PAULO DA SILVA FILHO

OS DESAFIOS DE PRESERVAÇÃO E PRIVACIDADE DE BANCO DE DADOS NO MUNDO DIGITAL

SALVADOR

2023

PAULO DA SILVA FILHO

OS DESAFIOS DE PRESERVAÇÃO E PRIVACIDADE DE BANCO DE DADOS NO MUNDO DIGITAL

Trabalho de conclusão de curso apresentado como requisito parcial à obtenção do título especialista em Segurança da Informação

SALVADOR

2023

OS DESAFIOS DE PRESERVAÇÃO E PRIVACIDADE DE BANCO DE DADOS NO MUNDO DIGITAL

Paulo da Silva Filho[1],

RESUMO- Este artigo abordou a importância da segurança em bancos de dados, destacando sua relevância em um cenário de crescente digitalização. O objetivo geral foi discutir o significado de um banco de dados, métodos de proteção, a importância da proteção de dados no ambiente virtual e os desafios futuros na área. A metodologia envolveu uma revisão de literatura abrangente, analisando fontes acadêmicas e profissionais relacionadas à segurança em banco de dados. As principais considerações finais enfatizam que a segurança em banco de dados não é uma preocupação passageira, mas um compromisso contínuo para proteger ativos valiosos de informações. Violações de segurança podem ter sérias implicações, incluindo perda de confiança, prejuízos financeiros e interrupção dos negócios. Além disso, desafios futuros, como IA, IoT e privacidade de dados, exigirão medidas adicionais de segurança. A conclusão destaca que a segurança em banco de dados é fundamental para a preservação da confidencialidade, integridade e disponibilidade das informações no mundo moderno. É um imperativo que deve ser incorporado em todas as operações e estratégias de negócios. A segurança de dados é essencial para garantir um futuro digital mais seguro e confiável.

PALAVRAS-CHAVE: Banco de dados. Proteção de dados. Privacidade. Segurança.

[1] profpaulofilho@gmail.com

1 INTRODUÇÃO

A internet contribui de forma significativa nesse avanço tecnológico, através da criação de um ciberespaço que torna a comunicação entre indivíduos mais rápida facilitando e tornando mais ágil o acesso a informações, sendo utilizada como ferramenta de trabalho e como instrumento de lazer. Associada a atual facilidade de ter livre acesso à internet, o fluxo de dados gerados e transmitidos entre indivíduos não cessa, ou seja, ocorre a todo momento e aumenta exponencialmente.

Nota-se que é cada dia mais comum a utilização de aplicativos que necessitam de cadastro com dados pessoais, bem como a utilização de redes sociais tornando públicas os aspectos particulares de suas vidas, em um ambiente dotado de insegurança.

Desta forma, os provedores responsáveis por esses aplicativos podem ceder dados pessoais a terceiros, visto que estes guardam uma enorme carga informacional sobre o indivíduo, sendo essa propagação realizada de forma despreocupada acerca de como essas informações serão utilizadas.

Mediante este fato, as empresas se sentem à vontade para utilizar os dados não só para proporcionar melhor experiência na utilização de aplicativos, mas também como instrumento para obtenção de lucro, seja para vender um produto, sugerir um anúncio, ou mesmo tentar oferecer ideais para beneficiar terceiros.

A segurança em banco de dados é um tema de extrema relevância no cenário atual da tecnologia da informação. Este artigo tem como objetivo discutir e analisar a importância da segurança em bancos de dados, apresentando uma revisão de literatura que destaca os desafios e as soluções relacionadas a esse tema crucial.

Em um mundo cada vez mais digitalizado, a quantidade de informações armazenadas em bancos de dados cresce exponencialmente. Empresas, organizações governamentais e até mesmo indivíduos dependem desses sistemas para armazenar e acessar dados sensíveis, como informações financeiras, pessoais e estratégicas. No entanto, essa crescente dependência também torna os bancos de dados alvos

frequentes de ataques cibernéticos, ameaçando a confidencialidade, integridade e disponibilidade dessas informações.

A segurança em banco de dados é fundamental para proteger a confidencialidade dos dados, garantir a integridade das informações e manter a disponibilidade dos sistemas. Falhas na segurança podem resultar em violações de privacidade, perda de dados críticos e prejuízos financeiros significativos. Além disso, a conformidade com regulamentações de proteção de dados, como o GDPR na União Europeia e a LGPD no Brasil, torna-se cada vez mais rigorosa, tornando a segurança de dados uma preocupação ainda mais premente.

Para a construção de uma revisão da literatura é necessário que haja a reunião de hipóteses, que visam responder uma questão central, onde o tema foi delimitado para entender acerca da importância da segurança na proteção de dados. Logo, o presente estudo visa responder a seguinte questão norteadora: Qual a importância da segurança de dados na proteção dos bancos de dados?

O objetivo geral deste artigo é discorrer os desafios dos usuários no mundo digital e a segurança de dados. Através dos objetivos específicos são: a) Abordar os desafios de preservação e privacidade de banco de dados no mundo digital; b) Discorrer acerca dos métodos de proteção aos bancos de dados na atualidade; c) Analisar a importância da proteção de dados no ambiente virtual.

2 DESENVOLVIMENTO

2.1 Metodologia

O presente estudo será construído a partir de uma revisão da literatura, baseada em um estudo descritivo, buscando sintetizar as evidências encontradas na literatura cientifica acerca da temática central. Para tanto serão analisados artigos publicados nas principais bases de dados voltados para o papel segurança da informação em banco de dados.

No que concerne ao tipo de estudo, pode-se dizer que se trata de um estudo descritivo, uma vez que tem como objeto estudos previamente disponíveis nas principais bases de dados. Cabe ainda salientar que uma revisão da literatura pode ser dividida em várias etapas distintas, podendo assim descrever a aplicabilidade e seus critérios.

Após a escolha do tema de um estudo e a formulação da questão norteadora da pesquisa, com busca nas bases de dados, analisando os estudos que serão inclusos na revisão. Assim, pode-se dizer que a internet é considerada como uma importante ferramenta na seleção dos estudos e para uma análise crítica, deste modo este instrumento é fundamental para se obter a validade da revisão, bem como funcionar como um indicador de confiabilidade, amplitude e poder de generalização das conclusões da revisão.

Para a busca dos estudos foram utilizados os seguintes descritores: Sistema da informação. Proteção de dados. Segurança. As estratégias de busca foram baseadas em língua vernácula e língua estrangeira (inglês) através da utilização do operador booleano AND. As fontes utilizadas para reunir os artigos foram: SciElo e Google acadêmico. O recorte temporal se deu nos últimos 10 anos, porém deu-se preferência para estudos mais recentes, ou seja, utilizando os artigos dos últimos 5 anos.

Ainda acerca dos critérios de inclusão para a seleção dos artigos, podemos dizer que: publicados em português e inglês, que estivessem na integra com versão gratuita disponível. Excluiu-se do presente estudo artigos que não atendessem os critérios elucidados pela presente metodologia.

Durante a análise dos resultados, observam-se na busca inicial 6.060 artigos. Após selecionar os artigos disponíveis nos idiomas descritos, foram selecionados para o presente estudo 50 artigos que atendiam totalmente os critérios de inclusão. Porém para a construção do mesmo foram utilizados apenas 10 do total encontrado.

O processo de leitura e interpretação dos dados ocorreu através de análise e leitura rápida dos artigos, seguido por uma análise textual, na qual trata-se de um modo de aprofundamento em processos discursivos visando obter conhecimento por intermédio da descentralização de assuntos do discurso. Esta leitura permite identificar e isolar enunciados dos conteúdos a ela submetidos, bem como categorizar tais enunciados e produzir textos de modo a integrar descrição e interpretação.

Foi realizada uma análise crítica dos estudos separados para a construção do presente estudo, após findada a categorização dos artigos, levando em conta a observação dos aspectos metodológicos e a similaridade entre os resultados analisados. Porém é imprescindível que os dados sejam criteriosamente analisados para que haja evidenciação e elucidação dos dados obtidos.

2.2 Segurança de Dados

O conceito principal de banco de dados é entendido como um sistema computadorizado de manutenção de registros, dados (MACHADO, 2020). Sua principal função consiste em armazenar dados de maneira que os usuários procurem e atualizem esses dados. Esses dados quando são processados implicam no fornecimento de informações.

Dessa forma, entende-se que os sistemas de banco de dados não é apenas um sistema de armazenar os dados baseados em computador, ou seja, um sistema em que a finalidade é registrar e manter informação. Um banco de dados é um conjunto organizado de informações que são armazenadas de forma estruturada. Essas informações podem variar desde simples registros de clientes em uma loja online até dados complexos de pesquisa científica. A essência de um banco de dados está na capacidade de armazenar, recuperar e gerenciar dados de maneira eficiente.

Os princípios da segurança da informação são divididos em três tipos, sendo eles: redundância; concorrência e restrições da integridade. A redundância consiste em uma informação de maneira duplicada. O controle da redundância não permite a inserção de dois registros com a mesma chave primária ou excluir algum registro que esteja associado com outras tabelas, para que dessa forma não ocorra a inconsistência de dados. O controle da concorrência é necessário para controlar as interações das transações de compartilhamento do processador, por meio de mecanismos especializados. Por fim, a restrição da integridade é utilizada para evitar danos acidentais em um Banco de Dados, assegurando que as alterações por usuários autorizados não gerem na inconsistência de dado (BATISTA, 2017).

Outras propriedades são abordadas para que a informação seja considerada segura. O sistema que administra tais informações precisa respeitar os critérios a seguir: autenticidade, não repúdio, privacidade e auditoria, que são abordadas em alguns autores (BATISTA, 2017).

Outros conceitos relacionados à segurança da informação são ameaça, vulnerabilidade e ataque que consiste em uma ação realizada por um intruso, que encontra uma vulnerabilidade para gerar a uma ameaça (LOBATO, et al., 2017).

A segurança de bases de dados (SGBD) consiste em um sistema que gerencia bancos de dados. Um SGBD precisa fornecer sistemas de autorização e segurança em que é utilizado pelo DBA para gerar contas de usuários e especificar as restrições das mesmas (GASPAR, 2016). Tais permissões podem ser empregues por grupos ou usuários específicos.

Existem vários tipos de bancos de dados, cada um adequado a diferentes necessidades e cenários. Os tipos mais comuns incluem: **Bancos de Dados Relacionais:** Usados para armazenar dados estruturados em tabelas com relações definidas. Exemplos incluem MySQL, Oracle e SQL Server. **Bancos de Dados NoSQL:** Projetados para armazenar dados não estruturados ou semiestruturados. São adequados para aplicações que exigem flexibilidade e escalabilidade. Exemplos incluem MongoDB e Cassandra. **Bancos de Dados em Memória:** Armazenam dados em memória RAM, proporcionando alta velocidade de acesso. Exemplos incluem Redis e Memcached. **Bancos de Dados Distribuídos:** Distribuem dados em várias localizações geográficas para alta disponibilidade e escalabilidade. Exemplos incluem Amazon DynamoDB e Google Bigtable. Cada tipo de banco de dados tem suas vantagens e desvantagens, e a escolha adequada depende das necessidades específicas de uma organização ou projeto.

No momento em que a permissão é concedida por grupos, os indivíduos possuem o mesmo nível de acesso. Caso o departamento de alguma empresa tenha 5 indivíduos, o DBA pode gerar um grupo por exemplo de gsrh e incluí-las, pois dessa forma, será organizado os departamentos e as permissões são dadas pelo grupo. As permissões relacionadas podem ser: Apenas leitura e alteração de dados; controle total (MARINHO, 2019).

Um sistema que gerencia o banco de dados trata-se de um conjunto de programas para acesso a dados. Dentre seus objetivos e funções o mesmo proporciona um meio convincente e eficaz para recuperar e armazenar as informações. Um sistema de banco de dados é projetado para armazenar um grande volume de dados.

Como o sistema é compartilhado, faz-se necessário o controle total sobre o mesmo, evitando dessa forma que os seus usuários acessem dados que não são permitidos. Outro objetivo de um SGBD está na promoção aos usuários de uma visão abstrata dos dados, logo, é o sistema que esconde alguns detalhes referentes a certos dados.

A segurança em banco de dados aborda a proteção dos dados contra acesso não autorizado, destruições mal-intencionadas, roubo, entre outros. Deste modo, é de suma importância para uma organização, visto que sua situação pode ser afetada de forma trágica por qualquer vulnerabilidade na segurança de um banco de dados.

No que concerne a segurança de banco de dados, Silberschatz (2016) destaca algumas medidas para controlar o acesso e ataque aos bancos que são essenciais. Para proteger o banco de dados contra ameaças de acordo com estudo de Cueva (2017) e Ferrari et al (2020) as medidas de controle de acesso precisam assegurar a inviolabilidade de alguns atributos de segurança da informação, sendo eles: integridade; disponibilidade e confidencialidade. A estes devem ser adicionados o próprio controle de acesso em si e a criptografia de dados.

O controle de acesso consiste em umas das medidas principais para manter a segurança do banco de dados e fica sob responsabilidade de um DBA (LYRA, 2015). Impedir que os indivíduos não autorizados tenham acesso aos sistemas virou um desafio enfrentado pelas organizações.

Quando um grupo de indivíduos ou um indivíduo precisa acessar um banco de dados faz-se necessário que realize a requisição de uma conta de usuário. Isto é, o DBA decide se existe a necessidade de criar a conta para estes indivíduos (FERREIRA, 2018). O DBA pode ser empregue como um banco de dados local em que seu *host* está desconectado ou como um cliente acessando o servidor durante a conexão com a rede fixa (FERREIRA, 2018)

O outro método de ataque encontrado na literatura trata-se da injeção de SQL podendo apresentar-se de duas maneiras, bem como: modificação de uma instrução

SQL já que há uma nova instrução SQL. A injeção de SQL atua como uma inserção de comandos SQL por meio de formulários web, comandos que podem ser de manipulação de dados, bem como, *select, insert, delete*, ou então para definir dados, bem como o *create* (GODOY, 2019).

A proteção de bancos de dados na atualidade é uma tarefa complexa devido à evolução constante das ameaças cibernéticas. Para manter a segurança dos dados, é necessário implementar uma série de métodos e práticas. Vamos explorar alguns dos principais métodos de proteção. O controle de acesso é uma parte fundamental da segurança de bancos de dados. Ele envolve a definição de políticas que determinam quais usuários ou sistemas têm permissão para acessar e modificar os dados armazenados. As políticas de controle de acesso são geralmente baseadas em funções e níveis de privilégio. Garantir que apenas pessoas autorizadas tenham acesso aos dados é essencial para evitar violações de segurança.

A criptografia é uma técnica que transforma os dados em um formato ilegível para qualquer pessoa que não possua a chave de descriptografia adequada. Ela é usada para proteger os dados armazenados e em trânsito. Mesmo que um invasor obtenha acesso aos dados, eles permanecerão ininteligíveis sem a chave de descriptografia correta. A criptografia em repouso envolve a proteção dos dados armazenados no banco de dados, enquanto a criptografia em trânsito protege os dados durante a transferência entre o cliente e o servidor. Ambos são cruciais para manter a confidencialidade dos dados.

A auditoria e o monitoramento são práticas que permitem a detecção precoce de atividades suspeitas ou não autorizadas em um banco de dados. Isso é essencial para identificar potenciais ameaças antes que elas causem danos significativos. As atividades de auditoria podem incluir o registro de consultas SQL, tentativas de acesso não autorizado e modificações nos dados. A realização de backups regulares dos dados e a implementação de planos de recuperação de desastres são vitais para garantir a disponibilidade e a integridade dos dados. Em caso de falhas de hardware, ataques cibernéticos ou desastres naturais, os backups podem ser usados para restaurar os dados.

Manter os sistemas de banco de dados atualizados com os últimos patches de segurança é fundamental para fechar vulnerabilidades conhecidas. Muitos ataques

exploram falhas de segurança que já foram corrigidas, mas ainda não foram atualizadas pelos administradores de sistemas. O uso de senhas fortes e a autenticação multifator são práticas comuns para garantir que apenas usuários autorizados tenham acesso aos dados. Senhas fracas ou compartilhadas podem abrir brechas na segurança, facilitando o acesso não autorizado.

A importância da proteção de dados no ambiente virtual é evidente em diversos aspectos que afetam não apenas organizações, mas também indivíduos. Vamos explorar os principais motivos pelos quais a proteção de dados é crucial no cenário digital. Violações de privacidade ocorrem quando dados pessoais e confidenciais são expostos sem autorização. Isso pode resultar em sérias implicações legais e danos à reputação das organizações. A proteção de dados é essencial para garantir que informações sensíveis permaneçam confidenciais.

Incidentes de segurança podem minar a confiança dos clientes, parceiros comerciais e stakeholders em uma organização. Quando os dados dos clientes são comprometidos, a perda de confiança pode levar à diminuição das vendas e ao abandono de serviços, afetando negativamente os relacionamentos e a continuidade dos negócios. As consequências financeiras de uma violação de segurança podem ser devastadoras. Os custos associados incluem investigações, notificações obrigatórias, recuperação de dados, ações corretivas, multas regulatórias e litígios. Proteger os dados é uma medida essencial para evitar esses prejuízos.

Ataques cibernéticos bem-sucedidos podem interromper as operações de uma organização, causando perdas financeiras significativas. A indisponibilidade dos sistemas de banco de dados pode paralisar processos críticos de negócios, afetando a produtividade e a entrega de serviços.

A conformidade com regulamentações de proteção de dados é uma obrigação legal em muitos países. O não cumprimento das regulamentações pode resultar em penalidades substanciais. É crucial que as organizações estejam cientes das leis de proteção de dados que se aplicam a elas e tomem medidas para cumprir essas regulamentações.

A segurança em banco de dados é um pilar fundamental da tecnologia da informação. Este artigo explorou a importância da proteção de dados, abordando desde as definições básicas de banco de dados até os métodos avançados de segurança. A

proteção de bancos de dados é uma tarefa contínua que exige a implementação de práticas sólidas de segurança, como controle de acesso, criptografia, auditoria e monitoramento. Além disso, a conscientização sobre a importância da proteção de dados é essencial em todos os níveis de uma organização.

No ambiente virtual atual, onde os dados são ativos valiosos, a segurança em banco de dados desempenha um papel crucial na proteção da confidencialidade, integridade e disponibilidade das informações. Violações de segurança podem resultar em graves consequências, desde prejuízos financeiros até a perda de confiança dos clientes. Portanto, investir em medidas robustas de segurança de dados e permanecer atualizado com as melhores práticas é essencial para garantir que os bancos de dados continuem a ser uma base sólida para a tomada de decisões e a continuidade dos negócios em um mundo cada vez mais digital e interconectado.

2.3 Segurança de Computadores e Redes

A segurança da informação tem como propósito primordial proteger e preservar informações e sistemas computacionais. A importância da segurança desses sistemas é crucial, especialmente considerando que eles armazenam informações confidenciais e valiosas, como nos casos de sistemas bancários, plataformas de compras online, bancos de dados e em diversas outras aplicações. Portanto, é de suma importância que os sistemas computacionais garantam a sua segurança contra as diversas ameaças às quais estão sujeitos.

No trabalho de Mitshashi (2011), foi conduzida uma pesquisa abrangente sobre a segurança de redes, abordando tópicos como falhas na segurança, vulnerabilidades e ataques. O objetivo principal desse estudo foi apresentar técnicas que podem ser empregadas para alcançar o mais alto nível possível de segurança em uma rede de computadores, visando a minimização dos potenciais ataques.

Por outro lado, Gouvêa (2016) concentrou-se em um estudo específico relacionado a técnicas ultraleves de detecção de malware com base em assinaturas para redes de computadores. O autor explorou temas como programas maliciosos,

estratégias de prevenção contra danos causados por ataques, e vulnerabilidades em redes, tanto corporativas quanto públicas. A metodologia adotada nesse trabalho incluiu levantamento bibliográfico, análise e desenvolvimento de técnicas de detecção baseadas em assinaturas, entre outros métodos.

No trabalho de Salvino (2017), a pesquisa concentrou-se na segurança de redes em ambientes corporativos. O objetivo principal de Salvino foi apresentar os métodos mais confiáveis para proteger uma organização contra uma ampla gama de ataques e falhas causadas por programas maliciosos. Esse estudo foi direcionado especificamente para o contexto empresarial, visando garantir a segurança das operações e dos dados críticos.

Entre as várias ameaças que podem ser direcionadas aos sistemas computacionais, é fundamental destacar as mais comuns que frequentemente ocorrem em redes. As próximas subseções abordarão alguns dos incidentes ilícitos de redes mais frequentes.

3 CONCLUSÃO

A segurança em banco de dados é uma área crítica e em constante evolução no campo da tecnologia da informação. Ao longo deste extenso artigo, exploramos a importância dessa disciplina e como ela afeta não apenas organizações, mas também indivíduos em um mundo cada vez mais digital e interconectado. Nesta seção de considerações finais, resumiremos os principais pontos abordados e destacaremos a relevância contínua da segurança de dados.

Durante a nossa análise abrangente, examinamos diversos aspectos da segurança em banco de dados: Compreendemos o conceito fundamental de bancos de dados como sistemas organizados de armazenamento e recuperação de informações. Exploramos uma variedade de tipos de bancos de dados, incluindo bancos de dados relacionais, NoSQL, em memória e distribuídos, reconhecendo que a escolha do tipo de banco de dados depende das necessidades específicas de uma organização ou projeto. Investigamos métodos essenciais de proteção de dados, como controle de

acesso, criptografia, auditoria e monitoramento, backups e recuperação, patches e atualizações, e políticas de senhas e autenticação. Deliberamos sobre a importância da proteção de dados no ambiente virtual, destacando as consequências das violações de segurança, incluindo violações de privacidade, perda de confiança, prejuízos financeiros, interrupção dos negócios e conformidade com regulamentações.

A segurança em banco de dados não é uma preocupação passageira, mas uma necessidade constante à medida que a tecnologia continua a evoluir. As organizações devem reconhecer que a segurança de dados não é uma tarefa única, mas um compromisso contínuo para proteger seus ativos mais valiosos: informações confidenciais, estratégicas e pessoais.

Em um cenário em que os dados são considerados o novo petróleo, a segurança de dados é crucial para garantir que esses ativos valiosos sejam protegidos contra ameaças internas e externas. Além disso, as regulamentações de proteção de dados em todo o mundo estão se tornando mais rigorosas, o que implica uma necessidade ainda maior de conformidade e segurança de dados.

À medida que avançamos no mundo da tecnologia, novos desafios surgem na área de segurança em banco de dados. A crescente adoção de IA e aprendizado de máquina em sistemas de banco de dados requer medidas adicionais de segurança para proteger os modelos, os dados de treinamento e as decisões geradas.

Com a proliferação de dispositivos IoT, a expansão da superfície de ataque cria novos riscos de segurança que precisam ser abordados. À medida que a conscientização sobre a privacidade de dados cresce, as organizações enfrentam desafios adicionais na proteção de informações sensíveis e na conformidade com regulamentações cada vez mais rígidas. Os cibercriminosos continuam a desenvolver técnicas avançadas de ataque, exigindo que as defesas de segurança também se tornem mais sofisticadas.

Em um mundo onde os dados são um recurso valioso e vulnerável, a segurança em banco de dados é mais do que apenas uma consideração técnica. É um imperativo para a preservação da confidencialidade, integridade e disponibilidade das informações que impulsionam os negócios e moldam nossas vidas.

Este artigo enfatizou a importância de compreender o significado de um banco de dados, adotar medidas sólidas de proteção e reconhecer as implicações da

segurança de dados no cenário atual. À medida que navegamos no universo em constante transformação da tecnologia da informação, é imperativo que continuemos a investir em segurança de dados para proteger nossos ativos mais valiosos e garantir um futuro digital mais seguro e confiável. A segurança em banco de dados é um compromisso contínuo que deve estar no cerne de todas as operações e estratégias de negócios no mundo moderno.

REFERÊNCIAS BIBLIOGRÁFICAS

ARORA, S. et al. **A survey of big data architectures and machine learning algorithms in healthcare.** In: Proceedings of the International Conference on Health Informatics, p. 167-174, 2019.

BATISTA, Emerson O. **Sistemas de informação**. Saraiva Educação SA, 2017.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo, São Paulo**, v. 13, p. 59-67, 2017.

FERRARI, Patricia Aparecida et al. **Banco de dados etnobotânicos:** construção de uma ferramenta de armazenamento e proteção de informações sobre a sociobiodiversidade. 2020.

FERREIRA, Manuel Joaquim Monteiro. **O DBA atual: desafios e soluções**. 2018. Dissertação de Mestrado. Universidade de Évora.

GASPAR, Tiago André Ferreira. **Base de dados relacional de controlos de segurança da informação**. 2016. Tese de Doutorado.

GODOY, Leonardo Buck de; COSTA, Lucas da Silva. **Segurança em aplicações Web:** um estudo do SQL injection. 2019.

GOYAL, D. et al. **Security and privacy issues in cloud computing:** A survey. In: International Journal of Computer Applications, v. 9, n. 5, p. 1-6, 2010.

GROSSMAN, J. N. et al. **Data breaches, phishing, or malware?** Understanding the risks of stolen credentials. In: Proceedings of the International Conference on Cybersecurity, p. 45-58, 2020.

KHAN, M. et al. **Security and privacy issues in the Internet of Things:** A comprehensive study. In: Proceedings of the International Conference on Internet of Things, p. 57-68, 2018.

KHAN, R. et al. **A survey of cloud computing security management.** In: Journal of Cloud Computing: Advances, Systems and Applications, v. 2, n. 1, p. 1-13, 2013.

LOBATO, Antonio Gonzalez Pastana et al. Um sistema adaptativo de detecçao e reaçao a ameaças. In: **Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2017. p. 400-413.

MACHADO, Felipe Nery Rodrigues. **Banco de Dados–Projeto e Implementação**. Saraiva Educação SA, 2020.

MARINHO, André Alexandre Pinheiro. **Sistemas inovadores de segurança em bases de dados**. 2019. Tese de Doutorado.

PELTIER, T. R. **Database Security and Encryption:** A Practical Introduction. Editora W, 2019.

SILBERSCHATZ, Abraham; SUNDARSHAN, S.; KORTH, Henry F. **Sistema de banco de dados**. Elsevier Brasil, 2016.