XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

SISTEMAS DE IOT NA ÁREA DE SAÚDE

Luan Alves Camargo Marques[1],Ivan Leal Morales[2]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – luancamargo.fib@gmail.com;
[2]Professor Me. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB – ilmoralesbr@gmail.com

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Internet das Coisas; IoT; Saúde 4.0; Dispositivos Médicos; Telemedicina.

Introdução: A Internet das Coisas (IoT) vem se consolidando como um dos pilares da transformação digital na área da saúde, promovendo avanços na forma como pacientes são monitorados e tratados. O conceito de Internet of Medical Things (IoMT) descreve o ecossistema formado por sensores, dispositivos vestíveis, equipamentos hospitalares e softwares conectados, que coletam e transmitem dados clínicos em tempo real, integrando-os a prontuários eletrônicos e sistemas hospitalares (FUTURECOM, 2024). Essa interconexão amplia a capacidade diagnóstica e permite respostas médicas mais rápidas e precisas, sendo um dos fundamentos da chamada “Saúde 4.0”, a aplicação dos princípios da Indústria 4.0 à medicina (ROSA et al., 2022). O IoMT não apenas conecta dispositivos, mas também cria uma rede inteligente de dados clínicos, suportada por tecnologias de computação em nuvem, edge computing, inteligência artificial (IA) e redes 5G. Essa integração favorece o desenvolvimento de sistemas de suporte à decisão médica, com diagnósticos automatizados e alertas preditivos para doenças crônicas (TENAGLIA, 2023).

Objetivos: O presente trabalho tem como objetivo analisar a aplicação dos sistemas de IoT na área da saúde, destacando seus benefícios, desafios e impacto na melhoria da qualidade de vida dos pacientes. Busca-se compreender como o uso de dispositivos conectados pode otimizar processos hospitalares, reduzir custos e ampliar o acesso à medicina preventiva e personalizada.

Relevância do Estudo: Com o avanço da conectividade e da digitalização dos serviços médicos, o uso de IoT na saúde tornou-se essencial para o desenvolvimento de soluções inteligentes e sustentáveis. O tema é relevante por promover melhorias na eficiência diagnóstica, redução de custos operacionais e maior autonomia dos pacientes, além de contribuir para a consolidação de um ecossistema médico mais integrado e baseado em dados (Morsch, 2024). O estudo também busca evidenciar as limitações e riscos associados à adoção dessa tecnologia, como a segurança cibernética e a proteção de dados sensíveis.

Materiais e métodos: A pesquisa foi conduzida por meio de análise bibliográfica e documental, com base em estudos científicos, relatórios técnicos e artigos publicados entre 2015 e 2024. Foram consideradas fontes de relevância acadêmica e tecnológica, como Futurecom (2024), Rosa et al. (2022), Tenaglia (2023) e Massola e Pinto (2021). O estudo adota uma abordagem qualitativa e descritiva, com foco em identificar os principais benefícios, aplicações e desafios relacionados à implementação da IoT em ambientes clínicos e hospitalares.

Resultados e discussões: Entre as principais aplicações da IoT na saúde, destacam-se o monitoramento remoto de pacientes, a automação hospitalar e o gerenciamento inteligente de medicamentos. Dispositivos vestíveis, como pulseiras e relógios inteligentes, registram parâmetros fisiológicos — pressão arterial, glicemia e frequência cardíaca — e enviam alertas

automáticos à equipe médica em casos de anomalias. Em ambientes hospitalares, leitos e equipamentos inteligentes otimizam o trabalho de enfermeiros, permitindo respostas rápidas em situações críticas e reduzindo erros humanos (MORSCH, 2024). O conceito de IoMT amplia essa visão ao conectar diferentes sistemas médicos em uma rede única, na qual sensores de sala cirúrgica, bombas de infusão e ventiladores mecânicos podem comunicar-se entre si e com plataformas de gestão hospitalar (FUTURECOM, 2024). Essa integração favorece o controle logístico e operacional, reduzindo desperdícios e aumentando a rastreabilidade de insumos e equipamentos. Além disso, algoritmos de IA aplicados aos dados gerados pela IoMT permitem detectar padrões anômalos, prever crises médicas e recomendar intervenções personalizadas (TENAGLIA, 2023). Estudos recentes apontam que o uso de tecnologias IoT e IoMT pode reduzir em até 25% as readmissões hospitalares, além de otimizar o tempo de resposta médica em até 40% (MCKINSEY GLOBAL INSTITUTE, 2015). O avanço dessas soluções é impulsionado pela integração entre universidades, startups e empresas de tecnologia, que têm desenvolvido ecossistemas colaborativos voltados à medicina preventiva, reabilitação e monitoramento de idosos. Apesar dos benefícios, desafios como a fragmentação de plataformas, custos de implementação e vulnerabilidades em dispositivos médicos conectados ainda limitam a adoção em larga escala (MASSOLA; PINTO, 2021).

Conclusão: A adoção de sistemas de IoT na saúde representa um avanço significativo rumo à digitalização e modernização dos cuidados médicos. Apesar dos desafios relacionados à segurança e interoperabilidade, os benefícios superam as limitações, permitindo monitoramento contínuo, redução de custos e melhor qualidade no atendimento ao paciente. Com a expansão da computação em nuvem, da inteligência artificial e das redes 5G, a IoT tende a se consolidar como elemento essencial da transformação digital na saúde, contribuindo para a criação de sistemas médicos mais eficientes, acessíveis e humanizados.

Referências:

FUTURECOM. **IoT na medicina: avanços, benefícios e desafios do setor de saúde conectado**. 2024. Disponível em: https://digital.futurecom.com.br/transformaodigital/iot-na-medicina-internet-das-coisas-na-saude/. Acesso em: 17 out. 2025.

MASSOLA, S. C.; PINTO, G. S. **O uso da Internet das Coisas (IoT) a favor da saúde.** Faculdade de Tecnologia de São Paulo (FATEC), 2021.

MCKINSEY GLOBAL INSTITUTE. **The Internet of Things: Mapping the value beyond the hype.** 2015. Disponível em: https://www.mckinsey.com/. Acesso em: 17 out. 2025.

MORSCH, J. A. **IoT na medicina: aplicações da Internet das Coisas em clínicas e hospitais.** 2024. Disponível em: https://digital.futurecom.com.br/transformaodigital/iot-na-medicina-internet-das-coisas-na-saude/. Acesso em: 17 out. 2025.

ROSA, C. M.; SOUZA, P. A. R.; SILVA, J. M. **Inovação em saúde e Internet das Coisas (IoT): um panorama do desenvolvimento científico e tecnológico**. 2022.

TENAGLIA, M. R. **Simulação de ataques cibernéticos em dispositivos IoT em ambientes de saúde**. Pontifícia Universidade Católica de Goiás, 2023.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

DESEMPENHO DOS PROTOCOLOS NA SEGURANÇA DO IOT

Jhonny Richard dos Santos[1]; João Pedro Maffei Carraro[2]; Leonardo Henrique Alves Pereira[3]; Ivan Leal Morales[4]
[1]Aluno de Ciências da Computação – Faculdades Integradas de Bauru – FIB – jhonnysantos1578@gmail.com;
[2]Aluno de Ciências da Computação – Faculdades Integradas de Bauru – FIB – jpmaffeicarraro@gmail.com;
[3]Aluno de Ciências da Computação – Faculdades Integradas de Bauru – FIB – leonardoalves72@hotmail.com;
[4]Professor do curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB – ilmoralesbr@hotmail.com;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Internet das coisas, IOT, protocolo, segurança, zigbee, mqtt.

Introdução: Os protocolos são conjuntos de regras padronizadas que permitem dispositivos de se comunicar, compartilhar dados e funcionar em conjunto para trocar informações de maneira eficiente e segura, superando limites geográficos, organizacionais ou tecnológicos. Sem esses protocolos, os dispositivos não seriam capazes de se comunicar, o que comprometeria a funcionalidade do sistema e a eficácia do hardware."

Objetivos: Analisar a importância dos protocolos ZigBee e MQTT no contexto da segurança e desempenho dos dispositivos IoT, destacando suas características técnicas e como eles contribuem para a comunicação eficiente e protegida no ambiente digital.

Relevância do Estudo: Este estudo sobre os protocolos ZigBee e MQTT é relevante para a Agenda 2030, especialmente no contexto do ODS 9 (Indústria, Inovação e Infraestrutura), pois fortalece a infraestrutura digital necessária para a inovação tecnológica. Sua aplicação em sistemas IoT facilita a comunicação eficiente entre dispositivos, promovendo soluções mais sustentáveis e contribuindo para a transformação digital, ao otimizar o uso de recursos e expandir a conectividade inteligente.

Materiais e métodos: Este trabalho de natureza teórica adota uma abordagem híbrida, combinando pesquisa bibliográfica com análise descritiva dos dados coletados em artigos e fontes relevantes. A metodologia baseia-se na revisão da literatura e na comparação das abordagens de segurança e desempenho dos protocolos ZigBee e MQTT. Conforme Cervo e Bervain (2012) argumentam, essa pesquisa visa explicar as vantagens tendo como base as contribuições de outros autores considerados relevantes

Resultados e Discussões: Segundo o PortalCripto (2024), protocolo de comunicação é um conjunto de regras que permite a troca de informações entre dois ou mais dispositivos em uma rede de comunicação. Essas regras definem a sintaxe, semântica e sincronização da comunicação, bem como os métodos de recuperação de erros possíveis. Os protocolos também possuem mecanismos específicos para garantir a segurança e a confiabilidade dos dados transmitidos. Um exemplo relevante é o ZigBee, amplamente utilizado em aplicações de Internet das Coisas (IoT). Trata-se de um protocolo de comunicação sem fio baseado no padrão IEEE 802.15.4, projetado para redes pessoais de área (WPANs), com requisitos de baixo consumo de energia, baixo custo e taxas de dados moderadas. Ele opera em frequências como 2.4 GHz, 915 MHz e 868 MHz, utilizando o método CSMA-CA (Carrier

Sense Multiple Access with Collision Avoidance) para evitar colisões na transmissão de dados. O ZigBee adiciona camadas superiores de rede, aplicação e segurança, o que o torna uma solução ideal para IoT e comunicação máquina-a-máquina (M2M). Sua principal vantagem está no baixo consumo energético: dispositivos ZigBee podem operar em modo *deep sleep* por longos períodos, garantindo autonomia de meses ou até anos com baterias pequenas. Embora sua taxa de transmissão seja limitada (de 20 kbps a 250 kbps), isso não o impede de ser eficiente no envio de pequenos pacotes de dados, como leituras de sensores ou comandos simples. No entanto, ele não é apropriado para aplicações que exigem largura de banda elevada, como transmissão de vídeo. Seu baixo custo, facilidade de implementação e confiabilidade fazem com que seja amplamente adotado em sistemas de automação residencial, controle de iluminação, medição inteligente e monitoramento ambiental. Outro protocolo importante no contexto de IoT é o MQTT, criado pela IBM em 1999 com o objetivo inicial de possibilitar a comunicação eficiente entre satélites e dispositivos com recursos limitados. Ele adota o modelo de publicação/assinatura e opera em uma arquitetura cliente/servidor, utilizando o protocolo TCP como base de transporte. As mensagens são enviadas a tópicos específicos, o que facilita a organização, roteamento e filtragem dos dados dentro do sistema. Apesar de sua eficiência e leveza, o MQTT não possui mecanismos nativos de segurança. Por isso, costuma ser combinado com camadas externas, como TLS/SSL, que fornecem criptografia, autenticação e proteção contra-ataques do tipo *man-in-the-middle*. Adicionalmente, podem ser implementados recursos como autenticação de usuários, controle de acesso a tópicos e assinaturas digitais, aumentando a integridade e a confidencialidade das mensagens. Sua escalabilidade, simplicidade e baixo consumo de energia o tornam ideal para aplicações que exigem comunicação em tempo real e integração com a nuvem.

Conclusão: Os protocolos ZigBee e MQTT não são concorrentes diretos, mas tecnologias complementares que atuam em diferentes camadas da comunicação em sistemas IoT. Em uma arquitetura comum, dispositivos se comunicam localmente via ZigBee e enviam os dados a um gateway, que os pública na nuvem por meio do MQTT, utilizando Wi-Fi ou Ethernet. O ZigBee é eficiente na comunicação local e de baixo consumo, enquanto o MQTT garante o envio remoto dos dados com segurança e escalabilidade. Essa integração permite monitoramento remoto com baixo custo e alta autonomia. A escolha entre um ou ambos dependem das necessidades específicas de cada aplicação, como alcance, infraestrutura e tipo de dados. A combinação é amplamente utilizada em soluções como casas inteligentes, agricultura de precisão e cidades conectadas.

Referências

CERVO, A. L.; BERVIAN, A. **Metodologia Científica.** 5. ed. São Paulo: Prentice Hall, 2012.
DUTRA, João V. C. P.; FRANCO, Leonardo M.; MACAIBA, Pedro H. C.; BOAS, Evandro C. Vilas. **Estudo do protocolo de comunicação Zigbee.** Santa Rita do Sapucaí: Inatel, [s.d.]. Disponível em: https://inatel.br/csilab/documents/4-estudo-do-proto.pdf. Acesso em: 1 set. 2025.
JAFFEY, Toby. **MQTT and CoAP, IoT protocols.** 2014. Disponível em: http://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php. Acesso em: 12 set. 2025.
MUNIZ, Vinicius Angelo de O.; BRITO, Lucas L. Freire; NETO, Milton M.; OLIVEIRA, Monica Rocha F.; MORAES, Igor A. **Protocolos de comunicação para Internet of Things (IoT).** Intercursos Revista Científica, v. 17, n. 1, 2019. Disponível em: https://revista.uemg.br/intercursosrevistacientifica/article/view/3712. Acesso em: 20 ago. 2025.
ROTTA, Giovanni; CHARÃO, Andrea; DANTAS, Mario. **Um Estudo sobre Protocolos de Comunicação para Ambientes de Internet das Coisas.** In: ESCOLA REGIONAL DE

ALTO DESEMPENHO DA REGIÃO SUL (ERAD-RS), 2017, Ijuí. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2017. ISSN 2595-4164.

MACHINE LEARNING: APLICAÇÃO DOS PRINCÍPIOS DA ENG. DE SOFTWARE A MODELOS DE DESENVOLVIMENTO E CICLO DE VIDA DE ML

Luan Alves Camargo Marques [1], Faberson Augusto Ferrasi [2]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – luancamargo.fib@gmail.com;
[2]Professor Dr. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB – faberson.ferrasi@fibbauru.br;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Engenharia de Software; Machine Learning; MLOps; Ciclo de Vida; Qualidade de Software.

Introdução: A Inteligência Artificial (IA) e o Machine Learning (ML) têm se destacado como pilares da transformação digital, promovendo avanços significativos em setores como tecnologia, saúde, indústria e educação (ZUP, 2022). Entretanto, grande parte dos modelos desenvolvidos em ambientes de pesquisa não atinge a fase de produção, revelando desafios relacionados à escalabilidade, manutenção e confiabilidade. Essa limitação evidencia a necessidade de integrar princípios da Engenharia de Software (ES) ao ciclo de vida de desenvolvimento de sistemas inteligentes (GOOGLE CLOUD ARCHITECTURE CENTER, 2024). Nesse contexto, emerge o campo denominado Software Engineering for Machine Learning (SE4ML), que adapta fundamentos e práticas da engenharia tradicional ao contexto dinâmico do aprendizado de máquina. O presente estudo busca compreender de que forma os conceitos da Engenharia de Software podem contribuir para aprimorar os processos de desenvolvimento, implementação e manutenção de sistemas baseados em ML, abordando especialmente a integração com práticas de Machine Learning Operations (MLOps).

Objetivos: O objetivo deste trabalho é analisar a aplicação dos princípios da Engenharia de Software no desenvolvimento e operação de sistemas de ML, destacando a importância de práticas como automação, rastreabilidade e controle de qualidade de modelos (ORACLE, 2019).

Relevância do Estudo: Embora as aplicações de ML estejam em rápida expansão, muitos projetos enfrentam dificuldades em transpor a barreira entre o ambiente de pesquisa e a produção, o que evidencia a falta de metodologias consolidadas e padronizadas (ZUP, 2022). Assim, a integração entre Engenharia de Software e ML se torna um tema estratégico tanto para a academia quanto para a indústria, contribuindo para aumentar a confiabilidade, a reprodutibilidade e a sustentabilidade das soluções de IA.

Materiais e métodos: A pesquisa é de natureza bibliográfica e qualitativa, fundamentada em publicações científicas, guias técnicos e manuais de boas práticas publicados entre 2019 e 2024. Foram priorizadas fontes reconhecidas na área de SE4ML e MLOps, como Google Cloud, Oracle e Zup. As citações e referências seguem as normas da ABNT NBR 10520:2023 e NBR 6023:2018 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2023). O estudo tem caráter descritivo e exploratório, considerando o ciclo de vida do desenvolvimento de software aplicado ao aprendizado de máquina, suas metodologias, ferramentas de suporte e casos relatados na literatura.

Resultados e discussões: Os resultados apontam que a integração entre Engenharia de Software e ML exige uma reinterpretação dos ciclos de desenvolvimento. Enquanto a ES tradicional se baseia em requisitos estáveis e código determinístico, o ML depende fortemente da qualidade dos dados e da capacidade de adaptação a mudanças, como data drift e concept drift (GOOGLE CLOUD ARCHITECTURE CENTER, 2024). Nesse cenário, o MLOps surge como uma extensão dos princípios de DevOps, orientado à automação de pipelines, integração contínua e monitoramento de modelos (ZUP, 2022).Essa abordagem promove maior rastreabilidade, governança e escalabilidade dos sistemas, reduzindo o tempo de implantação e aumentando a previsibilidade operacional (ORACLE, 2019). Além disso, as práticas de qualidade em ML precisam considerar aspectos além do desempenho técnico, como transparência, imparcialidade e robustez. Métodos clássicos de engenharia, como os de Sommerville (2011) e Pressman (2014), continuam sendo referência teórica, mas demandam adaptações para acomodar a natureza iterativa e experimental dos sistemas de aprendizado de máquina.

Conclusão: Conclui-se que a integração entre Engenharia de Software e Machine Learning é fundamental para o avanço da maturidade e da confiabilidade dos sistemas inteligentes. O campo de SE4ML representa uma evolução natural da engenharia, unindo práticas consolidadas de desenvolvimento com técnicas específicas de automação e controle de modelos. Em ambientes corporativos e acadêmicos, a adoção de MLOps contribui para otimizar fluxos de trabalho, garantir reprodutibilidade e promover a sustentabilidade das soluções de IA (ZUP, 2022). Recomenda-se o aprofundamento de pesquisas voltadas à padronização de processos e à criação de frameworks integrados que unam os princípios de SE4ML e MLOps, fortalecendo a base metodológica do desenvolvimento de sistemas de Machine Learning em escala produtiva.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520**: Informação e documentação – Citações – Apresentação. Rio de Janeiro, 2023.

GOOGLE CLOUD ARCHITECTURE CENTER. **Diretrizes para desenvolver soluções de ML de alta qualidade**. 2024. Disponível em: https://cloud.google.com/architecture/guidelines-for-developing-high-quality-ml-solutions?hl=pt-br. Acesso em: 15 maio 2024.

ORACLE. **Data Science Lifecycle. 2019**. Disponível em: https://www.oracle.com/br/a/ocom/docs/data-science-lifecycle-ebook-pt-br.pdf. Acesso em: 15 maio 2024.

PRESSMAN, R. S. **Engenharia de Software**: uma abordagem profissional. 8. ed. Porto Alegre: AMGH, 2014.

SOMMERVILLE, I. **Engenharia de Software**. 9. ed. São Paulo: Pearson, 2011.

ZUP. **SE4ML**: Engenharia de Software para Machine Learning. 2022. Disponível em: https://zup.com.br/blog/se4ml. Acesso em: 15 maio 2024.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

ANÁLISE COMPARATIVA DE FERRAMENTAS COMPUTACIONAIS PARA A PREDIÇÃO DO CICLO DE VIDA DE BACTERIÓFAGOS

Thaís Migliorini Antunes da Silva[1]; Marco Aurelio Migliorini Antunes[2]; Daiane de Lima Antunes[3]; Willames Marcos Brasileiro da Silva Martins[4]
[1]Graduada em Biotecnologia – Universidade Federal da Integração Latino-Americana – UNILA – thaismigliorini15@gmail.com;
[2]Professor Me. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB – mamantunes@gmail.com;
[3]Professora Me. do Curso de Desenvolvimento de Sistemas – SENAI – daiane.antunes.lima@gmail.com;
[4]Líder Científico de Pesquisa em Bacteriófagos, Doutor em Infectologia – Universidade Oxford – OXFORD – willames.martins@biology.ox.ac.uk;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Bacteriófagos; Ciclo de Vida; Bioinformática; Análise Comparativa

Introdução: Os bacteriófagos (ou fagos) são vírus capazes de infectar bactérias e desempenham papel essencial no equilíbrio microbiano, na regulação populacional bacteriana e na evolução genômica de seus hospedeiros (MOURA, 2023; DION et al., 2020). Dependendo de seu comportamento dentro da célula bacteriana, os fagos podem apresentar ciclo lítico ou ciclo lisogênico (SONG, 2020). No ciclo lítico, o genoma viral é replicado e novas partículas são liberadas pela lise da célula hospedeira, enquanto no ciclo lisogênico o fago integra seu DNA ao genoma bacteriano, permanecendo em estado de latência. Fagos lisogênicos, também chamados temperados, podem alternar entre os dois ciclos conforme estímulos ambientais, sendo importantes tanto para a adaptação bacteriana quanto para a fagoterapia (OLSZAK et al., 2017). Com o avanço das técnicas genômicas, surgiram diferentes ferramentas computacionais para predizer o ciclo de vida de fagos a partir de sequências genéticas (TURNER et al., 2023). No entanto, a precisão dessas ferramentas ainda é variável, o que torna relevante avaliar seu desempenho comparativo.

Objetivos: Comparar a performance preditiva de quatro plataformas bioinformáticas – PhageAI, PhageLeads, BACPHLIP e PhageTYP – utilizadas para a classificação do ciclo de vida de fagos em genomas completos e parciais, a fim de identificar qual apresenta maior consistência e acurácia.

Relevância do Estudo: A determinação correta do ciclo de vida é essencial para aplicações biotecnológicas, terapêuticas e ecológicas que envolvem fagos. Ferramentas precisas permitem distinguir com maior confiança fagos temperados e líticos, otimizando a seleção de candidatos para estudos de fagoterapia e para análises evolutivas de comunidades microbianas. Dessa forma, a comparação sistemática entre preditores é um passo necessário para padronizar análises genômicas e evitar interpretações equivocadas, possibilitando a seleção de fagos com potencial terapêutico e maior compreensão de seus mecanismos de integração e persistência em hospedeiros bacterianos.

Materiais e métodos: Foram avaliadas 57 sequências genômicas de fagos, previamente classificadas como completas (n=42) ou parciais (n=15). Cada sequência foi submetida às plataformas PhageAI, PhageLeads, BACPHLIP e PhageTYP, por meio do upload de arquivos

no formato FASTA. As ferramentas empregam diferentes algoritmos de aprendizado de máquina e análise de assinaturas genéticas para prever se o ciclo de vida é lisogênico (temperado) ou lítico (virulento). As predições de cada programa foram comparadas entre si, e as classificações incoerentes foram contabilizadas com base na literatura e na expectativa biológica de que fagos integrados em genomas bacterianos são, em sua maioria, temperados. As análises foram divididas por tipo de genoma (completo e parcial), e os resultados foram expressos em porcentagem de acerto e erro.

Resultados e discussões: Foram analisadas 57 sequências genômicas de fagos, classificadas em completas (n=42) e parciais (n=15). Por se tratarem de genomas obtidos a partir de bactérias hospedeiras, todos os fagos analisados são, teoricamente, lisogênicos (temperados), uma vez que representam elementos integrados ao DNA bacteriano. Assim, a expectativa biológica é de que todas as ferramentas prevejam o ciclo lisogênico como resultado correto. Nos fagos completos, o PhageAI apresentou o melhor desempenho, com 95,23% de acerto, classificando corretamente 40 das 42 sequências como lisogênicas. O PhageTYP e o BACPHLIP apresentaram desempenho intermediário, com 35,7% e 30,9% de acerto, respectivamente. O PhageLeads, por outro lado, mostrou o pior desempenho, com erro superior a 85%, classificando erroneamente fagos lisogênicos como líticos. Nos fagos parciais, o desempenho das ferramentas foi mais heterogêneo. O PhageTYP apresentou a melhor performance nesse grupo, com 86,6% de acerto, seguido pelo PhageAI, que obteve 33,3%. O PhageLeads novamente apresentou baixa precisão, com falhas na predição e incompatibilidade no processamento de algumas sequências. Ao considerar o conjunto total de 57 fagos, o PhageAI destacou-se como a ferramenta mais consistente, com 78,9% de acerto global, seguida pelo PhageTYP, enquanto o PhageLeads manteve a maior taxa de erro. Esses resultados evidenciam que, embora todas as plataformas utilizem algoritmos baseados em aprendizado de máquina, há diferenças significativas na capacidade de identificar corretamente fagos temperados.

Conclusão: A análise comparativa mostrou diferenças expressivas na precisão das plataformas de predição de ciclo de vida de fagos. O PhageAI destacou-se como a ferramenta mais confiável, com acurácia superior a 95% para fagos completos e desempenho global de 78,9%, enquanto o PhageLeads apresentou as maiores taxas de erro. Esses resultados reforçam a importância de selecionar cuidadosamente a ferramenta bioinformática para estudos envolvendo caracterização fagal, especialmente em contextos de fagoterapia e análise evolutiva.

Referências

DION, M. B.; OECHSLIN, F.; MOINEAU, S. Phage diversity, genomics and phylogeny. **Nature Reviews Microbiology**, v. 18, n. 3, p. 125–138, 2020.

MOURA, Cesar da Silva Santana. Caracterização genômica dos profagos e elementos parecidos com profagos nas bactérias láticas do gênero *Weissella*. 2023.

OLSZAK, T.; LATKA, A.; ROSZNIOWSKI, B.; VALVANO, M. A.; DRULIS-KAWA, Z. Phage life cycles behind bacterial biodiversity. **Current Medicinal Chemistry**, v. 24, n. 36, p. 3987–4001, 2017. DOI: 10.2174/0929867324666170413100136.

SONG, Kai. Classifying the lifestyle of metagenomically-derived phages sequences using alignment-free methods. **Frontiers in microbiology**, v. 11, p. 567769, 2020.

TURNER, D.; SHKOPOROV, A. N.; LOOD, C. *et al.* Abolishment of morphology-based taxa and change to binomial species names: 2022 taxonomy update of the ICTV bacterial viruses subcommittee. **Archives of Virology**, v. 168, n. 1, p. 74, 2023.

APLICAÇÃO DA LGPD NA COMPUTAÇÃO: MEDIDAS DE SEGURANÇA E BOAS PRÁTICAS NO TRATAMENTO DE DADOS PESSOAIS

Maria Gabriela Alves de Oliveira[1]; Maria Lucia dos Santos[2];
[1]Aluna de Ciência da Computação– Faculdades Integradas de Bauru – FIB
gabyalveswhats@gmail.com;
[2]Professora do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB –
mlucia@uol.com.br;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: LGPD, segurança da informação, computação, proteção de dados, medidas técnicas e organizacionais

Introdução: A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018) é um marco regulatório essencial para a proteção de dados no Brasil, estabelecendo regras claras para o tratamento de informações pessoais. No campo da computação, sua aplicação é fundamental, pois envolve sistemas, aplicações e soluções digitais que processam dados em larga escala. O Capítulo VII da LGPD, que trata da segurança e das boas práticas, define medidas técnicas e organizacionais para garantir a proteção dos dados, exigindo dos profissionais de tecnologia uma compreensão prática dos princípios legais e técnicos envolvidos.

Objetivos: Analisar a aplicação do Capítulo VII da LGPD no contexto da computação, identificando medidas técnicas e organizacionais que assegurem conformidade legal e segurança da informação. O trabalho busca relacionar os artigos 46 a 49 da LGPD aos princípios de confidencialidade, integridade e disponibilidade, apresentando exemplos práticos de implementação.

Relevância do Estudo: Com o aumento dos incidentes de segurança registrados pela Autoridade Nacional de Proteção de Dados (ANPD), compreender a aplicação da LGPD tornou-se essencial para profissionais e organizações. A conformidade não apenas evita sanções, mas fortalece a confiança dos usuários e melhora a qualidade dos sistemas de informação. A LGPD impulsiona a adoção de práticas éticas e seguras no desenvolvimento de software e na gestão de dados.

Materiais e métodos: A pesquisa baseou-se em revisão bibliográfica da legislação (Lei 13.709/2018) e documentos da ANPD, além de estudos de casos práticos e normas técnicas de segurança da informação. A metodologia incluiu a análise comparativa entre os princípios de segurança da informação e os requisitos legais da LGPD.

Resultados e discussões: Os artigos 46 a 49 da LGPD estabelecem fundamentos para a proteção de dados pessoais. Entre as principais práticas estão: autenticação multifator, criptografia de dados, backup seguro, monitoramento contínuo e políticas de segurança da

informação. Na computação, a segurança deve estar presente desde o desenvolvimento até o descarte dos dados (security by design e privacy by design). Casos práticos como e-commerce e aplicações em nuvem evidenciam a importância de controles técnicos, contratos de proteção de dados e auditorias periódicas para garantir conformidade e segurança.

Conclusão: A implementação das medidas do Capítulo VII da LGPD na computação representa um avanço na proteção de dados e na segurança digital. Mais do que uma obrigação legal, é uma oportunidade de aprimorar processos e sistemas. Profissionais de TI devem adotar práticas que integrem aspectos técnicos, organizacionais e legais, garantindo sistemas éticos, seguros e alinhados à privacidade do usuário.

Referências

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Diário Oficial da União, Brasília, DF, 15 ago. 2018.
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 15, de 24 de abril de 2024.** *Regulamento de Comunicação de Incidente de Segurança.* Diário Oficial da União, Brasília, DF, 26 abr. 2024.
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo: Segurança da Informação para Agentes de Tratamento de Pequeno Porte.** Brasília: ANPD, 2022.
NARDELLI, C. **LGPD aplicada no desenvolvimento de software.** *Escola Regional de Engenharia de Software*, v. 9, p. 183–192, 2021.
PONTES, M. M. G. **Estudo de caso da implantação da LGPD em uma empresa paraibana.** 2021. Trabalho de Conclusão de Curso (Licenciatura em Ciência da Computação) – Universidade Federal da Paraíba, Rio Tinto, 2021.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

ANÁLISE DOS ALGORITMOS RUNGE KUTTA DE ORDEM 4 E RUNGE KUTTA FEHLBERG PARA UM SISTEMA CAÓTICO E NÃO LINEAR DO CIRCUITO ELETRÔNICO CHUA

Lino Timóteo Conceição de Brito[1]; Ronaldo César Dametto[2]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – linotim@hotmail.com;
[2]Professor do curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB
computacao@fibbauru.br

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: equações diferenciais; componentes elétricos; diodo; atrator; não linearidade

Introdução: Comportamento caótico é caracterizado por uma pequena variação na entrada de um sistema e que gera uma saída muito exagerado (Savi, 2017) e caracterizando assim um comportamento não linear. O circuito CHUA representa um sistema caótico apresentado pelo seu diodo (diodo de CHUA) como em Viana (2023). O expoente de Lyapunov pode indicar o comportamento do sistema se é caótico ou não.

Objetivos: O objetivo é resolver um sistema de equações diferenciais de primeira ordem e mostrar que o método Runge Kutta de ordem 4 e o método de Runge Kutta – Felhberg fornecem o mesmo resultado, sendo que este último funciona em 6 estágios ao invés de 10 estágios como no primeiro caso.

Relevância do Estudo: Estudo de comportamento não linear e caótico é importante para prever se o comportamento de um sistema diverge ou não. Sistemas caóticos são sistemas imprevisíveis e estão em diversas áreas de engenharia, física, elétrica, mecânica e outros. Além disso a resolução de equações diferencias, que pode ser encontradas em Boyce (2001), são complexas torna-se tedioso feito a mão e por isso os métodos numéricos e computacionais a fazem em segundos como apresentado por Ruggiero e Lopes (1996).

Materiais e métodos: Primeiramente obtém-se as equações diferenciais para o circuito CHUA através das Leis de Kirchhoff como pode ser encontrado em (Close, 1975). Em seguida essas equações são parametrizadas para que a solução esteja em um sistema de coordenadas retangulares em três dimensões. Então as equações são solucionadas pelos dois métodos e obtendo-se assim o gráfico do atrator caótico e o Mapa de Poincaré (pontos aleatórios indicando caos).

Resultados e discussões: A simulação para o Mapa de Poincaré resulta em pontos aleatórios indicando caos e a simulação para os atratores caóticos tiveram o mesmo formato dentro dos mesmos limites numéricos para os atratores caóticos, todos os gráficos em um espaço 3D de coordenadas retangulares. Os dois métodos, Runge Kutta ordem 4 e Felhberg mostraram o mesmo resultado, sendo que o método Felhberg realizou os métodos de ordem 4 e 5 com 6 estágios. Seria necessários 10 estágios para o Runge Kutta ordem 4 e ordem 5 clássicos (4 estágios para o de ordem 4 e 6 estágios para o de ordem 5).

ISSN 2358-6044
2025

Conclusão: Finalmente é mostrado a validade dos dois modelos com os mesmos resultados para os atratores caóticos do diodo do circuito eletrônico CHUA, sendo que o método Felhberg usa estágios compartilhados. Os gráficos para o Mapa de Poincaré geraram pontos aleatórios indicando caos.

Referências

BOYCE, William E.; DIPRIMA, Richard C. **Equações Diferenciais Elementares e Problemas de Valores de Contorno**. 7. ed. [*S. l.*]: LTC -Livros Técnicos e Científicos Editora S.A., 2001.

CLOSE, Charles M. **Circuitos Lineares**. 2. ed. [*S. l.*]: LTC -Livros Técnicos e Científicos Editora S.A., 1975.

RUGGIERO, Márcia A. Gomes; LOPES, Vera Lúcia da Rocha. **CÁLCULO NUMÉRICO**: Aspectos Teóricos e Computacionais. 2. ed. [*S. l.*]: MAKRON Books, 1996.

SAVI, Marcelo Amorim. **Dinâmica Não - linear e Caos**. 2. ed. Rio de Janeiro: E-papers, 2017.

VIANA, Ricardo Luiz. **Introdução à Dinâmica Não-Linear e Caos**. [*S. l.*], 13 jan. 2023. Disponível em: https://fisica.ufpr.br/viana/apostilas/caos/Livro.pdf. Acesso em: 20 jan. 2025.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

ESTUDO SOBRE DUALIDADE DE CIRCUITOS ELÉTRICOS E VALIDAÇÃO DE UM CIRCUITO USANDO LINGUAGEM R

Lino Timóteo Conceição de Brito[1]; Ronaldo César Dametto[2]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – linotim@hotmail.com
[2]Professor do curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB
computacao@fibbauru.br

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: circuito elétrico; equações diferenciais; armazenadores de energia; distorção harmônica

Introdução: Existe dispositivos elétricos que têm comportamentos opostos em um circuito elétrico e esses dispositivos são chamados duais. O trabalho faz um estudo sobre um circuito elétrico e componentes com comportamentos duais e gerando assim, cada circuito uma equação diferencial de segunda ordem e de acordo com (Close, 1975, p.101) conhecendo-se um circuito o seu dual é imediatamente determinado.

Objetivos: O objetivo do trabalho é fazer uma análise dos elementos duais de um circuito RLC (paralelo) e o seu dual série, e usando a linguagem R, plotar as saídas desses elementos (tensão e corrente) e validar a dualidade de um circuito RLC série com o RLC paralelo.

Relevância do Estudo: Dualidade podem ocorrer em circuitos elétricos e obter o seu dual sem precisar calcular os dois, conhecendo-se um, determina-se o outro rapidamente. O circuito possui capacitores, indutores e resistência e esses dois primeiros são elementos armazenadores de energia e que geram uma equação diferencial que pode ser resolvida pelo método de Runge Kutta de ordem 4. Esse método acelera a resolução de equações diferenciais.

Materiais e métodos: O circuito RLC gera uma equação diferencial, que pode ser estudada em Boyce (2001) de segunda ordem obtida através das leis de Kirchhoff. Uma vez obtida a equação diferencial, esta pode ser resolvida pelo método numérico e computacional Runge Kutta (Ruggiero e Lopes, 1996).

Resultados e discussões: Para a simulação e obtenção da solução das equações diferenciais foi usado a Linguagem R. Um elemento armazenador de energia gera uma equação diferencial de ordem 1 e como há dois elementos armazenadores de energia no circuito (capacitor e indutor) então é gerada uma equação diferencial de ordem 2. Exemplos de elementos duais são o capacitor e indutor, tensão e corrente, circuito aberto e curto circuito, configuração série e paralelo, etc. estudos sobre esses elementos podem ser encontrados em Nahvi e Edminister (2014). Também é gerado, na simulação, uma distorção harmônica, por efeitos não lineares do circuito como exposto por Cogo e Filho (2018).

ISSN 2358-6044
2025

Conclusão: Os circuitos mostram, através de simulação, que os elementos duais tem suas formas de ondas semelhantes para cada circuito série e paralelo. Além disso, as fórmulas matemáticas de algumas grandezas já mostram sua dualidade. Assim é possível calcular de imediato as grandezas de um circuito dual, conhecendo-se as grandezas do circuito original.

Referências

BOYCE, William E.; DIPRIMA, Richard C. **Equações Diferenciais Elementares e Problemas de Valores de Contorno**. 7. ed. [*S. l.*]: LTC, 2001.

CLOSE, Charles M. **CIRCUITOS LINEARES**. 2. ed. [*S. l.*]: LTC -Livros Técnicos e Científicos Editora S.A., 1975.

COGO, João Roberto; FILHO, José Batista Siqueira. **Capacitores de potência e filtros de harmônicos**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2018.

NAHVI, Mahmood; EDMINISTER, Joseph A. **Circuitos Elétricos**. 5. ed. Porto Alegre: Bookman, 2014.

RUGGIERO, Márcia A. Gomes; LOPES, Vera Lúcia da Rocha. **Cálculo Numérico**: ASPECTOS TEÓRICOS E COMPUTACIONAIS. 2. ed. [*S. l.*]: MAKRON Books, 1996.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

ESTUDO SOBRE A RELAÇÃO DA TECNOLOGIA DA INFORMAÇÃO COM A LEI GERAL DE PROTEÇÃO DE DADOS

Lino Timóteo Conceição de Brito[1], Maria Lucia de Azevedo[2]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – linotim@hotmail.com;
[2]Professora do curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: princípios da LGPD, tecnologia da informação, consentimento, finalidade

Introdução: Com o crescente número de golpes, fraudes, violações de dados e discriminação (por dados sensíveis) houve a necessidade de criar uma lei que cuidasse desses temas. A tecnologia está sempre se modificando, então a lei deve estar sempre passando por atualizações para se adequar a essas mudanças e assim a tecnologia da informação também deve estar sempre adequada a essas leis. A LGPD visa proteger a liberdade e privacidade do indivíduo (gov.br). A proteção de dados é uma espécie de direito da personalidade (Stelzer et al, 2019).

Objetivos: Fazer um estudo sobre LGPD e como ela funciona dentro de uma empresa para adequar o correto trabalho de desenvolvimento de software com as leis.

Relevância do Estudo: As empresas estão sendo cobradas pela Agência Nacional de Proteção de Dados (ANPD) e as empresas que não cumprem tais regras podem sofrer multas e terem o seu desenvolvimento prejudicado (Moreira, 2025). Além disso, o titular dos dados deve ter suas informações protegidas, para não sofre danos materiais ou morais. A empresa deve estar ciente de suas obrigações para com o titular assim como a transparência do tratamento de seus dados e assegurar a proteção desses dados. Segundo Siqueira (2025) a proteção de dados pessoais é um grande desafio da era digital. Ainda segundo (Get Privacy) existem além dos dados pessoais, os dados sensíveis.

Materiais e métodos: Em uma empresa existem vários agentes que são responsáveis pelo tratamento dos dados. O titular é o dono dos dados e todos os agentes de tratamento devem tratar esses dados de forma transparente para o titular. Além do titular, existe o controlador que toma as decisões sobre o tratamento de dados, o operador, que age em nome do controlador e o encarregado ou DPO que interage com a ANPD.

Resultados e discussões: O tratamento de dados possui um ciclo que vai desde a coleta, passando pelo processamento, transferência, armazenamento e quando não mais é utilizado deve passar pela exclusão e anonimização. Caso o dado não possa ser excluído, a anonimização deve ser feita para quebrar qualquer meio de identificação do dado com o titular. Um documento (inventário) é elaborado para o armazenamento de dados pessoais e

ISSN 2358-6044
2025

sensíveis assim como relatórios deve ser elaborado em uma empresa (RIPD), Relatório de Impacto à Proteção de Dados. Medidas de segurança devem ser tomadas, não somente para a proteção de dados em meio eletrônico, mas também no formato de arquivos físicos. A proteção de dados é uma responsabilidade de todos funcionários da empresa e devem trabalhar em conjunto para o correto tratamento dos dados. O pessoal deve ser treinado para lidar como os dados durante todo o ciclo de vida dos dados de acordo com a LGPD. Para isso é necessário saber como caminhar e dar os passos corretamente para prática da LGPD em uma empresa.

Conclusão: Uma vez conhecida a LGPD, esta deve ser passada aos funcionários para que a empresa siga passo a passo para todos os agentes na empresa, como o controlador, o operador e o DPO (encarregado). Um comitê pode ser formado para a tomada de decisões e esse comitê pode ser composto por profissionais de diversas áreas atuantes na empresa.

Referências

GET PRIVACY (ed.). **10 bases legais da LGPD que justificam o tratamento de dados: consentimento, legítimo interesse e mais**. [*S. l.*], [2018-?]. Disponível em: https://getprivacy.com.br/entenda-as-bases-legais-da-lgpd/. Acesso em: 3 out. 2025.

LEI Geral de Proteção de Dados Pessoais (LGPD). [*S. l.*], [entre 2018 e 2025] [2018-?]. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd. Acesso em: 3 out. 2025.

MOREIRA, Bruno. **Adequação da TI a LGPD – Foco na área de Sistemas na prática**. [*S. l.*], 2025. Disponível em: udemy. Acesso em: 3 out. 2025.

SIQUEIRA, Patricia Gonzaga de. **A Lei Geral de Proteção de Dados (LGPD) no Brasil: desafios e impactos nas relações de consumo no ambiente digital**. [*S. l.*], 24 fev. 2015. Disponível em: https://colegioregistralrs.org.br/artigos/2130/artigo-a-lei-geral-de-protecao-de-dados-lgpd-no-brasil-desafios-e-impactos-nas-relacoes-de-consumo-no-ambiente-digital-por-patricia-gonzaga-de-siqueira/. Acesso em: 3 out. 2025.

STELZER, Joana; GONÇALVES, Everton das Neves; BAPTISTA, Rudá Ryuiti Furukita; VAZ, Rafael Medeiros Popini; WIEIRA, Keite; FIDELIS, Monique De Medeiros. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E OS DESAFIOS DAS INSTITUIÇÕES DE ENSINO SUPERIOR PARA A ADEQUAÇÃO. **XIX Colóquio Internacional de Gestão Universitária**, [*S. l.*], p. 1-14, 27 nov. 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/201939/103_00090.pdf?sequence=1&isAllowed=y. Acesso em: 3 out. 2025.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

ANÁLISE DE UM ALGORITMO KNN HÍBRIDO (CLÁSSICO - QUÂNTICO) PARA UMA BASE DE DADOS LIAR PARA A CLASSIFICAÇÃO DE FAKENEWS

Lino Timóteo Conceição de Brito[1]; Ronaldo César Dametto[2]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – linotim@hotmail.com;
[2]Professor do curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB
computacao@fibbauru.br

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: métricas; vizinhos; distância; validação cruzada; Grid Search

Introdução: A computação quântica leva uma grande vantagem em relação à computação clássica, pois sua velocidade de processamento é muito maior. A computação quântica possui o que se chama “paralelismo quântico”, isto é, um número exponencial de computação é realizado de forma simultânea (Almeida, 2020, p.73). O algoritmo *K_NN* é usado para avaliar uma base de dados liar *dataset* com textos em inglês para a classificação do nível de veracidade de uma informação (*fakenews* ou não *fakenews*).

Objetivos: O objetivo é usar uma base de dados contendo texto sobre fatos políticos e com classificação em níveis de veracidade da informação. Também avaliar o desempenho do algoritmo usando métricas como curva *AUC ROC*, *F1_Score*, *Variational Quantum Classifier* e validação cruzada.

Relevância do Estudo: A computação quântica surgiu com o conceito de Física Quântica e leva vantagem sobre a computação clássica, por ter uma velocidade de processamento muito maior. Isso porque na computação clássica é possível apenas dois estados, 0 ou 1, enquanto a computação quântica trabalha com superposição e *entanglement* (emaranhado), gerando uma superposição de *qubits* e podendo gerar inúmeros estados (estados quânticos). Os algoritmos quânticos são feitos para serem simulados em computadores quânticos sendo assim, esses algoritmos são processados em uma velocidade muito maior, o que revoluciona a computação. Existem vários algoritmos quânticos que podem ser encontrados na literatura e em bons livros de *Quantum Computing*.

Materiais e métodos: A base de dados possui 6 saídas, representando um nível de veracidade da informação, então as 3 saídas que mais se aproximam de falso foram classificadas como 1 (*fakenews*) e as outras 3 saídas que se assemelham como verdadeiras foram classificadas como não *fakenews* (0). Assim o classificador analisa saídas binárias.

Resultados e discussões: Um algoritmo *K – NN* baseado em *Fuzzy*, para diagnosticar e prever mal de Parkinson ainda em estágios iniciais é abordado por Abirami e Karthikeyan (2023). O algoritmo *GAK – DPC* (*Graph Distance and Adaptive K-Nearest Neighbors Selection-Based Density Peak Clustering*) é proposto Sun et al (2024) no lugar do algoritmo *DPC* (*Density Peak Clustering*). Um estudo sobre a teoria do algoritmo *K-NN* é feita por Granatyr (2025) e um algoritmo *K-NN* quântico é feito por Ramanathan (2024). As saídas são analisadas, como a curva *AUC ROC* que forneceu um resultado satisfatório para o *K-NN*

clássico e híbrido, porém insatisfatório para o *VQC*. Também foi feito um Grid Search para resultar no melhor parâmetro (k e distância). Para o k (número de vizinhos) foi igual a 2 e a melhor métrica foi a distância euclidiana entra as distâncias candidatas *euclidean*, *manhattan* e *cosine*.

Conclusão: Para o *K-NN* híbrido, a validação cruzada para o *VQC* mostra-se insatisfatória, a acurácia e *F1-Score* para o *VQC* mostram-se também insatisfatórias, enquanto que para o *K_NN* clássico e híbrido apresentam-se satisfatórios e a curva *AUC ROC* mostra-se insatisfatória para o *VQC* e eficiente para o *K-NN* clássico e híbrido. Foi usado um número reduzido de amostras devido ao longo tempo de execução no computador clássico, isso era esperado pois o algoritmo quântico é feito para ser simulado em um computador quântico.

Referências

ABIRAMI, L.; KARTHIKEYAN, J. Digital Twin-Based Healthcare System (DTHS) for Earlier Parkinson Disease Identification and Diagnosis Using Optimized Fuzzy Based k-Nearest Neighbor Classifier Model. **IEEE Access**, [*s. l.*], 2023. Disponível em: https://ieeexplore.ieee.org/document/10239395. Acesso em: 20 dez. 2024.

ALMEIDA, Norton Gomes de. **Introdução à computação e informação quântica**: Incluindo álgebra linear com kets e bras. 1. ed. São Paulo: Editora Livraria da Física, 2020.

GHAEMINEZHAD, Nourallah; CONG, Shuang. Preparation of Hadamard Gate for Open Quantum Systems by the Lyapunov Control Method. **IEEE/CAA Journal of Automatica Sinica**, [*s. l.*], 2018. Disponível em: https://ieeexplore.ieee.org/document/8332145. Acesso em: 21 dez. 2024.

GRANATYR, Jones. **Machine Learning e Data Science com Python de A a Z**. [*S. l.*]: IA Expert Academy, [entre 2014 e 2023] [2014?]. Disponível em: https://www.udemy.com/course/machine-learning-e-data-science-com-python-y/learn/lecture/26172974?start=15#overview. Acesso em: 27 dez. 2024.

LI, Jiaye; ZHANG, Jian; ZHANG, Jilian; ZHANG, Shichao. Quantum KNN Classification With K Value Selection and Neighbor Selection. **IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS**, [*s. l.*], 2024. Disponível em: https://ieeexplore.ieee.org/document/10366842. Acesso em: 21 dez. 2024.

RAMANATHAN, Kumaresan. **QC101 Quantum Computing & Intro to Quantum Machine Learning**. [*S. l.*]: Udemy, 2024. Disponível em: https://www.udemy.com/course/qc101-introduction-to-quantum-computing-quantum-physics-for-beginners/learn/lecture/35892972?start=15#overview. Acesso em: 27 dez. 2024.

SUN, YUQIN; WANG, JINGCONG; SUN, YUAN; ZHANG, PENGCHENG; WANG, TIANY. Graph Distance and Adaptive K-Nearest Neighbors Selection-Based Density Peak Clustering. **IEEE Access**, [*s. l.*], 2024. Disponível em: https://ieeexplore.ieee.org/document/10535104. Acesso em: 20 dez. 2024.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

ARMAZENAMENTO DE DADOS EM AMBIENTES DISTRIBUÍDOS

Luan Alves Camargo Marques [1], Marco Aurelio Migliorini Antunes [2]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – luancamargo.fib@gmail.com;
[2]Professor Me. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB - mamantunes@gmail.com;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Banco de Dados, Sistemas Distribuídos, Armazenamento de Dados.

Introdução: O armazenamento de dados é um componente essencial na era da informação digital, em que organizações e usuários necessitam gerenciar grandes volumes de dados gerados por aplicações de Big Data, Inteligência Artificial (IA), Aprendizado de Máquina (ML) e Internet das Coisas (IoT). Além de sustentar processos analíticos, o armazenamento também é vital para garantir a integridade e a disponibilidade das informações frente a falhas ou desastres. Segundo relatório da IBM (SUSNJARA; SMALLEY, 2024), o custo médio global de uma violação de dados em 2025 alcançou US$ 4,45 milhões, ressaltando a importância de estratégias de proteção e recuperação. Nesse contexto, os sistemas de armazenamento distribuído vêm sendo explorados como uma solução para lidar com o crescimento exponencial dos dados e a necessidade de acesso contínuo e seguro em diferentes locais.

Objetivos: Este estudo tem como objetivo explorar as principais abordagens de armazenamento de dados em ambientes distribuídos, analisando suas vantagens, desafios e tecnologias envolvidas. Além disso, busca-se identificar as tendências e inovações que contribuem para a evolução dessas soluções, especialmente no contexto de grandes volumes de dados e aplicações críticas.

Relevância do Estudo: A adoção de ambientes distribuídos para armazenamento de dados representa um avanço na infraestrutura computacional moderna. Essa abordagem permite que múltiplos dispositivos e servidores compartilhem recursos, proporcionando maior desempenho, escalabilidade e tolerância a falhas (GRAEBIN, 2006). Tanenbaum (2002, apud GRAEBIN, 2006) define um sistema distribuído como “um conjunto de computadores independentes que se apresenta aos usuários como um único sistema coerente”. Conceito esse que é essencial para aplicações críticas, por exemplo na área de IoT, onde há coleta massiva e descentralizada de dados. Assim, compreender as tecnologias, os desafios e as tendências que envolvem o armazenamento de dados distribuídos tornam-se fundamental para o desenvolvimento de soluções mais eficientes e seguras.

Materiais e métodos: A pesquisa foi conduzida por meio de uma revisão bibliográfica baseada em artigos científicos, livros e relatórios técnicos publicados nos últimos anos. Foram analisadas abordagens como sistemas de arquivos distribuídos (DFS), bancos de dados distribuídos, técnicas de replicação e particionamento, além de protocolos de consistência e tolerância a falhas. A análise comparativa dessas soluções permitiu identificar os principais desafios e avanços na área.

Resultados e discussões: Os sistemas de armazenamento distribuído têm evoluído com o suporte de protocolos como HTTP, FTP e Peer-to-Peer (P2P), que possibilitam o compartilhamento de arquivos entre computadores de forma econômica e flexível (GRAEBIN,

2006). Esses sistemas buscam garantir transparência, replicação e tolerância a falhas, fatores que influenciam diretamente sua eficiência e confiabilidade. No contexto corporativo, soluções como Data Warehouses também se beneficiam de ambientes distribuídos e do processamento paralelo, otimizando consultas complexas em grandes volumes de dados. Segundo Ruggiero Júnior (2007), o modelo estrela proposto por Kimball e Ross (2002) proporciona melhor desempenho nas operações de análise, ao reduzir a necessidade de múltiplas junções entre tabelas. Em ambientes de Internet das Coisas (IoT), o desafio é ainda maior. A coleta e o tratamento de dados em tempo real exigem arquiteturas altamente distribuídas e adaptáveis. Huacarpuma et al. (2016) destacam o desenvolvimento de um Serviço Distribuído de Coleta de Dados (SDCD) capaz de ajustar o grau de paralelismo conforme a demanda do ambiente. Tal abordagem demonstra como o armazenamento distribuído é fundamental para sustentar a escalabilidade e a eficiência de sistemas inteligentes interconectados.

Conclusão: O armazenamento de dados em ambientes distribuídos é uma solução estratégica para lidar com o volume, a velocidade e a variedade das informações geradas na era digital. Esse modelo oferece escalabilidade, segurança, tolerância a falhas e alta disponibilidade, sendo amplamente utilizado em aplicações de IA e IoT. Apesar dos avanços, persistem desafios relacionados à segurança, replicação e consistência dos dados, especialmente em ambientes híbridos. O progresso de tecnologias como computação em nuvem e automação inteligente tende a fortalecer essas soluções, tornando-as mais eficientes e confiáveis. Assim, o armazenamento distribuído consolida-se como um pilar fundamental da transformação digital, promovendo inovação e garantindo maior estabilidade e desempenho na gestão de dados em larga escala.

Referências:

GRAEBIN, Lucas. **Armazenamento distribuído.** 2006. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Centro Universitário Feevale, Instituto de Ciências Exatas e Tecnológicas, Novo Hamburgo, 2006. Disponível em: https://tconline.feevale.br/tc/files/0001_756.pdf. Acesso em: 7 out. 2025.

HUACARPUMA, Ruben C.; DE SOUSA JÚNIOR, Rafael T.; HOLANDA, Maristela; LIFSCHITZ, Sérgio. **Concepção e desenvolvimento de um serviço distribuído de coleta e tratamento de dados para ambientes de Internet das Coisas.** In: SIMPÓSIO BRASILEIRO DE BANCO DE DADOS (SBBD), 31., 2016, Salvador. Anais... Porto Alegre: Sociedade Brasileira de Computação, 2016. p. 28–39. ISSN 2763-8979. DOI: https://doi.org/10.5753/sbbd.2016.24306.

RUGGIERO JÚNIOR, Waldemar. **Data Warehouse utilizando processamento paralelo em ambiente distribuído.** 2007. Dissertação (Mestrado em Sistemas Digitais) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2007. DOI: https://doi.org/10.11606/D.3.2007.tde-09012008-093830. Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3141/tde-09012008-093830/en.php. Acesso em: 7 out. 2025.

SILVA, Marcelo Antonio da. **Utilização da computação distribuída para o armazenamento e indexação de dados forenses.** 2012. Dissertação (Mestrado em Engenharia Elétrica) – Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, 2012. Disponível em: http://repositorio.unb.br/handle/10482/10864. Acesso em: 7 out. 2025.

SUSNJARA, Stephanie; SMALLEY, Ian. **O que é armazenamento de dados?** IBM Think, [S. l.], 2024. Disponível em: https://www.ibm.com/br-pt/think/topics/data-storage. Acesso em: 7 out. 2025.

SEGURANÇA CIBERNÉRTICA E TENDÊNCIAS ATUAIS NO BRASIL

João Pedro Spadacini[1]; André Matias[2]; Vitor Godoy[3]; Marco Aurelio Migliorini Antunes[4]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – spadacinijoao@gmail.com;
[2]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB - andre.v.r.matias_@hotmail.com;
[3]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB vitorgodoy61@gmail.com;
[4]Professor Me. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB – mamantunes@gmail.com;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: cibersegurança, crimes virtuais, segurança da informação;

Introdução: A expansão do uso das tecnologias digitais no Brasil tem proporcionado avanços expressivos em diversos setores da sociedade, impulsionando a economia, a comunicação e a gestão de dados (Silva; Vieira 2021). Entretanto, esse crescimento também intensificou a ocorrência de crimes cibernéticos, que se tornaram uma preocupação crescente para instituições públicas e privadas. Este artigo analisa o panorama atual da segurança cibernética no país, destacando os principais desafios, tendências e políticas públicas voltadas à proteção das informações e à prevenção de incidentes digitais.

Objetivos: Investigar as formas predominantes de crimes cibernéticos no Brasil e analisar as estratégias governamentais e corporativas que vêm sendo adotadas para fortalecer a segurança digital e mitigar riscos no ambiente virtual.

Relevância do Estudo: A segurança cibernética é um componente essencial na proteção de informações sensíveis, da privacidade dos usuários e da integridade dos sistemas digitais. Com o avanço das tecnologias e a crescente digitalização de serviços, o volume de dados trafegados em redes públicas e privadas aumentou significativamente, tornando as organizações mais vulneráveis a ataques cibernéticos (Cecyber, 2025). Nesse contexto, torna-se indispensável adotar políticas de segurança robustas, investimentos em infraestrutura tecnológica e capacitação de profissionais especializados. Este estudo busca contribuir para a compreensão do impacto dos crimes virtuais no cenário brasileiro, analisando suas consequências econômicas, sociais e institucionais, além de propor medidas preventivas e estratégias de mitigação eficazes.

Materiais e métodos: Pesquisa bibliográfica e análise de relatórios de segurança, abordando as estratégias de defesa adotadas por organizações públicas e privadas no Brasil.

Resultados e discussões: Segundo o artigo (im)possibilidade de coerção (Tornem, 2025) os crimes cibernéticos mais comuns no Brasil incluem phishing, ransomware e fraudes financeiras. O phishing continua a ser uma técnica prevalente, enganando usuários para fornecer dados pessoais. O ransomware, que bloqueia o acesso a sistemas até que um resgate seja pago, também tem crescido, afetando tanto usuários individuais quanto empresas. A implementação da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) é uma medida significativa para combater essas ameaças, fornecendo diretrizes para a coleta e

tratamento de dados. No entanto, ainda existem desafios em relação à conscientização dos usuários sobre práticas seguras online, sendo necessário maior investimento em educação digital e campanhas de conscientização.
Analisando o artigo IBM Security (IBM, 2023) vemos que outra tendência crescente é o uso da inteligência artificial (IA) na cibersegurança, que pode auxiliar na detecção e resposta rápida a ameaças cibernéticas, otimizando a segurança e mitigando riscos antes que se tornem críticos. No entanto, o Brasil ainda enfrenta desafios econômicos na implementação dessas tecnologias, conforme discutido pela Kaspersky, além de um déficit de profissionais qualificados na área de cibersegurança.
Assim, a combinação de políticas como a LGPD, o uso de IA, e a conscientização dos usuários será crucial para o fortalecimento da segurança cibernética no Brasil.

Conclusão: Para fortalecer a segurança cibernética no Brasil, é essencial promover investimentos contínuos em educação digital, marcos regulatórios sólidos e tecnologias emergentes, como a inteligência artificial e a análise preditiva de dados. A educação digital desempenha papel estratégico na formação de uma cultura de segurança, capacitando usuários e profissionais para identificar ameaças e adotar boas práticas de proteção de dados. Paralelamente, legislações como a LGPD devem ser constantemente atualizadas para acompanhar a evolução tecnológica e garantir a responsabilização de agentes públicos e privados. Além disso, o fortalecimento da cooperação entre os setores governamental, corporativo e acadêmico será determinante para o desenvolvimento de soluções inovadoras e para a criação de políticas nacionais de cibersegurança mais eficazes. Essa integração é fundamental para mitigar riscos, reduzir vulnerabilidades e consolidar um ambiente digital mais seguro e resiliente no país.

Referências:

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**. Brasília, DF: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.html. Acesso em: 15 out. 2025.

SILVA, Ricardo Leopoldo da; VIEIRA, Anderson. **Segurança cibernética: o cenário dos crimes virtuais no Brasil**. Revista Científica Multidisciplinar Núcleo do Conhecimento, 2021. Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais. Acesso em: 20 out. 2025

CECYBER, **Tendências Emergentes em Cibersegurança. Cecyber**, 2023. Disponível em: https://cecyber.com/tendencias-emergentes-ciberseguranca/. Acessado em: 24 out. 2025

IBM, **Cibersegurança de inteligência artificial (IA).** 2023. Disponível em: https://www.ibm.com/br-pt/ai-cybersecurity. Acesso em: 15 out. 2025.

TORMEN, C. - **Crimes cibernéticos: (im)possibilidades de coerção**. Disponível em: https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4078.pdf. Acesso em: 20/10/2025.

ISSN 2358-6044
2025

GESTÃO DA INFORMAÇÃO E INTELIGÊNCIA COMPETITIVA NO SETOR INDUSTRIAL

Thaís Migliorini Antunes da Silva[1]; Marco Aurelio Migliorini Antunes[2]; Daiane de Lima Antunes[3]; Carlos Alexandre Cavalheiro[4]
[1]Graduada em Biotecnologia – Universidade Federal da Integração Latino-Americana – UNILA – thaismigliorini15@gmail.com;
[2]Professor Me. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB – mamantunes@gmail.com;
[3]Professora Me. do Curso de Desenvolvimento de Sistemas – SENAI – daiane.antunes@sp.senai.br;
[4]Professor do Curso de Desenvolvimento de Sistemas – SENAI – carlos.cavalheiro@sp.senai.br;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: organizações industriais, competência em informação e midiática, vantagem competitiva

Introdução: Com a rápida evolução das tecnologias da informação e comunicação (TICs), o setor industrial tem vivenciado profundas transformações em seus processos produtivos, logísticos e estratégicos. Nesse contexto, a informação passou a ser um dos principais ativos organizacionais, e seu uso eficiente tornou-se um diferencial competitivo fundamental. Assim, surge a necessidade de desenvolver novas competências voltadas à análise crítica, à interpretação de dados e à tomada de decisão baseada em evidências, destacando-se entre elas a competência em informação e midiática. Segundo Nonaka e Takeuchi (1997, p. 59), "[...] a organização que deseja lidar de forma dinâmica com as mudanças no ambiente precisa criar informação e conhecimento, não apenas processá-los de forma eficiente". Esse pensamento reforça a importância da geração e compartilhamento do conhecimento como elementos centrais para a inovação e para o crescimento sustentável das empresas. De acordo com De Sordi (2008, p. 12), "[...] conhecimento é o novo saber, resultante de análise e reflexões de informações segundo valores e modelo mental daquele que o desenvolve, proporcionando a esta melhor capacidade adaptativa às circunstâncias do mundo real". Dessa forma, o conhecimento organizacional não se limita ao simples acúmulo de dados, mas implica em transformar informação em ação estratégica, promovendo adaptação e vantagem competitiva em ambientes industriais cada vez mais complexos e dinâmicos.

Objetivos: Este estudo tem como objetivo promover maior assertividade nos processos decisórios no contexto industrial, sob o enfoque da competência em informação e midiática. Busca-se mapear as variáveis essenciais relacionadas ao acesso, análise e uso estratégico da informação, de modo a favorecer a construção do conhecimento organizacional e sua aplicação nas decisões empresariais. De forma específica, pretende-se contribuir para o fortalecimento da inteligência competitiva no setor industrial, ao demonstrar como o uso inteligente da informação pode otimizar processos, aumentar a capacidade de inovação e sustentar vantagens competitivas em um mercado cada vez mais orientado por dados

Relevância do Estudo: A relevância deste estudo está em evidenciar o papel estratégico da informação como ativo essencial à competitividade industrial. Em um cenário marcado pela transformação digital e pela intensa geração de dados, as empresas enfrentam o desafio de converter informações em conhecimento aplicável, capaz de sustentar decisões mais rápidas, precisas e inovadoras.

ISSN 2358-6044
2025

Materiais e métodos: O trabalho, de natureza teórica, é resultado de pesquisa bibliográfica, utilizando-se da análise da opinião de alguns autores contidas na literatura especializada. Conforme Cervo; Bervian (2002), considerando-se que essa pesquisa visa explicar um problema tendo como base as contribuições de outros autores considerados relevantes, podendo ser realizada independentemente ou como parte de pesquisa descrita ou experimental.

Resultados e discussões: De acordo com Fleury e Fleury (2004, p. 30), a competência pode ser entendida como "[…] um saber agir responsável e reconhecido, que implica mobilizar, integrar e transferir conhecimentos, recursos e habilidades, agregando valor econômico à organização e valor social ao indivíduo". Nesse sentido, o ambiente industrial contemporâneo exige profissionais capazes de transformar informação em ação estratégica, integrando habilidades cognitivas e tecnológicas ao processo decisório. Os diferentes níveis de competitividade demandam planejamento estratégico orientado por conhecimento, o que requer o uso de ferramentas de apoio à informação e análise de dados. Assim, a competência em informação e midiática, aliada à cognição organizacional, torna-se cada vez mais essencial para lidar com a complexidade do paradigma tecnológico atual (CASTELLS, 2000). Essa perspectiva impulsiona o desenvolvimento de projetos e práticas inovadoras, fortalecendo o engajamento de profissionais e organizações. O crescimento econômico sustentável depende do uso criativo e eficiente do conhecimento, aliado à eficácia dos serviços de informação. Dessa forma, a consolidação da competência em informação e midiática deve apoiar-se em três pilares fundamentais: cidadania, crescimento econômico e empregabilidade. A cidadania informacional envolve o uso crítico e ético dos dados, promovendo o desenvolvimento contínuo dos indivíduos, enquanto a empregabilidade está relacionada à capacidade de aplicar estratégias informacionais que impulsionem o sucesso profissional e organizacional.

Conclusão: É imprescindível que o avanço das indústrias esteja acompanhado pela eficiência no uso da informação, reconhecendo seu valor estratégico para o desenvolvimento organizacional. Para que essas instituições mantenham sua competitividade em um ambiente cada vez mais dinâmico e tecnológico, é essencial que dados, informações e conhecimento sejam produzidos, gerenciados e aplicados de forma integrada, orientando processos decisórios mais assertivos. O uso inteligente da informação permite melhor aproveitamento dos recursos, otimização do desempenho e elevação da qualidade dos produtos e serviços, fortalecendo o posicionamento das organizações no mercado. Dessa forma, a informação deixa de ser apenas um insumo operacional e passa a representar um ativo estratégico fundamental, capaz de sustentar a inovação, a eficiência e a vantagem competitiva no setor industrial.

Referências

CASTELLS, M. **A sociedade em rede**. 8. ed. São Paulo: Paz e Terra, 2000.v.1.

CERVO, A. L.; BERVIAN, A. **Metodologia científica**. 5. ed. São Paulo: Prentice Hall, 2002.

DE SORDI, J. O. **Administração da informação**: fundamentos e práticas para uma nova gestão do conhecimento. São Paulo: Saraiva, 2008.

FLEURY, M.T.L; FLEURY, A. **Construindo o conceito de competência**. 2001.Disponível em:
http://www.scielo.br/scielo.php?pid=S141565552001000500010&script=sci_arttext&tlng=pt>. Acesso em: 15 ago. 2025.

NONAKA, I.; TAKEUSCHI, H. **Criação de conhecimento na empresa**: como as empresas japonesas geram a dinâmica da inovação. 19 ed. Rio de Janeiro: Campus, 1997.

UMA ANÁLISE COMPARATIVA ENTRE O GOOGLE E O CHATGPT

Ana Rodrigues Gomes da Silva [1]; Thaís Migliorini Antunes da Silva[2]; Marco Aurelio Migliorini Antunes[3]
[1]Aluna de Ciência da Computação – Faculdades Integradas de Bauru – FIB – asilva4940@gmail.com;
[2]Graduada em Biotecnologia – Universidade Federal da Integração Latino-Americana – UNILA – thaismigliorini15@gmail.com;
[3]Professor Me. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB - mamantunes@gmail.com;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Algoritmo, ChatGPT, Google, Tecnologia.

Introdução: O Google revolucionou a forma como buscamos informações na internet. Desde seu surgimento em 1998, o motor de busca consolidou-se como uma das principais ferramentas de acesso ao conhecimento, atuando como uma vasta biblioteca digital capaz de indexar e organizar bilhões de páginas da World Wide Web. Seu sistema de busca baseia-se em algoritmos sofisticados que analisam palavras-chave, relevância e autoridade das fontes, oferecendo resultados rápidos e diversificados — desde artigos científicos até notícias, imagens, vídeos e documentos de acordo com Levy (2011). Para Teixeira (2025) o avanço da inteligência artificial (IA) generativa inaugurou uma nova forma de interação com o conhecimento. Ferramentas como o ChatGPT, desenvolvidas pela OpenAI, não apenas recuperam informações, mas compreendem e produzem linguagem natural, permitindo respostas personalizadas, explicações contextuais e até mesmo a criação de conteúdo original. Essa mudança representa uma transição importante: enquanto o Google funciona como um ponto de partida para a busca de dados, o ChatGPT atua como um agente conversacional capaz de sintetizar, interpretar e adaptar o conhecimento às necessidades do usuário. Dessa forma, comparar o Google e o ChatGPT significa analisar duas abordagens complementares na relação entre o ser humano e a informação — uma fundamentada na busca e outra no diálogo —, ambas essenciais para compreender o futuro do acesso e da mediação digital do conhecimento, Castells (2024).

Objetivos: O presente estudo tem por objetivo comparar as abordagens tecnológicas do Google e do ChatGPT, explorando as diferenças entre seus algoritmos e formas de interação com o usuário. Busca-se compreender como essas ferramentas moldam a maneira de buscar, interpretar e produzir conhecimento, destacando as vantagens e limitações de cada uma e suas implicações na relação entre humanos e informação.

Relevância do Estudo: De acordo com Russel (2023) discute-se amplamente o papel da Inteligência Artificial (IA) e seus impactos na forma como as pessoas interagem com a informação e com o conhecimento. Contudo, ainda há confusão conceitual ao comparar ferramentas como o Google e o ChatGPT, especialmente quanto à sua aplicabilidade e eficiência na realização de pesquisas online. Surge, assim, o questionamento: qual dessas tecnologias oferece os melhores resultados na busca por informações e em que situações cada uma se mostra mais vantajosa para o usuário? Este estudo se propõe a esclarecer as diferenças fundamentais entre essas plataformas, analisando como seus algoritmos e modelos de funcionamento influenciam a maneira de buscar, processar e apresentar

ISSN 2358-6044
2025

informações. Além disso, busca-se compreender em quais contextos cada ferramenta apresenta maior utilidade, seja na navegação e exploração da internet, seja na interpretação e geração de conteúdos personalizados. Essa análise é essencial para entender como Google e ChatGPT se complementam no ecossistema digital contemporâneo, oferecendo abordagens distintas, mas igualmente relevantes, para o acesso e a produção do conhecimento.

Materiais e métodos: O trabalho, de natureza teórica e prática, é resultado de pesquisa bibliográfica, utilizando-se da análise da opinião de alguns autores contidas na literatura especializada e da elaboração de código com os testes realizados. Conforme Cervo e Bervian (2012), considerando-se que essa pesquisa visa explicar um problema tendo como base as contribuições de outros autores considerados relevantes, podendo ser realizada independentemente ou como parte de pesquisa descritiva ou experimental.

Resultados e discussões: O Google e o ChatGPT desempenham papéis distintos, mas complementares, na busca e produção de informação. O Google atua como um buscador indexa e organiza páginas web, permitindo ao usuário comparar diferentes fontes e verificar dados rapidamente. Enquanto isso, há confiabilidade riscos informações, pois muitos resultados podem conter notícias falsas ou conteúdo não verificado. Além disso, uh anúncios e resultados patrocinados podem interferir na objetividade da busca. Por outro lado, o ChatGPT oferece uma experiência mais interativo e personalizado, providenciando respostas diretas ao invés de apenas apresentar links. Ele se destaca por explicar conceitos de forma contextualizada e permitir a continuidade no diálogo, o que facilita a aprendizagem. No entanto, apresenta limitações na atualização dos dados, o que pode gerar respostas imprecisas sobre temas muito recentes. Assim, conclui-se que o Google é mais adequado para ampla pesquisa e verificação das fontes, enquanto o ChatGPT é ideal para interpretação e compreensão dos conteúdos, tornando-se ferramentas complementares no ambiente digital contemporâneo.

Conclusão: Tanto o Google quanto o ChatGPT são ferramentas essenciais na era digital, cada uma com características que se complementam. O Google destaca-se pela amplitude de informações e pela possibilidade de comparar diferentes fontes, enquanto o ChatGPT se sobressai pela interatividade e pela clareza nas explicações. Com o uso combinado dessas tecnologias, o usuário pode alcançar uma pesquisa mais completa, crítica e eficiente, aproveitando o melhor de cada recurso para ampliar o acesso e a compreensão do conhecimento.

Referências:

CASTELLS, M., **Sociedade em rede.** 18. ed. São Paulo: Paz e Terra, 2024.

CERVO, A. L.; BERVIAN, A. **Metodologia Científica**. 5. ed. São Paulo: Prentice Hall, 2012.

Levy, S**. Google: A Biografia** - **Como o Google pensa, trabalha e molda nossas vidas**, 1.ed., São Paulo, Kindle Editions, 2021

Teixeira. M.A., **ChatGPT vs Google [2025] – Comparação de recursos de pesquisa e IA!** Disponível em: https://www.demandsage.com/chatgpt-vs-google/. Acesso em: 10 out. 2025.

RUSSELL, S. **Inteligência Artificial: Uma Abordagem Moderna.** 4. ed. São Paulo, Pearson, 2023.

ISSN 2358-6044
2025

COMPARAÇÃO DO SAMBA4 AO WINDOWS SERVER: ANÁLISE COMPARATIVO EM RELAÇÃO À FUNCIONALIDADE E CUSTO-BENEFÍCIO

Erick Ohashi Silva; Felipe da Silva Gordiano; Gabriel Ferreira Pinheiro Lira de Oliveira; Claudines Taveira Torres.

Aluno de Redes de Computadores – Faculdades de Tecnologia de Bauru – FATEC – erick.silva92@fatec.sp.gov.br;

Aluno de Redes de Computadores – Faculdades de Tecnologia de Bauru – FATEC – felipe.gordiano@fatec.sp.gov.br;

Aluno de Redes de Computadores – Faculdades de Tecnologia de Bauru – FATEC – gabriel.oliveira272@fatec.sp.gov.br;

Professor do curso de Redes de Computadores – Faculdades de Tecnologia de Bauru – Fatec – claudines.torres@fatec.sp.gov.br.

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Samba4, Windows Server, Active Directory, Servidores, Custo-Beneficio

Introdução: O crescimento da demanda por soluções de rede seguras e eficientes tem levado empresas a buscarem alternativas de menor custo e alta performance. O Windows Server, amplamente utilizado no meio corporativo, oferece recursos robustos e suporte técnico consolidado, mas exige alto investimento em licenciamento. O Samba4, é uma ferramenta livre que oferece serviços de Active Directory (AD) em sistemas baseados em Linux, permitindo a integração com máquinas Windows em redes corporativas. De acordo com o portal Linuxsolutions (2023), o projeto do Samba foi criado em 1992 por Andrew Tridgell, com o objetivo de implementar os protocolos Server Message Block (SMB) e Common Internet File System (CIFS) em sistemas Unix, possibilitando o compartilhamento de arquivos com o Windows.

Objetivos: O objetivo principal é demonstrar que, com o Samba 4, é possível reproduzir com eficácia as principais funcionalidades encontradas em servidores proprietários, como o Windows Server, reduzindo custos e mantendo um alto nível de segurança e desempenho.

Relevância do Estudo: A pesquisa é relevante por propor uma análise técnica e econômica entre uma solução paga e uma gratuita, considerando o impacto financeiro e operacional sobre as organizações. Dessa forma, contribui para decisões estratégicas na escolha de tecnologias de rede, especialmente em instituições que buscam reduzir custos sem comprometer a eficiência dos serviços.

Materiais e métodos: O estudo foi realizado com base em revisão bibliográfica e experimentação prática. Para a demonstração prática, foi utilizado o ambiente Ubuntu Server 24.04, com recursos oficiais que foram disponibilizados no site do Samba (2024) para a instalação da versão 4.22.1 do Samba4, que foi configurado como controlador de domínio. A instalação e configuração incluíram pacotes essenciais como Wget, que segundo Andrei (2025) oferece suporte à FTP, SFTP, HTTP e HTTPS, há também o ACL, Xattr, que permite atribuir pares de nomes e valor a arquivos e diretórios, sendo ambos essenciais para a gestão de usuários no Samba4 (Ribeiro, 2024), Python3, Winbind, segundo o portal Debian (2025), o serviço Winbind possibilita que o Linux autentique usuários do Active Directory e gerencie

seus grupos, além de permitir acesso a recursos do Windows Server, e por último o Chrony. Para comparação, utilizou-se o Windows Server 2025, configurado com Active Directory Domain Services (AD DS), DNS e Group Policy Management(GPO). As funcionalidades de ambos os sistemas foram testadas quanto à criação de usuários, grupos e políticas de acesso. **Resultados e discussões:** Os resultados demonstraram que o Samba4 oferece desempenho compatível ao Windows Server em controle de domínio e gerenciamento de usuários, sendo uma solução gratuita e flexível. No entanto, sua instalação exige maior conhecimento técnico e suporte depende da comunidade *open source*. O Windows Server, por outro lado, destaca-se pela facilidade de uso e suporte oficial, mas apresenta custo elevado. Em um cenário com 100 usuários, o investimento em licenças do Windows Server pode ultrapassar R$120.000,00 segundo o valor disponibilizado pela Microsoft(2025), enquanto o Samba4 não exige custo de licenciamento, limitando o investimento ao profissional responsável pela administração.

Conclusão: Conclui-se que o Samba4 é uma alternativa eficiente e econômica ao Windows Server, especialmente indicada para pequenas e médias empresas que possuem equipes com conhecimento técnico em Linux. O Windows Server mantém-se como a melhor opção para organizações que priorizam estabilidade, suporte técnico e integração nativa com o ecossistema Microsoft. A escolha entre as soluções deve considerar o perfil da empresa, orçamento disponível e capacitação da equipe de TI.

Referências –

ANDREI. L. **Wget Linux: O Que é, Como Instalar e Exemplos de Comandos Wget**. 2025. Disponível: https://www.hostinger.com.br/tutoriais/como-usar-o-comando-wget-no-linux. Acessado em: 20 abr. 2025.

DEBIAN. **Pacote: winbind (2:4.9.5+dfsg-5+deb10u5) [security]**. 2025. Disponível em: https://packages.debian.org/buster/winbind. Acessado em: 20 abr. 2025.

LINUXSOLUTIONS. **O que é Samba4.** 2023. Disponível em: https://linuxsolutions.com.br/o-que-e-Samba4/. Acessado em: 11 abr. 2025.

MICROSOFT. **Comprar Windows 11 Home - Microsoft Store Brazil.** 2025. https://www.microsoft.com/pt-br/d/windows-11-home/dg7gmgf0krt0. Acessado em: 13 maio. 2025.

RIBEIRO. U. **Domine Access Control Lists (ACLs) no Linux: Controle de Acesso Granular para Seus Arquivos**. 2024. Disponível em: https://www.certificacaolinux.com.br/domine-access-control-lists-acls-no-linux-controle-de-acesso-granular-para-seus-arquivos

SAMBA. **Configurando o Samba como um controlador de domínio do Active Directory. 2024.** Disponível em: https://wiki.Samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller. Acessado em: 02 maio. 2025.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

ATAQUES DE PHISHING E DEEP FAKES: UMA ANÁLISE SOBRE GOLPES DE CATFISHING E MEDIDAS DE DEFESA

[1]Marcelo Machado Pereira; [2]Lyan Gabriel Ruiz Morales; [3]Ivan Leal Morales
[1]Cientista de Dados Bauru – Cientista da Computação – FIB - machado.pereira@unesp.br
[2]Aluno do Curso Ciência da Computação - FIB - lyan.grmorales@gmail.com
[3]Ms Professor do Curso de Ciência da Computação – FIB – ilmoralesbr@hotmail.com

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Phishing, Deep Fakes, Golpes, Catfishing, Segurança

Introdução: A crescente sofisticação da tecnologia, especialmente no campo da inteligência artificial, tem dado origem a novas e complexas ameaças à segurança digital. Entre elas, destacam-se os ataques de phishing e a manipulação de mídia através de deep fakes. Este trabalho tem como objetivo analisar como a combinação dessas técnicas tem sido utilizada em golpes de catfishing, termo americano utilizado para descrever o ato de criação de um perfil falso em redes sociais ou em sites de relacionamento(CASTRO; ZAGANELLI, 2022), além de propor medidas de defesa eficazes para mitigar esses riscos.

Objetivos: Analisar as técnicas utilizadas em ataques de phishing que se aproveitam de deep fakes para criar perfis falsos e enganosos em golpes de catfishing além de mapear os tipos de dados que são visados nesses ataques (financeiros, pessoais, etc.) e as consequências para as vítimas.

Relevância do Estudo: O estudo sobre ataques de phishing, deep fakes e catfishing possui uma relevância significativa para a sociedade, especialmente em um mundo cada vez mais digitalizado e conectado. Segundo (SANTOS, 2023) este é um desafio contínuo que exige a colaboração de especialistas em segurança, legisladores, empresas e cidadãos para mitigar os riscos e garantir um ambiente digital mais seguro e protegido.

Materiais e métodos: Este trabalho, de abordagem teórica e prática, resultou de uma pesquisa bibliográfica que analisou as opiniões de diferentes autores. Conforme Cervo e Bervian (2012), essa pesquisa busca explicar um problema com base nas contribuições relevantes de outros autores e pode ser conduzida de forma independente ou como parte de uma pesquisa descritiva ou experimental.

Resultados e discussões: O estar próximo já não se faz tão necessário quanto há quinze ou vinte anos. A falta de proximidade é, atualmente, preenchida por *SMS's* e *emojis* exibidos na tela de dispositivos conectados à internet. Apesar disso, o contato físico ainda é, em menor grau, essencial. Com todas as ferramentas tecnológicas disponíveis na palma das mãos, o contato pessoal pode ser constante, mesmo que apenas de forma virtual. Problemas são resolvidos ou iniciados, decisões são tomadas e relações são rompidas; muitas ações são realizadas por meio de simples mensagens. Desta forma, a presença física para a realização de determinadas atividades já não constitui requisito prioritário (MORAES; BRANDÃO, 2018). O *catfishing*, por possibilitar que o indivíduo se oculta por trás de uma identidade que não lhe pertence, é frequentemente utilizado como meio para a prática de outros crimes, como fraude ou estelionato. É comum que a vítima seja induzida a iniciar um relacionamento virtual e passe a confiar em seu parceiro, que, posteriormente, solicita dinheiro, presentes ou tenta aplicar

golpes. A partir dos dados e casos analisados, percebe-se que as políticas de proteção das redes sociais não são suficientemente confiáveis, tampouco seguras. Dessa forma, é fundamental que o Estado intervenha a fim de cumprir seu dever de tutelar direitos e proteger as pessoas (CASTRO; ZAGANELLI, 2022). Os crimes digitais aproveitam-se do uso da internet para atingir inúmeras vítimas em larga escala. A conexão de milhares de pessoas por meio de redes fixas ou móveis permite que, em pelo menos uma tentativa de crime, haja alguma vítima, o que evidencia a amplitude de alcance e de acesso dessas práticas ilícitas (ALVES; FLORES, 2023). Para mitigar o problema do estelionato perpetrado pelo crime organizado no ambiente virtual, bem como definir formas de proteção social, é necessário que medidas de segurança sejam efetivamente adotadas (ALVES; FLORES, 2023). Contudo, apesar dos avanços tecnológicos e legislativos, o crime de falsa identidade cometido pela internet ainda carece de tipificação específica, o que faz com que as vítimas de determinadas práticas lesivas permaneçam desamparadas (CASTRO; ZAGANELLI, 2022). A implementação de políticas públicas que promovam a segurança digital, aliada à utilização de inteligência artificial, pode contribuir para o desenvolvimento de ferramentas capazes de detectar comportamentos anormais em acessos a dados, indicando possíveis tentativas de violação dos sistemas de proteção (SANTOS, 2023). Por fim, a segurança cibernética é uma responsabilidade compartilhada por empresas, organizações e indivíduos (MACHADO; MORALES, 2023).

Conclusão: A convergência entre a crescente sofisticação tecnológica e a fragilidade das relações virtuais cria um cenário propício para ataques cibernéticos complexos, como o *catfishing* impulsionado por *phishing* e *deep fakes*. Este estudo demonstrou que a ausência de proximidade física, preenchida por interações digitais constantes, facilita a criação de identidades falsas, as quais são frequentemente utilizadas para fins criminosos, como fraude e estelionato. A pesquisa revelou que as políticas de segurança das redes sociais são insuficientes para conter esses crimes, deixando as vítimas desprotegidas. A tipificação específica do crime de falsa identidade na internet ainda é uma lacuna legislativa, o que agrava a vulnerabilidade dos usuários. Para mitigar esses riscos, é crucial a colaboração entre especialistas em segurança, legisladores e empresas. A implementação de políticas públicas que promovam a segurança digital, aliada ao uso estratégico da Inteligência Artificial para detectar atividades anômalas, surge como uma necessidade urgente para proteger os cidadãos e garantir um ambiente digital mais seguro e confiável.

Referências:

ALVES, José G.; FLORES, Andréa. **Análise da prática do crime de fraude perpetrado por organizações criminosas e suas consequências no ambiente.** Campo Grande: UFMS, 2023.

CASTRO, Ana Flávia C. D. de;ZAGANELLI, Margareth V.; **Catfishing: crime e falsa Identidade?** Revista de Estudos Jurídicos UNESP. Franca: UNESP, 2022.

CERVO, A. L.; BERVIAN, A. **Metodologia Científica**. 5. ed. São Paulo: Prentice Hall, 2012.

MACHADO,M;MORALES,I. **Estratégias de defesa contra cyber ataques.** Disponível em ANAIS CIENCIA DA COMPUTACAO 2023.pdf Acesso 25 out 2025.

MORAES, Jefferson G.; BRANDÃO, Washington L. de O. **Relacionamentos Virtuais: uma Análise acerca dos padrões comportamentais dos "Catfish".** Revista Ensino, Educação e Ciências Humanas. Macapá: UNIFAP, 2018.

SANTOS, Roberta C. dos; **O Cibercrime e a investigação dos ataques cibernéticos: a experiência paulistana.** São Paulo: Mackenzie, 2023.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

ESTRATÉGIAS DE PREVENÇÃO E MITIGAÇÃO DE ATAQUES CIBERNÉTICOS EM AMBIENTES IOT

[1]Marcelo Machado Pereira; [2]Lyan Gabriel Ruiz Morales, [2]Ivan Leal Morales,
[1]Bacharel em Ciências da Computação – FIB - machado.pereira@unesp.br
[2]Aluno Ciência da Computação – FIB – drlyanmorales@gmail.com
[3]Ms Professor do Curso de Ciência da Computação – FIB – ilmoralesbr@hotmail.com

Grupo de trabalho: CIÊNCIAS DA COMPUTAÇÃO

Palavras-chave: Ciber Segurança, Internet das Coisas, Dados, Proteção.

Introdução: Com o avanço da transformação digital e a popularização da Internet das Coisas (IoT), dispositivos conectados estão cada vez mais presentes em residências, empresas e ambientes públicos. No entanto, essa conectividade também aumenta a superfície de ataque e os riscos de invasões, vazamentos de dados e uso indevido de informações pessoais. Segundo Tanenbaum (2003), a interconexão entre dispositivos requer protocolos e camadas de segurança adequadas, a fim de garantir confidencialidade, integridade e disponibilidade das informações trafegadas.

Objetivos: O presente trabalho tem como objetivo analisar os principais desafios e estratégias de cibersegurança aplicadas à Internet das Coisas, destacando mecanismos de proteção de dados, autenticação de dispositivos e prevenção contra ataques cibernéticos. Busca-se demonstrar soluções acessíveis e práticas que possam ser aplicadas tanto em ambientes domésticos quanto corporativos.

Relevância do Estudo: A relevância deste estudo está em discutir a necessidade urgente de segurança digital em um cenário onde dispositivos IoT controlam desde iluminação e temperatura até sistemas industriais e hospitalares. A falta de políticas de proteção e de padrões de segurança pode resultar em sérios danos econômicos e sociais. Assim, compreender e aplicar práticas de cibersegurança torna-se essencial para a confiabilidade e continuidade dos serviços conectados.

Materiais e métodos: A metodologia utilizada baseou-se em pesquisa bibliográfica e análise de estudos de caso de empresas que implementaram IA em seus sistemas de segurança. Segundo Cervo e Bervian (2002), a pesquisa bibliográfica busca examinar contribuições teóricas publicadas, proporcionando base para análise e comparação.

Resultados e discussões: Com o crescente uso dos dispositivos de IoT, a segurança cibernética ou Ciber Segurança tornou-se um dos maiores desafios para organizações e usuários domésticos. A integração entre dispositivos IoT e redes domésticas, corporativas e redes industriais depende de protocolos de comunicação seguros. Observou-se que vulnerabilidades comuns estão relacionadas à falta de criptografia, autenticação fraca e atualizações automáticas ausentes. Segundo a OWASP (2024), ataques como o *botnet Mirai* evidenciaram o impacto global que dispositivos desprotegidos podem causar. Entre as boas práticas identificadas, destacam-se: implementação de criptografia ponta a ponta entre dispositivos e servidores; autenticação multifator e controle de acesso baseado em funções; monitoramento contínuo e uso de inteligência artificial para detecção de anomalias; e educação do usuário, essencial para reduzir ataques de engenharia social. Além disso, a aplicação de políticas de atualização automática e segmentação de redes pode minimizar riscos em sistemas críticos. A adoção de frameworks de segurança específicos para IoT, como o IoT Security Foundation Framework, também contribui para padronizar medidas de

proteção. A colaboração entre fabricantes, desenvolvedores e usuários é fundamental para garantir um ecossistema mais resiliente. Dessa forma, a prevenção de ataques cibernéticos em redes IoT depende tanto de soluções tecnológicas quanto da conscientização de todos os envolvidos. Os aspectos gerais de segurança em sistemas IoT envolvem a confidencialidade, integridade e disponibilidade dos dados transmitidos. A confidencialidade assegura que apenas usuários autorizados tenham acesso às informações, enquanto a integridade garante que os dados não sejam alterados de forma indevida durante a transmissão. Já a disponibilidade visa manter os serviços ativos e acessíveis, mesmo diante de tentativas de ataque. Outro ponto relevante é a segurança física dos dispositivos, pois muitos sensores e atuadores são instalados em locais de fácil acesso, o que pode permitir adulterações manuais. A gestão de identidade e acesso é outro pilar essencial, exigindo políticas rigorosas de autenticação e autorização. O ciclo de vida do dispositivo — desde a fabricação até o descarte — deve incluir práticas seguras, como a remoção de credenciais padrão e o descarte adequado de dados sensíveis. A análise de vulnerabilidades e a realização periódica de testes de penetração ajudam a identificar falhas antes que sejam exploradas por agentes mal-intencionados. O uso de redes segmentadas e firewalls específicos para IoT também contribui para isolar dispositivos comprometidos, evitando a propagação de ameaças. Por fim, políticas de governança e conformidade com normas ABNT 27001 e a LGPD, fortalecem a segurança organizacional e a confiança dos usuários. Assim, um ambiente IoT seguro requer uma abordagem integrada que combine tecnologia, gestão de riscos e cultura de segurança cibernética.

Conclusão: Conclui-se que a cibersegurança é um pilar indispensável para o avanço seguro da Internet das Coisas. A pesquisa bibliográfica mostrou que, apesar dos benefícios trazidos pela automação e conectividade, a ausência de práticas de segurança pode comprometer toda a infraestrutura digital. O desenvolvimento de dispositivos IoT deve considerar a segurança desde o projeto (“security by design”), além de envolver o usuário como parte ativa da proteção. Futuras pesquisas podem abordar soluções baseadas em blockchain e aprendizado de máquina aplicadas à proteção de dados em ambientes IoT.

Referências

CERVO, A.L.; BERVIAN, A. **Metodologia científica**. 5.ed. São Paulo: Prentice Hall, 2002.

TANENBAUM, Andrew S.; SOUZA, Vandenberg D. de (trad.); JAMHOUR, Edgard (rev.). **Redes de computadores**. Rio de Janeiro: Elsevier, 2003.

OWASP. **IoT Security Guidelines**. Disponível em: <https://owasp.org/>. Acesso em: 05 out. 2025.

NIST. **Security and Privacy Controls for Information Systems and Organizations**. Special Publication 800-53, 2024.

ENISA. **Cybersecurity of IoT Devices: Good Practices for Manufacturers**. European Union Agency for Cybersecurity, 2023.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

COMO A LGPD SE APLICA AO TRATAMENTO DE COMANDOS DE VOZ EM ASSISTENTES VIRTUAIS COMO ALEXA E GOOGLE HOME

Caio Moreira Menoia[1]; João Vitor Casemiro de Lima[2]; Maria Lucia de Azevedo[3];
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB –
caio.menoia@alunos.fibbauru.br
[2]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB
joao.lima@alunos.fibbauru.br;
[3]Professora do curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB
maria.azevedo@fibbauru.br

Grupo de trabalho: Bacharelado em Ciência da Computação.

Palavras-chave: Lei Geral de Proteção de Dados, Assistentes Virtuais, Alexa, Google Home, Siri, LGPD, Ética.

Introdução: Na atualidade, observa-se que os assistentes virtuais estão cada vez mais humanizados. Com um simples “Ok Google”, acionamos um comando que inicia um chat de voz interativo, o que nos leva a questionar se estamos realmente seguros. Partindo desse princípio, este artigo analisa como as empresas promovem a privacidade do usuário e o impacto direto da Lei Geral de Proteção de Dados (LGPD) nesse contexto. Afinal, segundo Antônio Juarez Alencar, Eber Assis Schmitz e Leôncio Teixeira Cruz em sua pesquisa Assistentes Virtuais Inteligentes: Conceitos e Estratégias (2013), “Em síntese, os assistentes virtuais inteligentes propiciam a nossos clientes experiências prazerosas e enriquecedoras ao utilizarem os produtos e serviços que oferecemos”, contudo, não podemos olhar apenas para o lado fascinante, é necessário questionar se o produto que consumimos está dentro dos padrões de conformidade da LGPD.

Objetivos: Este estudo tem como objetivo aprofundar, de forma resumida, como as empresas lidam com a privacidade dos assistentes virtuais, abordando de que maneira elas garantem a transparência e a segurança no tratamento dos comandos de voz, com base nos princípios estabelecidos pela LGPD.

Relevância do Estudo: O ambiente doméstico é um espaço de intimidade por excelência. Conversas, hábitos e interações familiares. Todos esses são dados sensíveis, e a captura passiva e contínua desse ambiente representa um risco único à privacidade. A LGPD sendo uma legislação recente, e sua aplicação a tecnologias específicas ainda é um campo em aberto. Este trabalho será um caso de estudo sobre como os princípios legais abstratos da lei se chocam com a realidade técnica de uma das tecnologias mais invasivas da atualidade.

Materiais e métodos: Neste estudo, foi realizada uma análise qualitativa com enfoque na legislação da LGPD e sua aplicação prática no tratamento de comandos de voz por assistentes virtuais, como Alexa, Google Home e Siri. Para isso, foram coletadas informações em fontes oficiais, documentos técnicos, pesquisas acadêmicas e relatórios de privacidade fornecidos pelas empresas responsáveis por esses dispositivos. Além disso, foram examinados casos reais e políticas de segurança para compreender como a transparência e a proteção de dados são implementadas na prática. A abordagem adotada busca integrar aspectos legais e tecnológicos, permitindo uma visão ampla e crítica sobre a segurança e a privacidade dos usuários no uso desses assistentes virtuais.

Resultados e discussões: A análise da aplicação da LGPD no tratamento de comandos de voz por assistentes virtuais como Alexa e o Google Home revela que os dados coletados por

ISSN 2358-6044
2025

esses dispositivos são, em sua maioria, pessoais e sensíveis, uma vez que envolvem informações diretamente vinculadas ao usuário, suas preferências, hábitos e até dados contextuais do ambiente. Segundo o portal oficial do Google Assistant os dispositivos ficam em “espera” até detectar a ativação por comando de voz, para então enviar a gravação aos servidores da ferramenta. Do ponto de vista da segurança, os dados de voz, por sua natureza biométrica, são considerados dados pessoais sensíveis pela LGPD (Art. 5º, II), exigindo um nível de proteção ainda mais elevado. A discussão aponta que, apesar das empresas investirem em criptografia e anonimização, os riscos de violação de dados ou mesmo o uso indevido por parte de aplicativos de terceiros integrados aos assistentes ("skills" ou "actions") representam uma camada adicional de vulnerabilidade.
Muitas empresas também oferecem a opção de exclusão manual dos dados salvos, coletados, mas a ausência de uma exclusão automática por padrão pode ser interpretada como uma violação. A efetiva garantia dos direitos do titular, como a revogação do consentimento (Art. 8º, §5º) e a solicitação de exclusão de seus dados (Art. 18, VI), também se mostra um desafio, muitas vezes obscurecida por processos burocráticos dentro das plataformas.

Conclusão: Este estudo permitiu concluir que a aplicação da LGPD ao universo dos assistentes virtuais de voz é não apenas pertinente, mas urgente. A captura passiva e contínua de dados em um ambiente íntimo, como o lar, coloca esses dispositivos no centro de um dos maiores desafios contemporâneos: a proteção da privacidade na era digital. Conclui-se que, embora as empresas estejam se adaptando formalmente à LGPD, a efetiva proteção do usuário vai além da mera existência de políticas de privacidade e termos de uso. Mecanismos de consentimento mais explícitos e educativos, o oferecimento de opções de privacidade robustas por padrão (como a desativação do armazenamento de áudio) e a garantia dos direitos do titular de forma descomplicada são passos essenciais que precisam ser consolidados.

Referências

ALENCAR, A. J.; SCHMITZ, E. A.; CRUZ, L. T. **Assistentes virtuais inteligentes: conceitos e estratégias**. [S.l.: s.n.], 2013.

BLOOMBERG. **Amazon workers are listening to Alexa conversations to make your device smarter.** 2019. Disponível em: https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio. Acesso em: 05 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 set. 2025.

GOOGLE. **Protecting your Google Assistant privacy**. Google Safety Center. Disponível em: https://safety.google/products/assistant/. Acesso em: 05 set. 2025.

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

IA: BOAS PRÁTICAS NA GESTÃO DA SEGURANÇA DAS EMPRESAS

[1]Marcelo Machado Pereira; [2]Lyan Gabriel Ruiz Morales, [2]Ivan Leal Morales,
[1]Bacharel em Ciências da Computação – FIB - machado.pereira@unesp.br
[2]Aluno Ciência da Computação – FIB – drlyanmorales@gmail.com
[3]Ms Professor do Curso de Ciência da Computação – FIB – ilmoralesbr@hotmail.com

Grupo de trabalho: CIÊNCIAS DA COMPUTAÇÃO

Palavras-chave: Inteligência Artificial, Cibersegurança, Monitoramento, Redes, Automação

Introdução: Com o crescimento do volume de dados e a complexidade dos ataques cibernéticos, a Inteligência Artificial (IA) tornou-se uma ferramenta essencial na proteção e monitoramento das redes corporativas. A capacidade da IA de aprender padrões e identificar anomalias em tempo real permite que as empresas respondam mais rapidamente a incidentes de segurança. De acordo com o relatório da ENISA (2024), o uso de IA na cibersegurança tem se mostrado eficaz para prevenir ataques e mitigar vulnerabilidades antes que causem danos significativos.

Objetivos: Este trabalho tem por objetivo apresentar boas práticas no uso da Inteligência Artificial voltadas à proteção e monitoramento das redes empresariais. Busca-se demonstrar como a IA pode ser utilizada para automatizar processos de detecção de ameaças, análise de tráfego e resposta a incidentes, garantindo maior eficiência e segurança nas operações.

Relevância do Estudo: A aplicação de IA na segurança cibernética é um dos campos mais promissores da atualidade. Com a crescente digitalização dos negócios, proteger as redes corporativas tornou-se prioridade estratégica. Este estudo é relevante por abordar as melhores práticas e recomendações que permitem às empresas implementarem soluções de IA de forma ética, segura e eficiente, reduzindo riscos e fortalecendo suas defesas digitais.

Materiais e métodos: A metodologia utilizada baseou-se em pesquisa bibliográfica e análise de estudos de caso de empresas que implementaram IA em seus sistemas de segurança. Segundo Cervo e Bervian (2002), a pesquisa bibliográfica busca examinar contribuições teóricas publicadas, proporcionando base para análise e comparação.

Resultados e discussões: Segundo Security Business, em 2024, o custo médio de violação de dados alcançou US$ 4,9 milhões, representando um aumento de 10% em relação ao ano anterior, conforme aponta o novo Data Breach Report da IBM. NIST comenta que a escolha da Abordagem correta de gerenciamento de riscos e as ferramentas de apoio é importante para garantir que os sistemas estejam adequadamente protegidos. Há necessidade de que os projetistas compreendam como alcançar soluções de segurança em seus respectivos ambientes operacionais e que os altos responsáveis tenham informações suficientes para tomar decisões fundamentadas em risco e gerenciar seus riscos de cibersegurança. Syracuse (2025) comenta que à medida que as ameaças digitais se tornam mais complexas, as organizações devem usar diferentes tipos de IA em segurança cibernética para proteção dos dados. Os resultados demonstram que o uso de IA nas redes corporativas aumenta significativamente a capacidade de resposta a ataques e a eficiência dos times de segurança. Os quadros mostram as boas práticas e desafios:

Recurso de IA	Descrição
Análise comportamental	Aprende o comportamento normal da rede e identifica anomalias que indicam possíveis ameaças.
Detecção e resposta a ameaças em tempo real	Processa dados em grande escala rapidamente, permitindo bloqueios e reações automáticas.
Inteligência preditiva sobre ameaças	Analisa padrões históricos e globais para antecipar ataques e reforçar defesas.
Gerenciamento automatizado de vulnerabilidades	Escaneia sistemas continuamente, detectando falhas críticas e priorizando correções.
Detecção aprimorada de phishing e malware	Examina conteúdo de e-mails e links para identificar tentativas sofisticadas de ataque.
Gerenciamento aprimorado de identidade e acesso (IAM)	Analisa padrões de login para detectar acessos suspeitos e acionar medidas de proteção.
Implementação de confiança zero	Aplica o princípio de não confiar em nenhum usuário ou dispositivo por padrão, ajustando acessos dinamicamente.

Desafio	Descrição
Qualidade dos dados	Modelos de IA dependem de dados confiáveis; dados imprecisos comprometem a eficácia da detecção.
Ataques adversários	Criminosos podem manipular a IA com dados maliciosos, exigindo proteção contra envenenamento de modelos.
Supervisão humana	A IA precisa da experiência humana para interpretação e resposta a ameaças complexas.
Integração com sistemas existentes	A adoção da IA pode ser dificultada por sistemas legados e infraestrutura incompatível.
Ética e privacidade	O uso da IA exige cuidado com a privacidade e cumprimento das normas de proteção de dados.

Conclusão: Fica evidente que a cibersegurança precisa evoluir na mesma velocidade das ameaças. A inteligência artificial surge como aliada estratégica, oferecendo recursos como análise comportamental, resposta em tempo real e detecção preditiva. É fundamental enfrentar desafios como a qualidade dos dados, integração e preocupações éticas. Caminhos viáveis incluem o uso de abordagens baseadas em risco recomendadas pelo NIST, o fortalecimento da supervisão humana e a capacitação de projetistas e gestores para tomarem decisões fundamentadas. A aplicação de políticas zero Trust e automação no gerenciamento de vulnerabilidades também se mostram eficazes. A adoção da IA dependerá de uma implementação cuidadosa, sustentada por governança sólida, treinamento contínuo e investimento em infraestrutura. As organizações poderão equilibrar inovação com segurança, mantendo-se resilientes frente às ameaças digitais crescentes. Embora os métodos tradicionais de prevenção desempenhem um papel importante na segurança cibernética, se mostram cada vez mais limitados diante das ameaças modernas e devem evoluir dentro dos requisitos atuais, integrando-se a soluções baseadas em IA para formar defesas em camadas mais robustas.

Referências:

BUSINESS, S. **Crescem gastos com falhas de cibersegurança.** Disponível em Crescem os custos com falhas na cibersegurança, revela IBM Acesso em 16 out 2025

CERVO, A. L.; BERVIAN, A. **Metodologia científica**. 5. ed. São Paulo: Prentice Hall, 2002.

IBM. O QUE É ZERO TRUST. Disponível em **O que é zero trust? | IBM** Acesso em 22 out 2025.

NIST. **Cybersecurity Risk Management.** Disponível em Resultados da pesquisa | NIST. Acesso em 16 out 2025

SYRACUSE (2025). **AI in Cybersecurity: How AI is Changing Threat Defense.** Disponível em **AI in Cybersecurity: How AI is Changing Threat Defense.** Acesso em 16 out 2025

XX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2025

TRANSPORTE ACESSÍVEL SEGURO E SUSTENTÁVEL: APLICATIVO PARA MOBILIDADE URBANA

Paulo Henrique Yamashita Leão Pancini[1]; Gabriel Ferreira Pires dos Santos[2]; Yago de Souza Cardoso Dias[3]; Anderson Francisco Talon[4].
[1]Aluno de Redes de Computadores – Faculdade de Tecnologia de Bauru – FATEC – paulo.pancini@fatec.sp.gov.br;
[2]Aluno de Redes de Computadores – Faculdade de Tecnologia de Bauru – FATEC – gabriel.santos440@fatec.sp.gov.br;
[3]Aluno de Redes de Computadores – Faculdade de Tecnologia de Bauru – FATEC – yago.dias01@fatec.sp.gov.br;
[4]Professor do curso de Redes de Computadores – Faculdade de Tecnologia de Bauru – FATEC - anderson.talon@fatec.sp.gov.br.

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Rastreamento em tempo real; Transporte Público; ESP32; Firebase.

Introdução: O transporte público é um dos principais meios de deslocamento nas cidades e influencia na qualidade de vida da população. Em locais de médio porte, como Bauru, há falta de informações em tempo real, atrasos nas linhas e pouca acessibilidade digital.
De acordo com Araújo et al. (2011), a mobilidade urbana está diretamente ligada à acessibilidade e à qualidade dos serviços oferecidos, tornando essencial o uso de tecnologias que melhorem a comunicação entre usuários e veículos. Com base nessa necessidade, foi desenvolvido o Transporte Acessível, Seguro e Sustentável (TASS), um aplicativo móvel que permite acompanhar em tempo real a localização dos ônibus urbanos. O sistema busca melhorar a comunicação entre passageiros e veículos, reduzir o tempo de espera e tornar o transporte mais acessível e confiável.

Objetivos: O objetivo geral é desenvolver um aplicativo móvel integrado a um sistema embarcado e a um banco de dados em nuvem, capaz de mostrar em tempo real a localização dos ônibus urbanos.
Os objetivos específicos são: 1. Implementar o rastreamento dos veículos com ESP32 e módulo GPS, enviando dados ao Firebase a cada 5 segundos; 2. Exibir no aplicativo as localizações atualizadas, de forma precisa aos usuários; 3. Integrar recarga digital via Pix e validação por NFC; 4. Adicionar um botão de pânico e a função de compartilhamento de viagens para maior segurança; 5. Permitir futuras integrações com órgãos públicos de transporte, otimizando o controle e a operação das frotas.

Relevância do Estudo: A ausência de informações atualizadas e seguras sobre o transporte urbano impacta diretamente o dia a dia dos usuários. Pilon (2009) destaca que sistemas de informação bem estruturados permitem maior confiabilidade e eficiência nos serviços de transporte coletivo.
O TASS surge como uma proposta de solução prática, usando tecnologias acessíveis para aproximar a população de serviços públicos mais eficientes. Além de contribuir para a mobilidade urbana e sustentabilidade, o projeto também incentiva a inclusão digital e o uso de Internet das Coisas (IoT), conceito amplamente discutido por Araújo et al. (2020) e Lima, Brino e Cardia Neto (2020) como pilares das cidades inteligentes e sustentáveis. Essas aplicações tecnológicas demonstram o potencial entre dispositivos e sistemas em nuvem, promovendo uma gestão mais inteligente do transporte coletivo.

ISSN 2358-6044
2025

Materiais e métodos: O projeto foi desenvolvido com base em uma arquitetura de três camadas principais, semelhante à estrutura proposta por Anefalos (1999), em estudos sobre gerenciamento e rastreamento de frotas, adaptada aqui ao contexto de transporte público urbano: 1. Hardware (ESP32 com módulo GPS NEO-6M): coleta as coordenadas do ônibus e envia os dados a cada 5 segundos para o banco de dados; 2.Banco de Dados (Firebase Realtime Database): recebe e armazena os dados enviados pelo ESP32, garantindo atualização instantânea e sincronização automática com o aplicativo; 3.Aplicativo mobile (React Native + Expo): exibe os ônibus no mapa em tempo real e integra recursos como recarga Pix, NFC, notificações e botão de pânico.
Durante o desenvolvimento, foram realizados testes práticos com o ESP32 e o Firebase, comprovando a estabilidade do envio e a precisão na atualização dos dados.

Resultados e discussões: Os testes mostraram que o sistema é funcional e estável na atualização dos dados em tempo real. O ESP32, aliado ao módulo GPS, apresentou boa precisão na captura das coordenadas, com margem de erro média de 2,5 a 5 metros. O intervalo de 5 segundos configurado para envio ao Firebase mostrou-se ideal, garantindo fluidez no rastreamento sem sobrecarregar a rede. O aplicativo exibiu corretamente os veículos no mapa, e os recursos adicionais, como recarga Pix, publicações de trânsito e botão de pânico foram implementados com sucesso.

Conclusão: O TASS demonstra a viabilidade de integrar tecnologias acessíveis para tornar o transporte urbano mais eficiente, seguro e sustentável. A solução apoia usuários e a gestão pública, mostrando-se um caminho para cidades inteligentes e sustentáveis.

Referências

ANEFALOS, L. C. **Gerenciamento de frotas do transporte rodoviário de cargas utilizando sistemas de rastreamento por satélite.** 1999. Dissertação (Mestrado em Economia Aplicada) – Escola Superior de Agricultura Luiz de Queiroz, Universidade de São Paulo, Piracicaba. Disponível em: https://www.teses.usp.br/teses/disponiveis/11/11132/tde-16102002-181518/pt-br.php. Acesso em: 5 jun. 2025.

ARAÚJO, J. H. de et al. **Smart Cities: um estudo prospectivo sobre Internet das Coisas (IoT) aplicada ao setor de mobilidade urbana.** Cadernos de Prospecção, v. 13, n. 1, p. 138–152, 2020. Disponível em: https://periodicos.ufba.br/index.php/nit/article/view/32691. Acesso em: 5 jun. 2025.

ARAUJO, M. R. M. et al. **Transporte público coletivo: discutindo acessibilidade, mobilidade e qualidade de vida.** Psicologia & Sociedade, v. 23, n. 3, p. 573–582, 2011. Disponível em: https://www.scielo.br/j/psoc/a/XWXTQXKJ44BtT5Qw7dLWgvF/. Acesso em: 5 jun. 2025.

LIMA, M. R. B.; BRINO, G.; CARDIA NETO, J.B. **Cidades inteligentes: casos e perspectivas para as cidades brasileiras.** *Revista Interface Tecnológica*, v. 17, n. 2, p. 180–192, 2020. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/915. Acesso em: 5 jun. 2025.

PILON, J. **A. Sistema de informação ao usuário do transporte coletivo por ônibus na cidade de Vitória-ES**. 2009. Dissertação (Mestrado em Engenharia de Produção) Universidade Tecnológica Federal do Paraná. Disponível em: https://repositorio.utfpr.edu.br/jspui/handle/1/915. Acesso em: 5 jun. 2025.