UNIVERSIDADE ESTADUAL DO PIAUÍ

CAMPUS DRA. JOSEFINA DEMES

CURSO DE GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

CINTIA BEZERRA TEIXEIRA

SEGURANÇA EM BANCO DE DADOS: ANÁLISE DE VULNERABILIDADES E ESTRATÉGIAS DE PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

FLORIANO

2025

CINTIA BEZERRA TEIXEIRA

SEGURANÇA EM BANCO DE DADOS: ANÁLISE DE VULNERABILIDADES E ESTRATÉGIAS DE PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciências da Computação da Universidade Estadual do Piauí, como requisito parcial à obtenção do grau de bacharel em Ciências da Computação.

Orientadora: Prof. Dra. Suzana Matos de França Oliveira.

FLORIANO

2025

SEGURANÇA EM BANCO DE DADOS: ANÁLISE DE VULNERABILIDADES E ESTRATÉGIAS DE PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

Cintia Bezerra Teixeira[1], **Suzana Matos França de Oliveira**[1]

[1] Ciência da Computação – Universidade Estadual do Piauí (UESPI)
Floriano – PI – Brasil

cintiabt@aluno.uespi.br, suzana.matos@frn.uespi.br

Abstract. *This article aims to identify the main vulnerabilities in database systems and present protection strategies against cyber threats. The research adopts a systematic literature review methodology, focusing on articles published in the last five years. The results reveal that, despite technological advancements, databases are still susceptible to various risks, including attacks such as sql injection, phishing, and authentication failures. The vulnerabilities are both technical and human, with the human factor being one of the most critical points. Protection measures include the use of encryption, access control, user authentication, data masking, and secure development practices. The study reinforces the importance of security from the early stages of the system development lifecycle and the continuous adoption of protection mechanisms to ensure the integrity and confidentiality of stored information.*

Resumo. *Este artigo tem como objetivo identificar as principais vulnerabilidades em sistemas de BD e apresentar estratégias de proteção contra ameaças cibernéticas. A pesquisa adota uma metodologia de revisão sistemática da literatura, com foco em artigos publicados nos últimos cinco anos. Os resultados revelam que, apesar dos avanços tecnológicos, os Banco de Dados (BD) ainda estão suscetíveis a diversos riscos, incluindo ataques como sql injection, phishing, e falhas de autenticação. As vulnerabilidades são tanto técnicas quanto humanas, sendo o fator humano um dos pontos mais críticos. Como medidas de proteção, destacam-se o uso de criptografia, controle de acesso, autenticação de usuários, mascaramento de dados e práticas seguras de desenvolvimento. O estudo reforça a importância da segurança desde o início do ciclo de desenvolvimento de sistemas e da adoção contínua de mecanismos de proteção para garantir a integridade e a confidencialidade das informações armazenadas.*

1. Introdução

Atualmente, a tecnologia está integrada a todos os aspectos da vida cotidiana, desde instituições de ensino, empresas e bancos até sistemas de saúde, facilitando a rotina de milhões de pessoas ao redor do mundo. No passado, empresas e organizações armazenavam informações em papel, o que tornava a consulta e a organização dos dados uma tarefa lenta e complexa, além de oferecer pouca ou nenhuma segurança. Com o avanço

tecnológico, essa prática evoluiu, e hoje sistemas de Banco de Dados (BD) são amplamente utilizados para armazenar e gerenciar informações de maneira mais eficiente e segura.

Segundo Date (2004) um BD é um sistema que armazena uma coleção de registros gerenciados por um Sistema de Gerenciamento de Banco de Dados (SGBD). Esse sistema é operado por um profissional conhecido como *Database Administrator* (DBA – Administrador de Banco de Dados), cuja função é gerenciar, proteger e, se necessário, recuperar os registros. Para empresas e organizações que lidam com grandes volumes de dados, o BD é essencial, pois não só facilita o armazenamento, mas também permite a consulta, alteração e exclusão de dados. Conforme descrito por Matioli (2010) "dados", referem-se a fatos como o nome de um cliente, nome de uma rua, número de telefone, idade de uma pessoa, tamanho de uma cidade, entre outros.

Para Alves et al. (2024), a proteção da informação é um desafio que continua em transformação, visto que as ameaças evoluem na mesma velocidade que as inovações tecnológicas. Mesmo com o progresso da tecnologia e a implementação de estratégias de defesa, como barreiras de segurança e codificação de dados, o comportamento e as escolhas dos usuários seguem sendo um fator relevante de fragilidades. Por esse motivo, é frequente que criminosos virtuais, ao conduzirem suas investidas, comecem explorando a brecha mais vulnerável: o elemento humano. Reforçando essa ideia, Pollini et al. (2022) e Kobis (2021), destacam que o elemento humano é amplamente reconhecido como o ponto mais vulnerável dos sistemas de informação. A maioria dos ataques a sistemas ocorrem por meio de ações humanas, o que torna os humanos fontes críticas que acometem a eficácia de proteção desses sistemas.

Nesse contexto, Wang (2008), define o termo "elemento humano" como as atividades desempenhadas por pessoas dentro de um sistema. No âmbito da tecnologia da informação, isso significa que o indivíduo atua como peça central do sistema e impacta diretamente o grau de proteção. Se os usuários estiverem bem preparados e cientes dos riscos, poderão contribuir positivamente para reforçar a segurança do ambiente digital.

Apesar do avanço da tecnologia de segurança, os ataques e as vulnerabilidades ainda continuam, o que tornam os sistemas suscetíveis a riscos significativos. De acordo com Matioli (2010), o BD deve assegurar a integridade dos dados, restringir o acesso de usuários não autorizados e garantir a recuperação das informações. Com isso, este trabalho tem como objetivo identificar as principais vulnerabilidades presentes em BD, mostrar a importância da segurança para garantir a integridade dos dados e o acesso restrito a usuários autorizados. Para isso, será realizada uma revisão sistemática de literatura, que permitirá identificar, analisar e sintetizar os estudos mais relevantes sobre o tema. Contudo, ao longo do desenvolvimento deste trabalho, foram identificados estudos cujas abordagens se mostraram divergentes do escopo estabelecido, especialmente por abordarem métodos e técnicas que não serão objeto de análise nesta pesquisa.

As próximas seções deste trabalho estão organizadas da seguinte forma: a Seção 2 apresenta a fundamentação teórica, na qual são discutidos os principais conceitos e estudos relacionados ao tema; a Seção 3 expõe a metodologia adotada, com ênfase na execução do mapeamento sistemático da literatura; a Seção 4 contempla a exposição dos resultados obtidos, acompanhada de suas respectivas análises e discussões; Por fim, a

Seção 5 apresenta as conclusões deste trabalho, destacando as principais contribuições e limitações.

2. Fundamentação Teórica

Segundo Date (2004), um BD é um conjunto integrado de informações que consolida e organiza diversos arquivos distintos, evitando redundâncias e otimizando o gerenciamento de dados. Os usuários desse sistema, realizam diversas operações que consistem em: acrescentar novos arquivos ao BD, inserir dados em arquivos já criados, buscar informações nos registros, excluir dados de documentos armazenados no BD, realizar alterações em conteúdos previamente salvos e remover itens presentes no sistema.

Para Matioli (2010), essa integração permite que diferentes departamentos compartilhem o acesso às informações, de maneira controlada e estruturada. A administração eficiente do BD é realizada por DBAs, profissionais altamente especializados responsáveis por garantir que o sistema opere de forma eficiente, confiável e livre de falhas. Dependendo da complexidade e do tamanho do BD, pode haver equipes de administradores para gerenciar e distribuir responsabilidades. No contexto de segurança, o SGBD desempenha um papel central ao implementar mecanismos que protegem os dados contra acessos não autorizados. Ele permite aos DBAs criar contas de usuários, definir restrições e gerenciar privilégios, limitando o acesso apenas ao necessário para cada usuário. Esses privilégios são essenciais para prevenir abusos, como alterações indevidas em dados sensíveis, como informações financeiras. Além disso, SGBDs modernos incluem funcionalidades robustas, como autenticação de usuários, auditorias de acesso e definições de níveis de autorização, protegendo a base de dados mesmo em ambientes inseguros.

De acordo com Iqbal et al. (2023), um ataque a BD é definido como um incidente que compromete um recurso ao modificar ou eliminar dados essenciais. O objetivo principal dos ataques a BD é obter acesso a informações sensíveis. A obtenção não autorizada de dados privados, como informações de cartões de crédito, contas bancárias e identificadores pessoais, também é uma motivação comum para os ataques a BD. Para mitigar esses riscos, métodos eficazes de criptografia devem ser aplicados para garantir a proteção dos BDs. Entre os modelos mais robustos de segurança de BD está o modelo multinível, que organiza informações com base em seus níveis de confidencialidade e utiliza o controle de acesso obrigatório (MAC). Além disso, serviços de BDs desempenham um papel crucial na segurança, ao implementar técnicas como *backup* e recuperação para proteger os dados dos clientes. Na construção desse sistema, é imprescindível priorizar a segurança como o objetivo principal durante o desenvolvimento de sistemas de dados. Nesse sentido, a segurança deve ser abordada em todas as etapas do ciclo de desenvolvimento de software, garantindo a criação de sistemas mais resilientes.

Segundo Marques e Cruz (2021), para proteger os sistemas contra ameaças, três tipos principais de medidas podem ser implementados: controle de acesso, controle de fluxo e criptografia. O controle de acesso é realizado por meio da criação de contas de usuário e senhas, permitindo ao SGBD gerenciar o processo de *login*. Quando uma pessoa ou grupo necessita acessar o BD, torna-se imprescindível solicitar uma conta de usuário. Nesse contexto, o DBA decide sobre a necessidade de criação dessa conta. Para os autores, o controle de fluxo visa impedir que informações sejam direcionadas a usuários não autorizados. Para isso, são analisados os canais por onde os dados transitam, regu-

lando o fluxo e a distribuição de informações entre os objetos acessíveis. A criptografia é utilizada para proteger informações confidenciais, como números de cartões de crédito, especialmente em transmissões por redes de comunicação. Além disso, é empregada para impedir que usuários não autorizados acessem partes sensíveis de um BD, codificando os dados e dificultando sua decodificação por terceiros. Entre as estratégias para segurança de dados, a criptografia se destaca como uma solução eficaz para armazenar ou transmitir informações de forma protegida. Mesmo em caso de invasão ou acesso não autorizado, dados criptografados apresentam obstáculos para a interpretação, sendo compreensíveis apenas por usuários previamente autorizados. Para acessar os dados originais, é indispensável a aplicação de um algoritmo de descriptografia.

Para Americo (2022), vulnerabilidade é uma falha encontrada no *software*, que pode ser explorada por um invasor que tem como propósito ultrapassar as camadas de segurança de um sistema. O autor ressalta que apenas as vulnerabilidades existentes no *software* não causam danos, pois é preciso que um invasor cometa um ataque dentro da aplicação, quebrando uma ou mais camadas de proteção do sistema, e tendo assim acesso as informações do sistema, de modo que comprometa os dados. Uma boa prática ainda segundo o autor, é comunicar a empresa responsável pelo *software* das vulnerabilidades existentes no sistema, para que possa ser corrigidas.

Os ataques que podem ser realizados em um sistema são classificados em duas categorias principais (AMERICO, 2022): engenharia social, na qual o invasor busca enganar a vítima de alguma forma, podendo se passar por outra pessoa por meio de ligações telefônicas, com o objetivo de obter informações pessoais e confidenciais; e *phishing*, em que o atacante envia um e-mail à vítima, fingindo representar uma instituição legítima, solicitando dados pessoais ou induzindo o acesso a uma página web fraudulenta, cujo endereço URL difere do site oficial. Além disso, o autor ressalta a existência de ataques realizados por meio da instalação de códigos maliciosos no computador da vítima, sendo esse tipo de ameaça conhecido como *malware*.

Uma das causas das vulnerabilidades que podem ser exploradas por invasores nos sistemas está relacionada aos programadores, onde os códigos são escritos sem a aplicação das boas práticas de programação, fazendo assim com que o sistema apresente vulnerabilidades que podem ser exploradas por um invasor (AMERICO, 2022).

Segundo Silberschatz (2020), ao criar um BD, é fundamental considerar a proteção das informações desde o início. Isso envolve garantir a autenticação dos usuários e limitar o acesso às funções autorizadas para cada indivíduo. O autor também destaca a existência de diversas ameaças à segurança das aplicações, como os ataques de *sql injection*, nos quais comandos maliciosos são executados de forma a manipular o sistema. Esses ataques podem ter consequências graves, permitindo ao invasor burlar as camadas de segurança e realizar operações críticas no BD. Como forma de prevenção, recomenda-se a utilização de comandos projetados especificamente para consultas SQL. Americo (2022) define que as informações não seguras são obtidas por meio do navegador e inseridas por indivíduos que buscam iludir o interpretador para executar comandos não autorizados ou viabilizar o acesso a sistemas sem deter credenciais apropriadas, permitindo a leitura, geração, alteração ou remoção de dados no banco de informações.

3. Metodologia

Esta seção tem como objetivo apresentar, de forma detalhada, os procedimentos adotados para a realização deste trabalho.

3.1. Definição das Bases de Dados

A pesquisa foi conduzida por meio de consultas em três bases de dados acadêmicas: IEEE Xplore[1], SciELO[2] e Scopus[3].

3.2. Definição dos Termos de Buscas

Os termos selecionados para compor a *string* de busca foram definidos com base no objetivo principal deste trabalho, que se concentra na análise de segurança em BD. Para isso, foram utilizados termos como "segurança em BD" e "ataques SQL", tanto em português quanto em inglês, visando ampliar o escopo dos resultados obtidos.

3.3. Definição da String de Busca

Nesta etapa, as buscas foram realizadas nas bases de dados previamente mencionadas, com ajustes progressivos na construção da *string* de busca a cada iteração, de forma a refinar os resultados obtidos. Para garantir a relevância dos estudos identificados, foram considerados apenas aqueles cujos títulos apresentavam relação direta com o tema deste trabalho. O operador booleano "AND" foi empregado para conectar os termos principais e seus correlatos, assegurando maior precisão na filtragem dos dados. Em cada uma dessas bases, foram utilizadas palavras-chave e *strings* de busca especificas, tais como:

- ("security") AND ("vulnerability") AND ("database");
- ("sql injection") AND ("attack") AND ("database");

3.4. Critérios de Inclusão e Exclusão

Em todas as bases consultadas, foram aplicados critérios de inclusão e exclusão. Para inclusão, foram selecionados artigos publicados nos últimos cinco anos, com temática diretamente relacionada ao objetivo deste trabalho e escritos nos idiomas inglês ou português.

Como critérios de exclusão, foram desconsiderados os trabalhos que propunham métodos específicos de identificação de ataques a bancos de dados, por não se alinharem ao foco desta pesquisa, bem como aqueles que não demonstravam aderência ou relevância ao tema central do estudo. Por exemplo, foram excluídos artigos que tratavam da detecção e prevenção de ataques cibernéticos a bancos de dados quando baseados em abordagens como aprendizado de máquina ou o uso de inteligência artificial, por se distanciarem do escopo estabelecido nesta investigação. Foram também descartados estudos que focavam exclusivamente em ataques de engenharia social, temática que não integra o escopo deste trabalho. Ademais, foram eliminadas duplicatas, ou seja, publicações idênticas recuperadas em mais de uma base de dados.

[1]https://ieeexplore.ieee.org
[2]https://www.scielo.org
[3]https://www.scopus.com

3.5. Extração dos Dados

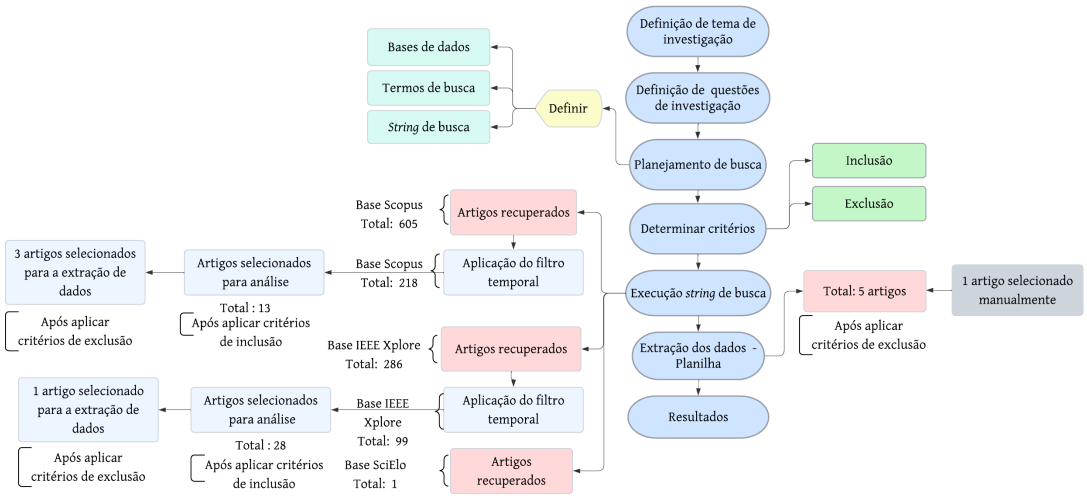
Para cada artigo selecionado, foram extraídas as seguintes informações: título do artigo, nomes dos autores, ano de publicação e objetivo do estudo. Esses dados foram organizados de forma estruturada em uma tabela no Excel, possibilitando uma análise detalhada e sistemática.

4. Resultados

Esta seção tem como finalidade apresentar os resultados obtidos por meio de uma revisão sistemática da literatura, realizada com foco no tema central deste trabalho. Os dados coletados foram posteriormente analisados com o objetivo de identificar desafios associados à segurança em BD e as principais vulnerabilidades. A análise incluiu a categorização dos estudos selecionados com base nos temas abordados, proporcionando uma visão abrangente do estado atual da pesquisa na área.

Foram utilizadas três bases de dados acadêmicas para a realização da pesquisa: IEEE Xplore, Scopus e SciELO. Dentre elas, a base IEEE Xplore foi a que apresentou o maior número de resultados, seguida pela Scopus e, por fim, pela SciELO. A Figura 1 apresenta graficamente os dados de busca, filtragem e seleção dos artigos nas bases consultadas.

Figura 1. Processo de seleção e filtragem dos artigos utilizados na pesquisa



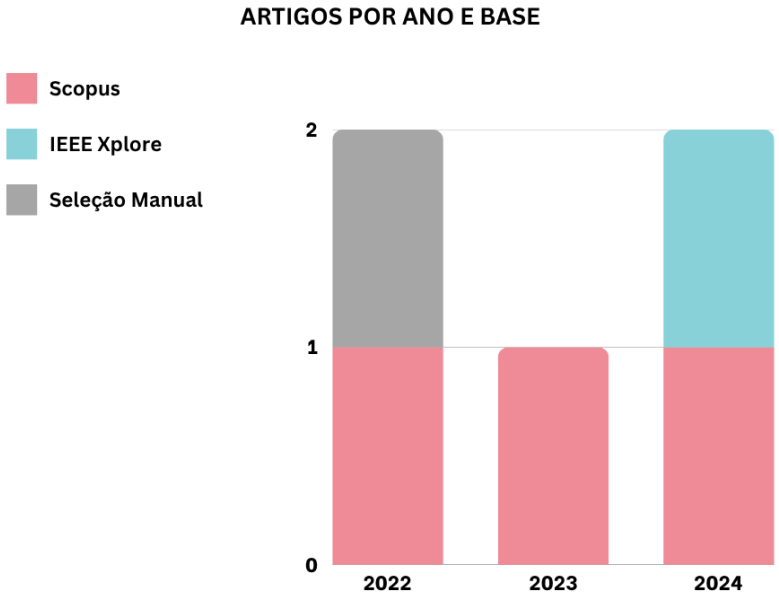
Fonte: Elaborado pela autora.

Na base Scopus, foram inicialmente recuperados 605 artigos sem a aplicação de filtros. Após a aplicação do filtro temporal, restringindo os resultados ao período de 2021 a 2025, restaram 218 artigos, dos quais apenas 13 foram selecionados para análise por atenderem aos critérios de inclusão definidos neste trabalho. No IEEE Xplore, a busca inicial retornou 286 artigos; após a aplicação do mesmo filtro temporal, restaram 99, sendo 28 deles incluídos na análise por atenderem aos critérios de inclusão. A base SciELO retornou apenas um artigo, que não foi incluído na análise por não apresentar aderência ou relevância com o tema deste trabalho. A tabela completa está disponível em formato Excel. (Link para a planilha.)

Ressalta-se que a *string* de busca foi elaborada e aplicada no idioma inglês, resultando exclusivamente em artigos também redigidos nesse idioma. A tentativa de execução da mesma *string* em português não retornou resultados nas bases consultadas. Dessa forma, todos os artigos selecionados para a análise encontram-se escritos em inglês.

Foram selecionados cinco artigos para a síntese dos dados, dos quais três são provenientes da base Scopus, um da base IEEE Xplore e um foi incluído por seleção manual. Este último não se encontrava nas bases mencionadas, tendo sido identificado fora delas durante o processo de solicitação de um dos artigos previamente selecionados nas bases. A Figura 2 apresenta os anos de publicação dos respectivos artigos sintetizados.

Figura 2. Quantidade de artigos por ano



Fonte: Elaborado pela autora.

A partir deste ponto, serão detalhados os resultados extraídos dos artigos que abordaram as questões de investigação propostas nesta pesquisa.

Q1. Quais as principais vulnerabilidades presentes em BD?

Conforme Almaiah et al. (2024), os riscos cibernéticos potenciais que podem tirar proveito das falhas existentes em um BD são divididos em duas categorias, sendo: riscos técnicos e riscos não técnicos. Ainda segundo o autor, os riscos técnicos são:

- *Phishing:* É empregado como um método para capturar credenciais do sistema visando obter vantagens financeiras.
- Tentativas de invasão: Esse tipo de ameaça acontece quando indivíduos mal-intencionados tentam ultrapassar as barreiras de proteção existentes no BD para conseguir acesso não autorizado ao sistema.
- Ataques *sql injection:* O atacante insere comandos SQL maliciosos em campos de Entrada ou consultas do usuário para manipular o sistema; esse tipo de ataque pode fornecer aos invasores acesso restrito ao BD.
- Exploração de falhas: Ocorre quando o sistema não recebe as atualizações necessárias para corrigir falhas conhecidas, o que pode aumentar a chance de

ocorrências maliciosas.

- Concessão indevida de permissões: A atribuição exagerada de permissões a usuários ou a não revogação de acessos de ex-colaboradores representa um risco, já que esses usuários podem utilizar tais acessos para objetivos maliciosos. Para Almaiah et al. (2024), permissões excessivas constituem uma ameaça relevante à segurança em BD. Usuários autorizados podem utilizar dados de forma indevida, comprometendo a integridade e a confidencialidade do sistema. Aproximadamente 80% dos ataques a dados corporativos são provocados por antigos funcionários que ainda detêm privilégios de acesso ou pelos atuais (ABDULLAYEV; CHAUHAN, 2023).
- Exposição de cópias de segurança: Dispositivos físicos de *backup*, como fitas e discos, caso não sejam armazenados em locais protegidos e monitorados, podem ter seus dados acessados indevidamente.

As ameaças não técnicas aos sistemas de BD estão diretamente relacionadas a fatores humanos, que podem ser explorados para comprometer a segurança das informações. Uma das principais fragilidades nesse contexto é a autenticação deficiente, a qual permite que indivíduos não autorizados assumam a identidade de usuários legítimos. Essa vulnerabilidade pode ser explorada por meio de ataques de força bruta e técnicas de engenharia social. A seguir, as ameaças não técnicas serão discutidas com base na abordagem apresentada pelo autor.

- Riscos internos: Usuários com acesso a dados confidenciais podem utilizá-los de forma inadequada. Algumas práticas incluem copiar arquivos para dispositivos USB *(Universal Serial Bus)*, enviar dados sensíveis por e-mail para contas pessoais ou compartilhar credenciais com pessoas não autorizadas.
- Falhas humanas: A exposição não intencional de informações sensíveis, e-mails enviados para destinatários incorretos e o vazamento acidental de credenciais de acesso.
- Identificação equivocada: Esse problema ocorre quando usuários não autorizados são erroneamente reconhecidos como legítimos dentro do sistema, ou o caso inerso, em que usuários legítimos não são identificados como autorizados.
- Engenharia social: Esse tipo de risco explora a tendência das pessoas a confiarem umas nas outras, com o objetivo de obter dados sigilosos, como nomes de usuário e senhas, para conseguir acesso ao BD.

De acordo com o autor, as fragilidades mais recorrentes encontradas em um BD são organizadas em vinte categorias principais, sendo elas: autenticação insuficiente, terceiros não confiáveis, concessão indevida de acesso a terceiros, falhas de *software*, BD desatualizado, práticas de programação inseguras, mecanismos de proteção deficientes, registro de auditoria limitado, conhecimento e capacitação em segurança reduzidos, informações sensíveis não controladas, rede vulnerável, uso inadequado de senhas, falhas na plataforma, dificuldades de integração, complexidade na administração, técnicas de criptografia fracas, mascaramento de dados ineficiente, reutilização de contas, baixa conscientização sobre segurança e gestão de chaves ineficaz (ALMAIAH et al., 2024).

Conforme Basilio e Oliveira (2022), em diversas aplicações — sejam elas páginas web, aplicativos, sistemas operacionais ou quaisquer outros tipos de programas — as

mensagens de erro não são tratadas adequadamente. Para ataques de *sql injection*, isso representa uma grave vulnerabilidade, pois agentes mal-intencionados com habilidade para interpretar a lógica, trechos de código, variáveis, dados ou outras informações contidas na mensagem de erro, podem explorá-las para obter maior compreensão sobre os dados armazenados.

Q2. Qual é a importância da segurança para assegurar a integridade dos dados e o acesso restrito apenas a usuários autorizados?

Aplicações web que não utilizam mecanismos apropriados de validação de entrada e segurança na comunicação com o BD por meio da linguagem de consulta estruturada (SQL) tornam-se suscetíveis a ataques de *sql injection*, os quais podem provocar consequências severas no sistema, desde a exposição de informações confidenciais até o comprometimento total da estrutura (NAGUIB; FOUAD, 2024).

Conforme Abdullayev e Chauhan (2023), antes que uma aplicação realize o processamento dos dados fornecidos pelo usuário, é necessário que esses dados passem inicialmente por um processo de verificação de entrada. Um possível indício de um ataque de *sql injection* é a presença de determinados caracteres ou termos-chave. Segundo o mesmo autor, o uso de instruções SQL pré-compiladas e armazenadas no BD constitui uma forma adicional de proteção contra ataques desse tipo, podendo também ser empregadas para executar operações complexas no ambiente do BD.

De acordo com Naguib e Fouad (2024), é essencial que as organizações implementem e mantenham práticas de segurança nos BD com o objetivo de resguardar não apenas informações confidenciais, mas também de preservar a confiança de seus *stakeholders*. De acordo com o autor, as soluções voltadas à proteção de BD são imprescindíveis para garantir a segurança de dados sensíveis e preservar a integridade dos sistemas corporativos. Tais medidas são fundamentais para mitigar o risco de acessos não autorizados, violações de dados e outras ameaças à segurança da informação. O autor define as soluções como:

- Criptografia: Um dos principais benefícios da criptografia é a camada adicional de proteção que ela proporciona aos dados, dificultando significativamente o acesso por indivíduos não autorizados, uma vez que as informações criptografadas tornam-se ininteligíveis sem a devida autorização. A criptografia pode ser aplicada a diferentes tipos de dados, como e-mails, arquivos, BD e canais de comunicação, assegurando a proteção tanto de dados armazenados quanto em trânsito (em transferência pelo sistema).
- Controles de acesso: Esse recurso possibilita às organizações limitar o acesso a informações, sistemas e recursos sensíveis exclusivamente a usuários devidamente autorizados, por meio da definição de diferentes níveis de permissão conforme o perfil do usuário ou departamento. Além disso, permite restringir o acesso a locais ou dispositivos específicos e possibilita o monitoramento das ações dos usuários, identificando comportamentos suspeitos, como tentativas de acesso fora do horário comercial ou a partir de locais incomuns.
- Identificação/Autenticação de usuários: Conhecer a identidade dos usuários é um requisito indispensável para garantir a segurança de um sistema. Assim, a existência de um processo eficaz de autenticação e identificação é essencial para assegurar que apenas indivíduos autorizados tenham permissão de acesso aos dados.

- Mascaramento: O mascaramento de dados em BD é uma das estratégias fundamentais de proteção. Essa técnica consiste em ocultar ou modificar informações específicas, de forma a impedir que sejam acessadas por usuários não autorizados. O mascaramento protege tanto os dados armazenados quanto os em trânsito.

De acordo com Abdullayev e Chauhan (2023), existem diversas técnicas preventivas contra ataques de *sql injection*, incluindo métodos que asseguram a validação correta dos dados fornecidos pelos usuários e a execução segura de comandos SQL. Em sua pesquisa, o autor destaca três métodos de prevenção contra esse tipo de ataque: validação de entrada, consultas parametrizadas e procedimentos armazenados. A seguir, são apresentadas essas abordagens, segundo o autor:

- Validação de entrada: Este método busca garantir que os dados inseridos pelo usuário sejam verificados conforme critérios preestabelecidos, assegurando que possam ser processados adequadamente pelo sistema. Seu principal objetivo é evitar que comandos maliciosos sejam enviados ao BD como parte de uma consulta SQL. A validação inclui a verificação do tipo dos dados (por exemplo, números ou cadeias de caracteres) e pode também identificar caracteres ou termos suspeitos que indiquem uma tentativa de ataque.
- Consultas parametrizadas: Este método promove a execução segura de instruções SQL ao separar os parâmetros da consulta principal. Ao eliminar a possibilidade de o invasor inserir código malicioso diretamente na consulta, essa técnica previne de forma eficaz ataques de *sql injection*.
- Procedimentos armazenados: Esse recurso consiste em comandos SQL previamente compilados e mantidos no BD. Essa abordagem dificulta a inserção de código malicioso por parte de invasores, pois a execução ocorre diretamente no servidor do BD, e não no servidor web.

Conforme Almaiah et al. (2024), em seu estudo identificou diferentes mecanismos de controle de segurança desenvolvidos para fortalecer a proteção dos sistemas de BD frente a ataques cibernéticos, entre os quais se destacam: backup de dados, monitoramento de comportamentos, detecção de spam, auditorias de segurança e técnicas de identificação de anomalias, entre outros.

Segundo Hallo e Suntaxi (2021), ataques do tipo *sql injection* podem comprometer o sistema de BD de diversas maneiras. Esses ataques permitem que agentes mal-intencionados modifiquem dados confidenciais, afetando a integridade do sistema, ou acessar informações sensíveis, afetando a confidencialidade do mesmo. As autoras também discutem diversas estratégias desenvolvidas para lidar com esse tipo de ameaça, as quais serão exploradas a seguir.

- Amnesia: Trata-se de uma abordagem automatizada, que combina técnicas dinâmicas e estáticas para identificar e impedir vulnerabilidades em aplicações web durante sua execução. Esse método reconhece comandos inválidos antes de sua execução na aplicação.
- Prevenção SQL: Esta abordagem consiste em um interceptador de requisições HTTP, no qual a aplicação web envia os comandos SQL para um módulo de detecção de *sql injection*, que realiza a verificação das instruções e identifica possíveis códigos maliciosos.

- SQLCheck: Esse método examina a estrutura da consulta antes e depois do acesso do usuário ao sistema, a fim de identificar automaticamente padrões anômalos em SQL.
- Verificador de Tautologia: Esse método monitora as entradas do sistema e avalia os valores dos atributos informados, verificando se um dado atributo é válido ao compará-lo com os valores de um modelo predefinido. Essa técnica é voltada exclusivamente para detectar ataques do tipo tautologia, nos quais se inserem expressões logicamente sempre verdadeiras.
- Contaminação Positiva: Esse método protege sistemas web contra ataques de *sql injection* ao identificar *strings* confiáveis originadas da aplicação, permitindo assim a construção segura das consultas SQL.
- WAVES: Técnica de análise caixa-preta que realiza testes de *sql injection* em aplicações web com o objetivo de identificar falhas de segurança existentes.
- CANDID: Essa abordagem monta automaticamente a estrutura de uma consulta com base nas entradas fornecidas pelos usuários, decidindo se determinada entrada representa uma ameaça.
- SQLIMW: Método voltado à prevenção de ataques baseados em *middleware*, impedindo ataques de *sql injection* na comunicação entre programador e servidor. Utiliza ainda técnicas de criptografia para reforçar a segurança em aplicações web.
- SQLIPA: Essa técnica utiliza funções *hash* como mecanismo de validação durante a autenticação de usuários no sistema.
- Avaliação de String Sensível ao Contexto (CSSE): Método de detecção e defesa contra *sql injection* que converte metadados para as entradas dos usuários e realiza uma análise contextualizada dessas *strings*.

Conforme Basilio e Oliveira (2022), a auditoria em BD pode ser efetuada de duas maneiras: abordagem convencional e eliminação de riscos. Ainda de acordo com o autor, a abordagem convencional realiza uma análise detalhada da estrutura do BD, das informações nele contidas, das diretrizes do banco e da organização, e com o suporte de um *checklist* é feita uma inspeção em busca de falhas e brechas. Por sua vez, a eliminação de riscos procura avaliar o controle das vulnerabilidades e realizar uma avaliação para aplicar a medida mais eficaz alcançada para cada propósito, não se restringindo apenas a um método, podendo empregar estratégias corretivas ou preventivas. Ainda segundo o autor, as atualizações de *software* são importantes para todo o cenário da segurança, pois visam corrigir falhas e promover melhorias de forma geral. No que diz respeito a ataques de *sql injection*, as atualizações tornam-se fundamentais, pois tendem a mitigar brechas e vulnerabilidades encontradas em versões anteriores.

5. Conclusão

Com o avanço constante da tecnologia, é essencial que empresas e organizações façam bom uso das inovações, principalmente no que diz respeito ao armazenamento de grandes volumes de dados, que são gerenciados por sistemas de BD. Esses sistemas precisam ser bem protegidos e resistentes a ataques cibernéticos, pois falhas na segurança podem causar grandes prejuízos. Diante desse cenário, é fundamental entender quais são as principais ameaças que afetam os BD e conhecer estratégias eficazes para reduzir seus impactos. Este trabalho utilizou como metodologia uma revisão sistemática da literatura,

com foco em identificar vulnerabilidades comuns e as formas mais eficientes de proteger os dados, garantindo que apenas usuários autorizados tenham acesso.

A revisão sistématica seguiu os passos: a escolha de bases de dados confiáveis (IEEE Xplore, Scopus e SciELO), a definição dos termos e combinações de busca em português e inglês, a aplicação de critérios de inclusão e exclusão (como o recorte temporal de cinco anos), e a organização dos dados dos artigos selecionados em uma planilha. A partir dessa análise, foi possível destacar os principais riscos aos BD, como ataques de *sql injection*, falhas de autenticação, permissões mal configuradas e ausência de criptografia. Também foram identificadas soluções importantes, como validação de dados, uso de criptografia, controle de acesso baseado em papéis e registro de atividades no sistema. Além disso, observou-se que o fator humano tem grande influência na segurança dos sistemas. Por isso, é necessário investir em treinamentos e na conscientização dos usuários.

Este estudo, portanto, oferece um panorama atual das ameaças aos BD e das boas práticas de segurança que podem ser adotadas. Como sugestão para trabalhos futuros, seria interessante explorar ferramentas automáticas para detectar falhas em tempo real e avaliar como essas estratégias funcionam na prática, em ambientes corporativos variados.

Referências

ABDULLAYEV, V.; CHAUHAN, A. S. *SQL Injection Attack: Quick View*. [S.l.]: Mesopotamian Academic Press, 2023. 30-34 p. 8, 9, 10

ALMAIAH, M. A. et al. Classification of cybersecurity threats, vulnerabilities and countermeasures in database systems. *Computers, Materials and Continua*, Tech Science Press, v. 81, p. 3189–3220, 2024. ISSN 15462226. 7, 8, 10

ALVES Ângela R. N. et al. Fator humano na segurança da informação: um mapeamento dos comportamentos de risco no ambiente digital. *Texto Livre*, Belo Horizonte-MG, v. 17, p. e51184, 2024. 2

AMERICO, W. M. *Segurança em desenvolvimento de sistemas web*. Monografia (Graduação em Tecnologia em Segurança da Informação) — Faculdade de Tecnologia de Americana "Ministro Ralph Biasi", 2022. 4

BASILIO, G. M.; OLIVEIRA, W. D. Segurança em banco de dados: Análise de vulnerabilidades e ferramentas de proteção contra injeção sql. *RBTI - Revista Brasileira em Tecnologia da Informação*, Campinas, n. 10, 2022. 8, 11

DATE, C. J. *Introdução a Sistemas de Banco de Dados*. 8. ed. Rio de Janeiro: Elsevier Editora, 2004. 1–1623 p. ISBN 9788535284454. 2, 3

HALLO, M.; SUNTAXI, G. A survey on sql injection attacks, detection and prevention techniques-a tertiary study. *International Journal of Security and Networks*, 2021. 10

IQBAL, A. et al. Advancing database security: a comprehensive systematic mapping study of potential challenges. *Wireless Networks*, Springer, 10 2023. ISSN 15728196. 3

KOBIS, P. Human factor aspects in information security management in the traditional it and cloud computing models. *Operations Research and Decisions*, Wrocław University of Science and Technology, v. 31, p. 61–76, 2021. ISSN 23916060. 2

MARQUES, G. F.; CRUZ, R. C. C. Importância da segurança em banco de dados. *Revista Eletrônica da Faculdade Invest de Ciências e Tecnologia*, 2021. 3

MATIOLI, D. C. *Importância da Segurança em Banco de Dados*. 1-55 p. Monografia (Monografia) — FEMA - Fundação Educacional do Município de Assis, 2010. 2, 3

NAGUIB, A.; FOUAD, K. M. Database security: Current challenges and effective protection strategies. In: *Proceedings of the 6th International Conference on Computing and Informatics (ICCI)*. [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2024. p. 120–130. 9

POLLINI, A. et al. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology and Work*, Springer Science and Business Media Deutschland GmbH, v. 24, p. 371–390, 5 2022. ISSN 14355566. 2

SILBERSCHATZ, A. *sistema de banco de dados*. sétima. [S.l.]: LTC, 2020. 4

WANG, Y. On cognitive properties of human factors and error models in engineering and socialization. *International Journal of Cognitive Informatics and Natural Intelligence (IJCINI)*, 2008. 2