A7a%20nas%20Redes,expor%20seus%20dados%20a%20ningu%C3%A9m.). Acesso em: (30/05/2022).

JACKSON, Shawn. Tutorial: Proteger um banco de dados no Banco de Dados SQL do Azure, 2022. MICROSOFT.

KEYWORDS. Hackers Attack Every 39 Seconds ! Confira nosso guia completo do assunto. 10 de fevereiro de 2017. Disponível em: (https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds) . Acesso em 07 de mar. de 2022.

LIMA, Luís. Segurança em Banco de Dados. Gran cursos online, 2021. Disponível em: (https://blog.grancursosonline.com.br/seguranca-em-banco-de-dados-parte-1/) . Acesso em: (11/03/2022).

MACÊDO, Diego. Conceitos sobre Segurança em Banco de Dados, DIEGOMACÊDO, 2011. Disponível em: (https://www.diegomacedo.com.br/conceitos-sobre-seguranca-em-banco-de-dados/). Acesso em: (14/05/2022)

MASIERO, Bárbara. Como proteger a sua conta no Instagram, PIPE MARKETING, 2022. Disponível em: (https://pipemarketing.com.br/2022/02/18/como-proteger-a-sua-conta-no-instagram/). Acesso em: (03 de junho de 2022).

Melhores práticas para segurança de banco de dados. Techsolucoes, 2020. Disponível em: (https://www.1techsolucoes.com.br/blog/melhores-praticas-para-seguranca-de-banco-de-dados/) . Acesso em: (25/03/2022).

MENDES, Carina. O que faz um Administrador de Bancos de Dados? Freelancermap ,2020. Disponível em: (https://www.freelancermap.com/blog/pt/que-faz-administrador-bancos-dados/) . Acesso em: (26/03/2022).

MENDES. Tatyane. Segurança da informação: entenda a alta demanda por profissionais de cibersegurança, NA PRATICA, 2020. Disponível em: (https://www.napratica.org.br/seguranca-da-informacao-ciberseguranca/) Acesso em: (25 de maio de 2022)

Métodos de controle de segurança de banco de dados. Acervolima, 2022. Disponível em: (https://acervolima.com/metodos-de-controle-de-seguranca-de-banco-de-dados/) . Acesso em: (20/03/2022).

MONTEIRO, Fabio. Segurança em banco de dados relacional: Revista SQL magazine 111. DEVMEDIA, 2013. Disponível em: (https://www.devmedia.com.br/seguranca-em-banco-de-dados-relacional-revista-sql-magazine-111/27854) . Acesso em: (03/03/2022).

MORAES, José. Como proteger de forma eficaz os seus bancos de dados: Qual seu plano para não ser mais uma vítima? Itforum, 2021. Disponível em: (https://itforum.com.br/noticias/como-proteger-de-forma-eficaz-o-seus-bancos-de-dados/) . Acesso em: (05/03/2022).

MOURA, Bianca. O que é malware? Disponível em: (https://www.psafe.com/blog/o-que-e-malware-e-como-se-proteger/) . Acesso em: 20 de maio. de 2022.

NAKAMURA, Emílio. Segurança de redes em ambientes cooperativos ,2007. Google Books

O que faz e qual é a importância do profissional de TI?, 2022. Disponível em: (https://www.perallis.com/news/o-que-faz-e-qual-e-a-importancia-do-profissional-de-ti). Acesso em: (01/06/2022)

O que faz um profissional de segurança da informação? 2022. Disponível em: (https://www.infotecblog.com.br/o-que-faz-profissional-seguranca-informacao/). Acesso em: (27/05/2022)

PERALLIS SECURITY, Saiba como aumentar a segurança do celular e dos aplicativos de mensagens, 2022. Disponível em: (https://www.perallis.com/news/saiba-como-aumentar-a-seguranca-do-celular-e-dos-aplicativos-de-mensagens). Acesso em: (05/06/2022).

Pereira, Danilo. Ransomware: origens, consequências e prevenção. Disponível em: (https://propi.ifto.edu.br/ocs/index.php/jice/10jice/paper/viewFile/9705/4320) . Acesso em: 22 de maio. de 2022.

PINHEIRO, Walber. Segurança e privacidade em Internet das Coisas (IoT): como aumentar a confiança do usuário?, IPOG, 2022, Disponível em : (https://blog.ipog.edu.br/tecnologia/segurana-e-privacidade-em-internet-das-coisas-iot-como-aumentar-a-confiana-do-usurio/amp/) acessado em: (06 de maio de 2022)

Regan, Joseph. O que é malware? O Guia Definitivo para Malware. AVG. 2022. Disponível em: (https://www.avg.com/pt/signal/what-is-malware) . Acesso em: 26 de maio. de 2022.

Rodrigues, Suellen. Espionagem industrial, você sabe o que significa?. Disponível em: (https://suellenrvianaa.jusbrasil.com.br/artigos/432306800/espionagem-industrial-voce-sabe-o-que-significa) . Acesso em: 22 de maio de 2022.

Segurança de BDs por concessão de privilégios de acesso a usuários no Oracle. Devmedia, 2015. Disponível em: (https://www.devmedia.com.br/seguranca-de-bds-por-concessao-de-privilegios-de-acesso-a-usuarios-no-oracle/33266) . Acesso em: (10/03/2022).

Segurança em banco de dados: As 5 causas de ataque mais comuns. Santo digital, 2022. Disponível em: (https://santodigital.com.br/seguranca-em-banco-de-dados-5-causas-de-ataques-mais-comuns/). Acesso em: (14/03/2022).

Segurança em banco de dados: Com o que se preocupar. Netsupport, 2021. Disponível em: (https://netsupport.com.br/segurança-em-banco-de-dados/) . Acesso em: (08/03/2022).

SILVA, Douglas. Segurança de dados na internet: por que se preocupar? Zendesk,2020. Disponível em: (https://www.zendesk.com.br/blog/segurança-dados-internet/) . Acesso em: (15/03/2022).

SOLUTIONS, Agility. As vulnerabilidades e necessidades de segurança da Internet das Coisas, AGILITY SOLUTIONS, 2016. Disponível em: (https://agilitysolutions.com.br/as-vulnerabilidades-e-necessidades-de-seguranca-da-internet-das-coisas/). Acesso em: (04 de junho de 2022).

STEFANINI, GROUP. Tudo sobre segurança da Informação! Confira nosso guia completo do assunto. Stefanini. 2021. Disponível em: (https://stefanini.com/pt-

br/trends/artigos/guia-sobre-seguranca-da-informacao). Acesso em 03 de mar. de 2022.

TAMASSIA, Roberto. Introdução a segurança de computadores., 2013. Google Books

Tiinside. As 5 maiores preocupações em cibersegurança para os gestores de TI ! Confira nosso guia completo do assunto. 15 de setembro de 2021. Disponível em: (https://www.google.com/amp/s/tiinside.com.br/15/09/2021/as-5-maiores-preocupacoes-em-ciberseguranca-para-os-gestores-de-ti/%3famp) . Acesso em 05 de mar. de 2022.

WHATSAPP, Segurança do WhatsApp, 2021. Disponível em: (https://www.whatsapp.com/security/?lang=pt_br). Acesso em: (15/05/2022).

WILLIAMS, Alan. Cinco boas práticas para melhorar a segurança do seu banco de dados, ORACLE BLOG BRASIL, 2019. Disponível em: (https://blogs.oracle.com/oracle-brasil/post/cinco-melhores-praticas-para-melhorar-a-seguranca-do-seu-banco-de-dados-v2). Acesso em: (18 de maio de 2022)