Banco De Dados: Um Estudo Sobre A Segurança Da Informação

Autor(res)

Aléssio Adrian Chiuratto
Anderson Doniseti De Araujo

Categoria do Trabalho

Trabalho Acadêmico

Instituição

FACULDADE ANHANGUERA DE ITAPETININGA

Introdução

A segurança, por definição, refere-se à ação de tornar algo seguro, enquanto informação é entendida como conhecimento ou notícia. Quando unidas no contexto de Segurança da Informação, essas palavras abordam a proteção de dados contra ameaças, garantindo autenticidade, confidencialidade, confiabilidade e privacidade. O problema da pesquisa é: “Qual a importância da Segurança da informação nos bancos de dados?” Para respondê-lo, será realizada uma pesquisa literária, abordando conceitos, origem e relevância da Segurança da Informação e dos Bancos de Dados.
A segurança da informação é um direito de todas as pessoas e entidades, independentemente de classe social, gênero ou finalidade do dado. Cada informação deve ser protegida, seja de caráter pessoal, profissional, público ou histórico. Organizações utilizam políticas de segurança para resguardar dados, desde transações financeiras até informações confidenciais, prevenindo modificações indevidas e usos incorretos.
O objetivo geral deste estudo é demonstrar a importância da tecnologia da informação na proteção de dados. Os objetivos específicos incluem:
Explicar a origem e conceito de Bancos de Dados;
Compreender aspectos da Segurança de dados digitais;
Discutir a relevância da proteção da informação.
Apesar dos avanços tecnológicos, transações de informações ainda são vulneráveis, seja por falhas de sistemas, programas ou ação de hackers. A proteção de dados é essencial para que transações sejam realizadas com segurança, especialmente em ambientes digitais, como e-mails, aplicativos, sites e caixas eletrônicos.
Embora a evolução tecnológica proporciona facilidades, a segurança não é automática. A criação de leis como a LGPD reforça a necessidade de proteção legal dos dados. A metodologia adotada consiste em uma revisão literária, baseada em livros, artigos científicos e materiais online sobre Tecnologia da Informação, Segurança da Informação e Bancos de Dados, abrangendo publicações de 2005 a 2019.

Objetivo

O objetivo geral deste conteúdo foi mostrar como a tecnologia da informação é um elemento importante, enquanto que seus objetivos específicos tratam de explicar a origem e conceito de Banco de Dados, entender o aspecto de Segurança de Dados Digitais e discutir a relevância de se proteger os dados.

Material e Métodos

A metodologia aplicada neste conteúdo foi cuidadosamente planejada e executada visando garantir a qualidade e a confiabilidade do material apresentado. Para isso, foi realizada uma revisão bibliográfica extensiva, envolvendo a pesquisa em diversas fontes de renome, como publicações científicas, livros especializados e periódicos acadêmicos.

A seleção das obras utilizadas como base para o conteúdo abrangeu o período de 2005 a 2014, com o intuito de abordar tanto os conceitos e fundamentos consolidados da área quanto eventuais avanços e mudanças ocorridos nesse intervalo de tempo. Além disso, foram coletados materiais atualizados em sites especializados e plataformas online, que abrangem o período de 2017 a 2019, para incluir as mais recentes tendências e desenvolvimentos nessas áreas.

Para assegurar a qualidade e a relevância dos materiais selecionados, foram adotados critérios rigorosos de escolha, considerando a experiência e a expertise dos autores das obras, bem como a consistência e a atualidade dos dados apresentados. Dessa forma, busca-se proporcionar aos leitores uma visão abrangente e atualizada sobre os temas abordados.

Por meio dessa metodologia, embasada em pesquisas atualizadas e reconhecidas, busca-se fornecer aos leitores informações precisas, confiáveis e de qualidade, contribuindo para ampliar o conhecimento nas áreas de Tecnologia da Informação, Segurança da Informação, Banco de Dados e Crimes Cibernéticos.

Resultados e Discussão

A Tecnologia da Informação tornou-se indispensável no cotidiano, transformando processos que antes eram físicos e manuais em sistemas informatizados. Nesse contexto, os Bancos de Dados surgiram como forma eficaz de armazenar, consultar e manipular informações.

No início, os dados eram tratados como entidades – informações únicas e distinguíveis – que precisavam se relacionar para permitir processos completos, como vendas, repasses ou produção (ABREU; MACHADO, 2012).

Na década de 1960, a IBM iniciou soluções para relacionar informações, e em 1970, Edgar Frank Codd apresentou o Modelo Relacional, que deu origem ao Sistema R e à linguagem SQL (Structured Query Language) (ALVES, 2014).

Além do modelo relacional, existem outros tipos de modelos de banco de dados, como:

- Hierárquico
- Rede
- Orientado a objetos
- Relacional-objetos
- Entidade-Relacionamento

Esses modelos representam a estrutura lógica do banco de dados, incluindo relações e restrições, geralmente representadas por diagramas e projetadas segundo regras definidas pelos designers (ALVES, 2014).

O trabalho apresentou, no primeiro capítulo, a evolução do tratamento das informações por meio de Bancos de Dados, incluindo modelos de armazenamento e tipos existentes no mercado, mostrando que a tecnologia é acessível a todos, não apenas a especialistas.

No segundo capítulo, a pesquisa sobre Segurança da Informação permitiu compreender os crimes digitais, técnicas utilizadas por hackers e as formas de atuação da lei frente a esses delitos.

O terceiro capítulo abordou a importância da proteção de dados, destacando que não existe um único método eficaz, sendo necessária a combinação de processos técnicos e políticas organizacionais e interpessoais.

Na década de 1960, a IBM iniciou soluções para relacionar dados, e em 1970, Edgar Frank Codd apresentou o Modelo Relacional, dando origem ao Sistema R e à linguagem SQL (ALVES, 2014). Outros modelos incluem:

hierárquico, de rede, orientado a objetos e entidade-relacionamento, representando a estrutura lógica do banco de dados e suas restrições.

Segurança da Informação é a proteção de dados, envolvendo senhas, criptografia, acessos físicos e digitais, visando garantir autenticidade, confidencialidade, integridade e disponibilidade das informações (FONTES, 2006).

As organizações devem implementar políticas e regras de segurança, abrangendo todos os colaboradores, e utilizar backups e armazenamento em nuvem como medidas preventivas. Exemplos de serviços de nuvem: Google Drive, OneDrive, Mega, iCloud, Dropbox (TEIXEIRA FILHO, 2015).

Crimes Cibernéticos

A falta de segurança pode resultar em crimes cibernéticos, como:

- Phishing: obtenção de dados via e-mails ou sites falsos;
- Malware: vírus, cavalos de Tróia, ransomware, spyware;
- Furto de dados e plágio;
- SIM Swap: clonagem de chips para acessar contas;
- Apologia ao crime e criação de perfis falsos (BAARS et al., 2018; FONTES, 2006).

Proteção de Dados

- Medidas de proteção incluem:
- Antivírus confiáveis (Avast, AVG, Norton, Kaspersky);
- Controle de acesso e auditoria;
- Backup e armazenamento seguro;
- Políticas de conscientização dos colaboradores (MACHADO, 2014).

Os cinco princípios essenciais da segurança da informação são:

- Disponibilidade
- Integridade
- Confidencialidade
- Legalidade
- Auditabilidade e não-repúdio

A LGPD (Lei nº 13.709/2018) regulamenta o tratamento de dados pessoais, garantindo privacidade, autodeterminação informativa e proteção de direitos fundamentais.

Conclusão

Concluiu-se que informações podem ser protegidas independentemente de sua origem ou destino, sendo a segurança viável para todas as entidades.

Ainda existem temas para pesquisas futuras, como:

Novas tecnologias e automação/robotização;

Conscientização de funcionários sobre segurança;

Cybersecurity, criptografia, Inteligência Artificial, IoT, GDPR e Wipers.

Esses tópicos representam caminhos para aprofundar o conhecimento e acompanhar a evolução da Segurança da Informação.

Referências

ABREU, Mauricio; MACHADO, Felipe. Projeto de Banco de dados: Uma visão prática. São Paulo: Érica, 2012.

ALVES, William. Banco de dados. São Paulo: Érica, 2014.

ARMAZENAMENTO EM NUVEM. Disponível em: <https://www.ohub.com.br/ideias/servicos-de-armazenamento-

em-nuvem/> Acesso em :15 abr.2023.
BAARS, Hans; SMULDERS, André; HINTZBERGEN, Jule; HINTZBERGEN, Kees.Fundamentos da Segurança da Informação: Com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.
BELLOVIN, Steven; RUBIN, Aviel;CHESWICK, William.Firewalls e Segurança na Internet: Repelindo o hacker ardiloso. Porto Alegre: Bookman,2005.
CANTUÁRIA, Guilherme. Modelo Orientado a Objetos.
CAIÇARA JUNIOR, Cícero; PARIS, Wanderson. Informática, Internet e Aplicativos. Curitiba: IBPEX, 2008)
ESET. Porcentagem de crimes cibernéticos no Brasil e na América Latina. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=40971&sid=18>Acesso em: 05 maio 2023.
FONTES, Edson. Segurança da Informação: O usuário faz a diferença. São Paulo: Saraiva, 2006.
LEI LGPD.Lei Geral de Proteção aos Dados. Disponível em: <https://canaltech.com.br/legislacao/senado-aprova-adiamento-da-lgpd-para-agosto-de-2021-162863/> Acesso em: 05 maio.2023.
MACHADO, Felipe. Segurança da Informação: Princípios e controle de ameaças. São Paulo: Érica, 2014.
MODELO DE REDE. Disponível em: <http://bancodedadosterceiroemiep.blogspot.com/2015/>Acesso em:15 abr.2023.
MODELO ENTIDADE RELACIONAMENTO. Disponível em: <https://www.guj.com.br/t/modelo-entidade-relacionamento-de-vendas/346446> Acesso em: 15 abr.2023.
MODELO HIERÁRQUICO. Disponível em: <https://www.devmedia.com.br/trabalhando-com-dados-hierarquicos-no-mysql/20097> Acesso em: 15 abr.2023.
MODELO RELACIONAL DE BANCO DE DADOS. Disponível em: <https://www.researchgate.net/figure/Figura-3-Modelo-relacional-do-banco-de-dados_fig3_312531321> Acesso em: 15 abr.2023.