RBTI

# Revista Brasileira em Tecnologia da Informação

ISSN: 2675-1828

V. 6, N.1, 2024

## Conheça as novas tendências para Tecnologia da Informação.

FATEC Campinas

Centro Paula Souza

SÃO PAULO GOVERNO DO ESTADO

Janeiro a Junho 2024

RBTI – Revista Brasileira em Tecnologia da Informaçãoa
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

# EDITORIAL

É com grande satisfação que apresentamos o Volume 06, Número 1, da *Revista Brasileira de Tecnologia da Informação*, referente ao primeiro semestre de 2024. Esta edição reúne estudos que abordam temas fundamentais no campo da tecnologia da informação (TI), com foco em aplicações práticas e teóricas, em diferentes contextos, demonstrando a relevância crescente das inovações tecnológicas em diversas áreas do conhecimento.

O artigo de Djones Braz de Araujo Costa e Flávia dos Santos Alves, intitulado *Os Impactos da Inteligência Artificial (IA) na Enfermagem*, examina como a IA está transformando práticas na área de saúde, particularmente na enfermagem. A pesquisa aborda as aplicações dessa tecnologia em diagnósticos, monitoramento e otimização de processos, além das questões éticas relacionadas à supervisão humana e proteção de dados.

Já o trabalho de Anderson Julianelli do Nascimento e Djones Braz de Araujo Costa, *A Segurança da Informação: uma observação sobre os aspectos técnicos, humanos, sociais e jurídicos conhecidos*, explora os desafios e as práticas voltadas à proteção de dados digitais. A pesquisa analisa os impactos dos fatores humanos, técnicos e legais, destacando a adaptação da legislação brasileira ao contexto atual de segurança cibernética.

Em seguida, o artigo de Eduardo Nascimento e João Emmanuel S'Alkmin Neves, *Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação*, discute o modelo Zero Trust, apresentando suas vantagens e desafios para a segurança de redes e o gerenciamento de riscos. A obra aprofunda-se nos benefícios dessa abordagem inovadora e nos desafios culturais e financeiros para sua implementação.

O impacto da tecnologia no desenvolvimento sustentável é tratado no artigo de Alan Rodrigues Cola, Carlos Rogério Pegrucci de Souza e João Emmanuel D'Alkmin Neves, *Impacto da tecnologia de informação na sustentabilidade da indústria*. A análise de dois estudos de caso revela como a adoção da TI pode otimizar processos produtivos, reduzir desperdícios e aumentar a sustentabilidade, reforçando o papel da indústria 4.0 na preservação de recursos naturais.

No campo do aprendizado de máquina, o estudo de Stewart Evangelista Gonçalves, *Uma revisão sistemática da literatura sobre a utilização de algoritmos de Machine Learning para realização de análise de sentimentos*, apresenta uma análise abrangente dos algoritmos mais utilizados em Processamento de Linguagem Natural (NLP) para a análise de sentimentos, destacando a crescente adoção de técnicas como Naive Bayes, SVM e Random Forest.

A importância da TI na construção de cidades inteligentes e sustentáveis é destacada por Vinícius Teixeira Juste, Wandderley Luiz de Freitas Apaza e João Emmanuel D'Alkmin Neves, no artigo *O papel das tecnologias da informação na construção de cidades inteligentes e sustentáveis*. A pesquisa examina como tecnologias como IoT, sensores e IA podem otimizar o consumo de energia e reduzir os impactos ambientais nas áreas urbanas, alinhando-se com os Objetivos de Desenvolvimento Sustentável (ODS).

No campo da ética e da educação, Marcos Ferreira Guedes da Costa discute o imaginário coletivo e as narrativas míticas no artigo *As míticas histórias: contos e histórias*. A obra explora como alunos do curso de Gestão da Produção Industrial da FATEC Itatiba revisitaram mitos universais, conectando suas experiências pessoais com criaturas mitológicas e a evolução ética dos comportamentos humanos.

Finalmente, o artigo de Everton Trevisan Silva, *Segurança da informação em internet banking*, revisa a literatura sobre a segurança em transações bancárias online, um tema cada vez mais relevante com o aumento dos ataques cibernéticos. A pesquisa foca nas ameaças emergentes e nas melhores práticas para proteger os usuários e os sistemas financeiros digitais.

Esta edição da *Revista Brasileira de Tecnologia da Informação* reafirma o compromisso com a divulgação de pesquisas que trazem soluções inovadoras e reflexões críticas sobre o papel da TI em diferentes setores da sociedade. Agradecemos aos autores, revisores e colaboradores que tornaram possível a publicação deste volume. Desejamos a todos uma leitura proveitosa e inspiradora.

Editor-Chefe

*Revista Brasileira de Tecnologia da Informação*

RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

# Impacto da Tecnologia de Informação na Sustentabilidade da Indústria

**Alan Rodrigues Cola**
Fatec Araraquara, alanrodriguescola93@gmail.com
**Carlos Rogerio Pegrucci De Souza**
Fatec Araraquara, carlos.souza101@fatec.sp.gov.br
**João Emmanuel D'Alkmin Neves**
Fatec Americana, jeneves@gmail.com

**RESUMO**

No cenário atual diante da escassez de matérias primas vitais para a indústria e desafio da sustentabilidade, a adoção da tecnologia da informação nos processos produtivos, o que pode ser classificado como parte da indústria 4.0, é um caminho para manter competitividade e a garantir a sustentabilidade. O objetivo deste trabalho é analisar os impactos da adoção da tecnologia da informação nos processos produtivos, para isso foi feita uma revisão bibliográfica e um estudo de caso. Através da comparação dos resultados observados em uma pequena ourivesaria e da linha de montagem final de uma grande empresa do setor automobilístico de Araraquara, foi possível constatar os impactos positivos em ambos os casos apesar das proporções. Ambos os casos demonstram a tecnologia da informação como um caminho para a sustentabilidade, pois as duas empresas comparadas tiveram redução de desperdícios e recursos gastos no processo, mesmo tratando-se de empresas muito diferentes, tanto em porte, quanto no ramo de atuação.

**Palavras-Chave**: Indústria; Sustentabilidade; Tecnologia.

Artigo Submetido: 12/06/2023

Artigo Aceito Publicação: 15/05/2024

# Impact of information technology on industry sustainability

**ABSTRACT**

In the current scenario facing the shortage of vital raw materials for the industry and the challenge of sustainability, the adoption of information technology in production processes, which can be classified as part of industry 4.0, is a way to maintain competitiveness and ensure sustainability. The objective of this work is to analyze the impacts of the adoption of information technology on production processes, for which a bibliographical review and a case study were carried out. By comparing the results observed in a small jewelery shop and the final assembly line of a large company in the automotive sector of Araraquara, it was possible to verify the positive impacts in both cases despite the proportions. Both cases demonstrate information technology as a path to sustainability, as the two companies compared had a reduction in waste and resources spent in the process, even though they are very different companies, both in size and in the field of activity.

**Key Words:** Industry; Sustainability; Technology.

## 1. Introdução

Hoje as indústrias buscam manter a produtividade e a competitividade, mesmo frente ao desafio da sustentabilidade, para que esse objetivo possa ser alcançado é necessário produzir mais com menos, um jeito de tornar esse objetivo em realidade é com o uso da tecnologia de informação dentro das indústrias.

No contexto atual onde os recursos naturais necessários para o crescimento econômico se mostram escassos, a adoção da tecnologia de informação é um dos meios de tornar as indústrias mais sustentáveis.

Este trabalho busca mostrar os impactos positivos da adoção da tecnologia de informação na produção industrial, comparando a implantação de um sistema de controle na linha de montagem final uma de uma grande empresa do setor automobilístico de Araraquara e a implantação de um CAD em uma pequena ourivesaria, analisando os recursos otimizados em ambos os casos e o avanço de suas atividades em busca da sustentabilidade. Também buscamos analisar se a crescente utilização de tecnologia da informação leva a uma maior sustentabilidade e competitividade.

## 2. Indústria 4.0

A quarta revolução industrial ou indústria 4.0 é caracterizada pelo uso de tecnologias digitais no processo produtivo, nesse conceito existem alguns pilares como a internet das coisas, a computação em nuvem, big data, sistemas ciberfísicos, realidade virtual e aumentada e impressão 3D.

As grandes potências mundiais adotam a indústria 4.0 como o futuro, a busca por processos mais eficientes passa pela indústria 4.0, que não está restrita a grandes plantas industriais, mas já começa a fazer parte do cotidiano. (LIMA; PINTO, 2019).

A energia elétrica é um recurso essencial para o funcionamento da indústria como um todo e conforme os trabalhos citados a seguir é possível ter uma ideia do tamanho desta relevância.

No ano de 2014 as indústrias brasileiras gastaram 62042868,83 MWh o equivalente a 18% do total nacional deste ano, desembolsando uma soma de 20808073215,94 reais. (GODINHO; et al, 2017).

De acordo com um relatório da CNI de 2016 até 2025 a indústria 4.0 pode economizar até 20% de energia elétrica. (LIMA; PINTO, 2019).

Apesar do avanço inegável da tecnologia da informação nas mais diversas áreas, bem como a sua popularização, o consumo de papel não caiu, pelo contrário cresceu muito nos últimos anos.

Trinta anos atrás a revolução da informática poderia causar a impressão de que o papel ia quase deixar de ser usado, mas o que se observou é justamente o contrário, o consumo de papel cresceu 6 vezes nos últimos 30 anos. (BRAGA, 2010).

O processo de plantio da madeira e produção do papel tem se tornado mais sustentável com o plantio da madeira, mas ainda tem os impactos inerentes de qualquer monocultura.

100% do papel consumido no Brasil é fruto de reflorestamento feito no modelo de monocultura. Com certeza é melhor a monocultura de eucalipto do que derrubar floresta nativa para fazer papel, mas o processo de plantio e a própria indústria do papel gera impactos ambientais como o secamento e os insumos gastos na produção do papel. (BRAGA, 2010).

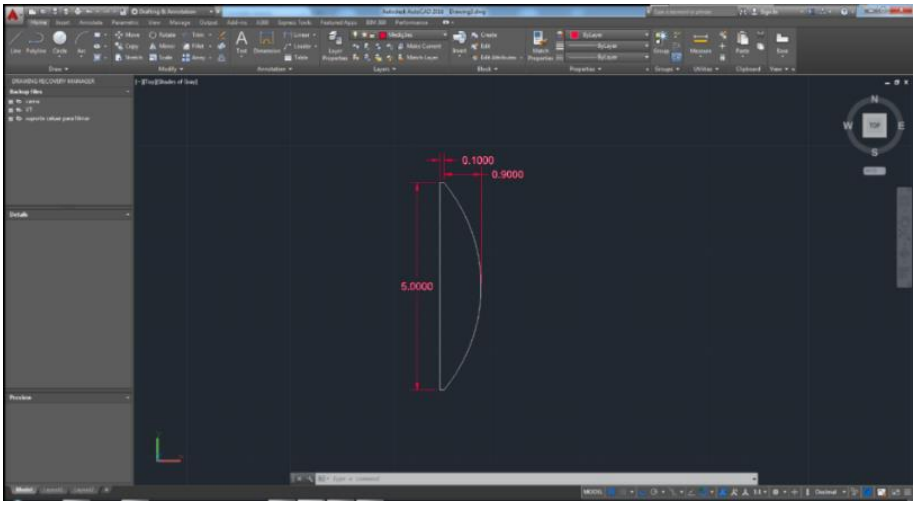
O papel pode até ser biodegradável, mas ainda usa recursos escassos no seu processo de produção, bem como tem um impacto inevitável no objetivo da sustentabilidade.

O uso da tecnologia de informação nos processos industriais é um dos caminhos para realizar mias com menos, otimizar os processos e reduzir o consumo de recursos escassos, no caso deste trabalho do papel e da energia elétrica. Como um exemplo prático podemos citar uma ourivesaria.

Uma pequena empresa, instalada em uma sala, na cidade de Juiz de Fora/MG com um torno mecânico comprado recentemente. O uso do torno mudou o processo produtivo a ponto de mudar o modelo de venda, pois antes do torno o cliente recebia o orçamento da peça antes mesmo de começar o processo de manufatura, com o uso do torno isso se tornou impossível, uma vez que o torno retira material alterando o peso da peça no processo.

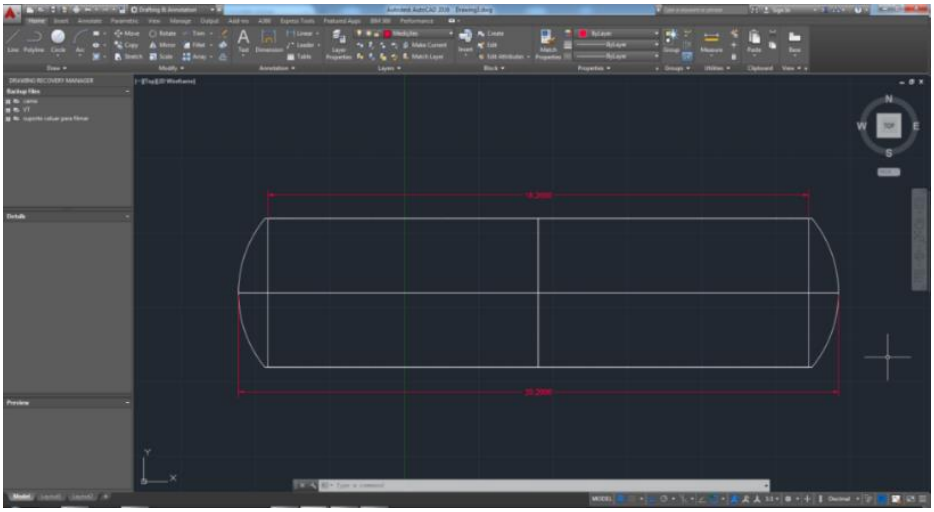
A implantação de software CAD, no caso o autoCAD resolveu este problema, pois ao desenhar a peça no software é possível calcular o peso da peça antes do início da manufatura, com isso o antigo modelo de venda pode retornar. (FIGURA 1) e (FIGURA 2). (ASSIS; et al, 2017).

**Figura 1 - PERFIL INTERNO DE UMA ALIANÇA DESENHADA NO CAD**




FONTE: ASSIS Diana Martins Stefanon et al 2017 página 329

**Figura 2 - VISTA LATERAL DE UMA ALIANÇA DESENHADA NO CAD**



FONTE: ASSIS Diana Martins Stefanon et al 2017 página 329

A ourivesaria em questão produz em pequena escala um produto customizado e com muito valor agregado, com processos de transformação e uso de mão de obra especializada e com a adoção de um processo automatizado pode tornar a empresa mais eficiente e mais competitiva.

## 3. Coleta de dados

Além da revisão bibliográfica, foi feito para este trabalho um estudo de caso sobre a implantação de um sistema de controle informatizado na linha de montagem final em uma planta de uma grande empresa do setor automobilístico de Araraquara, por meio de entrevistas realizadas com funcionários do setor.

## 4. Resultados e discussão

Na planta industrial são fabricados semirreboques basculantes, sendo que cada semirreboque pode ter algumas diferenças, de acordo com as especificações do cliente.

Para a implantação do sistema foram instalados alguns computadores ao longo da linha e distribuídos alguns tablets para os funcionários do setor, assim como o treinamento necessário para registrar a execução de cada etapa do processo produtivo.

De acordo com as entrevistas realizadas com os funcionários do setor houve um ganho expressivo na praticidade do manuseio das informações relativas ao produto, com informações mais claras e ágeis chegando aos usuários, reduzindo dessa maneira os erros no processo de fabricação e os desperdícios. Também foram constatados redução no tempo de apontamento e registros do produto.

O papel antes usado para a impressão das notas de serviço como um padrão agora serve apenas como uma contingência, dessa forma os custos com papel, tinta e relacionados foi drasticamente reduzido.

Como resultado observado da implantação do sistema de controle da linha de montagem final, observou-se uma redução de até 10% do tempo total do processo de montagem final dos semirreboques basculantes, logo também houve uma redução no consumo de energia elétrica, uma vez que o mesmo processo é realizado mais rápido e com menos desperdícios e com uma menor chance de retrabalho. Podemos dizer também que a mesma parte desta planta industrial, consumindo a mesma quantidade de energia elétrica, produz 10% a mais.

Devido ao resultado positivo deste sistema, a implantação em toda a linha de produção está em estudo.

## 5. Considerações finais

Este trabalho teve como objetivo analisar o impacto positivo da implantação da tecnologia de informação na indústria, de maneira a tornar a atividade industrial mais sustentável através da otimização dos recursos empregados, fazendo mais com menos, para isso foi feita uma revisão bibliográfica para o embasamento teórico e a observação dos resultados da implantação de um sistema de controle na linha de montagem final uma grande empresa do setor automobilístico de Araraquara, onde foi observado uma redução drástica do uso de papel e uma redução no consumo de energia elétrica.

O caso analisado nos mostra resultados positivos, resguardados as proporções em questão, similares ao caso da pequena ourivesaria, com redução de desperdício, tempo e menor chance de erros, também foi possível observar uma facilidade muito maior ao manusear as informações referentes ao produto final.

Dadas as similaridades observadas entre os resultados da uma grande empresa do setor automobilístico de Araraquara e a pequena ourivesaria, mesmo em atividades tão distintas, envolvendo empresas de portes tão distintos, podemos concluir que a adoção da tecnologia da informação em processos industriais e de transformação, pode otimizar recursos escassos, fazendo mais com menos e tornando as indústrias mais sustentáveis e competitivas.

Para uma melhor compreensão do impacto total da otimização dos recursos da planta industrial analisada, seria necessária uma coleta de dados mais abrangente, colhendo dados ao longo do tempo, de antes e depois da implantação do sistema e mais específicos para cada processo e equipamento envolvido, possibilitando levantar qual máquina gasta mais energia elétrica e avaliar o quanto cada máquina ficou mais produtiva. Seria possível também realizar um levantamento da quantidade de papel utilizada em cada etapa, a fim de quantificar o quanto de papel deixou de ser gasto de fato.

## Referências

ASSIS, Diana Martins Stefanon. BARROSO, Ana Flávia da Fonseca. FERREIRA, André Luiz Francisco. **Tecnologia da informação no processo de fabricação de alianças**: um estudo de caso. In: SIMPROD, IX, 2017, Sergipe, Departamento de Engenharia de Produção - Universidade Federal de Sergipe, dez 2017, páginas 323 a 332, disponivel em: <https://ri.ufs.br/handle/riufs/7685>, acesso em 28 de maio de 2023.

BRAGA, Helena Marcia Nogueira Cavalcanti. **As alternativas para a redução do consumo de papel nas empresas**, 2010, 62. pós graduação “lato sensu” em gestão ambiental Universidade Candido Mandes, Rio de Janeiro, disponível em <http://www.avm.edu.br/docpdf/monografias_publicadas/k215732.pdf>, Acesso em 28 de maio de 2023.

GODINHO, Silvio Martins. ROCCA, Graciela Alessandra Dela. RAMOS, James Oto. STEFENON, Frizzo Stéfano. AMÈRICO, Jonatas Policarpo. **Espacios,** V38, nº 36, 2017, pagina 0. Disponível em <http://ww.revistaespacios.com/a17v38n36/a17v38n36p01.pdf.>. acesso em 28 de maio de 2023.

LIMA, Alison Gustavo de. PINTO, Giuliano Scombatti. indústria 4.0 um novo paradigma para a indústria. **Interface Tecnológica**, Taquaritinga, V16, nº 2, páginas 299 a 311, 2019. disponível em DOI <https://doi.org/10.31510/infa.v16i2.642>. Acesso em 28 de maio de 2023.

SOUZA, Clayton José Cavalcante de. **Aplicações da Tecnologia da Informação e Comunicação na Automação Industrial,** 2008, 64 páginas, trabalho de conclusão de curso, bacharelado em sistemas de informação. Universidade Federal do Pará, Marabá. Disponível em <http://repositorio.unifesspa.edu.br/handle/123456789/222.>, acesso em 28 de maio de 2023.

RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

# O papel das Tecnologias da Informação na Construção de Cidades Inteligentes e Sustentáveis

**Vinícius Teixeira Juste**
Faculdade de Tecnologia de Americana, viniciusjuste2019@gmail.com
**Wandderley Luiz de Freitas Apaza**
Faculdade de Tecnologia de Americana, wandderley.apaza@fatec.sp.gov.br
**João Emmanuel D Alkmin Neves**
Faculdade de Tecnologia de Americana, joao.neves11@fatec.sp.gov.br

**RESUMO**

Este trabalho científico analisa o papel da tecnologia da informação na construção de cidades inteligentes e sustentáveis, em consonância com o Objetivo de Desenvolvimento Sustentável 9 - Indústria, Inovação e Infraestrutura. O uso de tecnologias como sensores, IoT, GIS e IA é crucial para reduzir o consumo de energia e minimizar os impactos ambientais das cidades. O trabalho discute as principais tecnologias de TI e seu papel na criação de cidades mais sustentáveis, além dos desafios e oportunidades de implementá-las em diferentes contextos urbanos. Questões como o alto custo de implementação em larga escala, a desigualdade no acesso à tecnologia e a dependência excessiva da TI também são abordadas. O objetivo é analisar as tecnologias utilizadas e identificar os principais desafios para sua implementação, bem como recomendar estratégias para minimizar problemas e maximizar benefícios. A literatura demonstra que a TI é crucial para a construção de cidades inteligentes e sustentáveis, permitindo a coleta e análise de dados em tempo real, otimização de processos e desenvolvimento de soluções mais eficientes e econômicas. A aplicação da TI pode melhorar a participação dos cidadãos na gestão urbana, permitindo acesso a informações relevantes e colaboração. A TI deve ser integrada para garantir sua aplicação adequada na construção de cidades inteligentes e sustentáveis. A justificativa para este trabalho científico é a necessidade global de construir cidades mais eficientes e menos poluentes, embora questões relacionadas a custos, privacidade, desigualdade e dependência tecnológica precisem ser abordadas adequadamente. O uso da TI é uma maneira eficaz de alcançar este objetivo.

**Palavras-Chave:** Cidades inteligentes; Desenvolvimento Sustentável; Sustentabilidade; Tecnologia da informação; Tecnologias de TI.

Artigo Submetido: 21/06/2023

Artigo Aceito Publicação: 15/05/2024

# *The Role of Information Technologies in Building Smart and Sustainable Cities*

**ABSTRACT**

This scientific work analyzes the role of information technology in building smart and sustainable cities in line with Sustainable Development Goal 9 - Industry, Innovation, and Infrastructure. The use of technologies such as sensors, IoT, GIS, and AI is crucial to reduce energy consumption and minimize the environmental impacts of cities. The work discusses the main IT technologies and their role in creating more sustainable cities, as well as the challenges and opportunities of implementing them in different urban contexts. Issues such as the high cost of large-scale implementation, inequality in access to technology, and excessive dependence on IT are also addressed. The objective is to analyze the technologies used and identify the main challenges for their implementation, as well as recommend strategies to minimize problems and maximize benefits. Literature shows that IT is crucial to building smart and sustainable cities, allowing for real-time data collection and analysis, process optimization, and development of more efficient and cost-effective solutions. The application of IT can improve citizen participation in urban management, allowing access to relevant information and collaboration. IT must be integrated to ensure its proper application in building smart and sustainable cities. The justification for this scientific work is the global need to build more efficient and less polluting cities, although issues related to costs, privacy, inequality, and technological dependence need to be addressed properly. The use of IT is an effective way to achieve this objective.

**Key Words:** Smart cities; Sustainable Development; Sustainability; Information technology; IT technologies.

## 1. Introdução

As cidades são responsáveis por grande parte do consumo de energia e dos impactos ambientais. Com o aumento da população e da urbanização, é necessário encontrar soluções sustentáveis para tornar as cidades menos poluentes e mais eficientes. Uma das soluções é o uso de tecnologias da informação para a construção de cidades sustentáveis e mais inteligentes. Neste trabalho científico, pode-se abordar as principais tecnologias de TI utilizadas para a construção de cidades inteligentes, tais como sensores, dispositivos IoT (Internet das Coisas), sistemas de informação geográfica (GIS) e inteligência artificial (IA), e discutir como essas tecnologias podem ajudar a tornar as cidades mais sustentáveis, através da redução do consumo de energia, da melhoria da mobilidade urbana, da gestão de resíduos e da conservação de recursos naturais. Além disso, pode-se explorar os desafios e oportunidades para a implementação dessas tecnologias em diferentes contextos urbanos, considerando fatores sociais, econômicos e políticos.

Nesse contexto, a inclusão da ODS número nove - Indústria, Inovação e Infraestrutura - é relevante. A ODS 9 tem como objetivo "construir infraestruturas resilientes, promover a industrialização inclusiva e sustentável e fomentar a inovação". A implementação de tecnologias de informação e comunicação (TIC) para a construção de cidades inteligentes se enquadra nessa meta.

Ao utilizar tecnologias como sensores, dispositivos IoT, sistemas de informação geográfica e inteligência artificial, as cidades podem melhorar sua infraestrutura e promover a inovação em diversos setores. Isso inclui a criação de sistemas de transporte inteligentes, redes de energia eficientes, sistemas de gestão de resíduos mais inteligentes e soluções de governança urbana baseadas em dados.

O problema que pode ser encontrado na construção dessas cidades inteligentes é o custo para implantação de tecnologias em larga escala, principalmente em países pouco desenvolvidos ou em áreas periféricas.

A hipótese central é que o uso de tecnologias de TI pode contribuir de forma significativa para a criação de cidades sustentáveis, para isso é necessário que sejam abordados de forma adequada os desafios mencionados.

O objetivo deste trabalho é analisar as principais tecnologias utilizadas e identificar os principais desafios para a implantação destas tecnologias na construção de cidades, avaliaremos as melhores estratégias visando minimizar os problemas e maximizar os benefícios assim podendo propor recomendações para a implantação correta destas tecnologias

A justificativa para a realização deste trabalho científico é que, apesar dos desafios envolvidos, a construção de cidades inteligentes e sustentáveis é uma necessidade em todo o mundo.

A construção delas é uma maneira eficaz de tornar as cidades mais eficientes e menos poluentes, mas é necessário abordar adequadamente as questões relacionadas aos custos, privacidade, desigualdade e dependência tecnológica.

## 2. Referencial teórico

Segundo os pesquisadores as cidades inteligentes são o futuro, elas diminuirão o aquecimento global, trarão qualidade de vida e mais conforto para a sociedade. A tecnologia da informação será crucial para este processo de modernização, no Brasil o desafio será maior do que seria em países mais desenvolvidos, por conta da corrupção, falta de estrutura e cultura do nosso povo.

De acordo com Almeida, E. C., & Santoro, F. M. (2017) As tecnologias da informação são fundamentais na construção de cidades inteligentes e sustentáveis, permitindo a coleta e análise de dados em tempo real, a otimização de processos e o desenvolvimento de soluções mais eficientes e econômicas para a gestão urbana.

Segundo H., Kalasek, R., Pichler-Milanović, N., & Meijers, E. (2007). A aplicação das tecnologias da informação é um componente chave na construção de cidades inteligentes e sustentáveis, permitindo o monitoramento e controle de diversos aspectos da cidade, como transporte, energia, segurança e meio ambiente. Giffinger, R., Fertner, C., Kramar,

De acordo com Nam, T., & Pardo, T. A. (2011 As tecnologias da informação podem ser usadas para melhorar a participação dos cidadãos na gestão urbana, permitindo o acesso a informações relevantes e a possibilidade de feedback e colaboração.

Segundo Chen, Y., Zhang, Y., & Lu, Y. (2019). Smart city research: A review of the literature. A aplicação das tecnologias da informação na construção de cidades inteligentes e sustentáveis deve ser feita de forma integrada, considerando as diferentes áreas da gestão urbana e os objetivos de desenvolvimento sustentável.

De acordo com Batty, M. (2013), um dos principais desafios enfrentados pelas cidades atualmente é a rápida urbanização, que traz consigo problemas como congestionamentos, poluição e demanda crescente por energia. O autor destaca que as tecnologias da informação desempenham um papel crucial na busca por soluções para esses desafios, permitindo a coleta de dados em tempo real, a análise de informações e a tomada de decisões baseada em evidências. Ele argumenta que o uso inteligente das tecnologias da informação pode levar a uma melhor gestão urbana, tornando as cidades mais eficientes, sustentáveis e habitáveis.

Seguindo essa linha, Caragliu, A., Del Bo, C., & Nijkamp, P. (2009) afirmam que as tecnologias da informação e comunicação (TIC) são fundamentais para o desenvolvimento de cidades inteligentes, permitindo a integração de sistemas e a coleta de informações sobre diversos aspectos urbanos, como transporte, energia, segurança, meio ambiente e governança. Eles destacam que a utilização eficaz das TIC pode melhorar a qualidade de vida dos cidadãos, promover a sustentabilidade e impulsionar o desenvolvimento econômico.

No que diz respeito à mobilidade urbana, Bieker, T., & Edler, D. (2017) apontam que as tecnologias da informação têm um papel central na criação de soluções inovadoras, como sistemas de transporte inteligentes e compartilhados, que podem reduzir congestionamentos e emissões de carbono, além de melhorar a acessibilidade e a eficiência dos deslocamentos na cidade.

Em relação à gestão de energia, Abanda, F. H., et al. (2019) destacam que as tecnologias da informação desempenham um papel importante na transição para redes de energia inteligentes (smart grids). Essas redes permitem o monitoramento em tempo real do consumo de energia, o gerenciamento eficiente da distribuição e a integração de fontes

de energia renovável, contribuindo para a redução do consumo de energia e das emissões de carbono nas cidades.

No campo da governança urbana, Acs, G., et al. (2018) argumentam que as tecnologias da informação podem promover a participação dos cidadãos na tomada de decisões e na gestão da cidade. Por meio de plataformas digitais e aplicativos, os cidadãos podem ter acesso a informações relevantes sobre a cidade, expressar suas opiniões e contribuir para a solução de problemas locais. Essa abordagem participativa fortalece a democracia local e permite uma governança mais transparente e responsiva.

Outra área em que as tecnologias da informação têm sido amplamente aplicadas é a gestão de resíduos. De acordo com Zorpas, A. A., et al. (2018), as tecnologias como sensores e dispositivos IoT podem ser usadas para monitorar o nível de enchimento dos contentores de resíduos.

## 3. Exemplos de cidades inteligentes

Segundo o site “O consumidor moderno”, São Paulo se destaca na área de Mobilidade e Acessibilidade, especialmente devido à diversidade de modos de transporte disponíveis. A cidade foi uma das pioneiras no Brasil a implementar o bilhete eletrônico em seu sistema de transporte público, permitindo o pagamento até mesmo por meio do PIX. Além disso, São Paulo também é uma das primeiras cidades a contar com semáforos inteligentes, que contribuem para um trânsito melhor.

A capital paulista possui atualmente mais de 600 km de ciclovias, oferecendo uma opção de transporte inteligente que ocupa menos espaço, reduz a emissão de poluentes e incentiva a prática de exercícios físicos, promovendo a saúde dos seus usuários. Com uma média de 5,53 km de ciclovia por habitante, São Paulo tem se destacado nessa área. A frota de veículos de baixa emissão também apresentou um crescimento, passando de 0,10% para 0,21% do total.

No âmbito da mobilidade, os moradores da cidade de São Paulo têm acesso, em um raio de 100 km, a três dos maiores e mais movimentados aeroportos do país (Congonhas, Guarulhos e Viracopos). Além disso, há uma ampla oferta de transporte rodoviário interestadual, conectando a população a mais de 940 destinos brasileiros.

A cidade de São Paulo também possui um ambiente propício para o setor tecnológico. Com um polo tecnológico declarado pela prefeitura, a cidade abriga 4,5% dos empregos formais no setor de tecnologia, além de 4,4% no setor de educação, pesquisa e desenvolvimento. São Paulo também conta com quatro incubadoras de empresas e registrou um aumento de 0,2% no número de empresas do setor de tecnologia.

Outros aspectos que merecem destaque em São Paulo incluem: acesso universal à água para a população urbana, com 97% tendo acesso ao sistema de esgoto e 99,1% sendo atendidos com coleta de resíduos sólidos. A cidade também possui um cadastro imobiliário informatizado e georreferenciado, disponibilizado aos cidadãos. Quanto à conectividade, São Paulo registrou uma velocidade média de 210,6 mbps nas conexões de banda larga, um aumento significativo em relação à pesquisa anterior que apontava 93,7 mbps. Além disso, 99,8% da população é coberta pelo sinal de 4G. A população também se beneficia com o agendamento online de consultas na rede pública de saúde e a presença do Centro de Controle e Operações, responsável pela segurança pública. A

independência de empregos no setor público chega a 85% e houve um crescimento de 6,7% no número de empregos em 2022.

**Figura 1 - Cidade de São Paulo**

Fonte: Consumidor Moderno

Segundo o blog "Maplink Blog", Copenhague, a capital da Dinamarca, é amplamente reconhecida como uma das cidades mais sustentáveis do mundo. O compromisso da cidade com a bicicleta como meio de transporte e sua meta ambiciosa de se tornar neutra em carbono até 2025 são evidências desse empenho. É considerada uma das principais cidades inteligentes da Europa, ocupando a 6ª posição no ranking Cities in Motion, divulgado pela IESE Business School, que avalia as cidades com maior inteligência em todo o mundo.

Um excelente exemplo que destaca o caráter inteligente de Copenhague é o projeto EnergyLab Nordhavn, que demonstrou a viabilidade de integrar transporte elétrico, edifícios energeticamente eficientes, eletricidade e aquecimento em uma iniciativa capaz de reduzir consideravelmente as emissões de carbono.

Essas medidas não apenas melhoram a qualidade de vida dos habitantes, mas também desempenham um papel ativo na redução da poluição, servindo como um exemplo inspirador para outros países ao redor do mundo.

Outro aspecto notável é o fato de que mais da metade da população de Copenhague opta por utilizar bicicletas como principal meio de transporte para o trabalho, escola e lazer. No entanto, é importante ressaltar que essa prática só é viável graças à existência de uma infraestrutura cicloviária abrangente e eficiente.

Isso demonstra que a construção de uma cidade inteligente não depende exclusivamente do governo ou do setor privado, mas requer ações conjuntas que envolvam também os cidadãos em sua implementação e sustentação.

**Figura 2- Copenhague – Dinamarca**


Fonte: Maplink Blog

De acordo com o site “Eco Parking”, Singapura: A cidade-estado de Singapura é conhecida por sua abordagem inovadora para o planejamento urbano, incluindo o uso extensivo de tecnologia para melhorar a eficiência dos serviços públicos e a qualidade de vida dos moradores.

Uma das nações mais ricas do mundo, a cidade-estado abriga o porto mais movimentado do mundo em termos de tonelagem de transporte. Nos últimos anos, o governo implementou uma estratégia para transformar Singapura numa ‘cidade num jardim’ com ‘super árvores’ movidas a energia solar que podem atingir até 50 metros de altura e edifícios inteligentes e sustentáveis. Fachadas verdes, Aproveitamento do vento para climatizar edifícios, assim como uma visão progressiva de transporte urbano também contam para Singapura.

**Figura 3 - Jardins de Singapura**

Fonte: Eco telhado

Segundo o site “Pensamento verde”, Songdo, uma cidade localizada na Coreia do Sul, foi concebida desde o início como uma cidade inteligente, com uma infraestrutura interconectada e tecnologia de ponta nas áreas de transporte, energia e comunicações.

Um dos aspectos distintivos das cidades inteligentes é a incorporação de tecnologia no desenvolvimento de projetos, e isso também se aplica a Songdo. A cidade implementou diversas inovações tecnológicas que já estão em pleno funcionamento.

Um exemplo notável é o centro de operações e transporte, que foi inspirado na NASA. A cidade também possui estações de recarga para carros elétricos e um sistema que monitora o consumo de eletricidade em tempo real.

No que diz respeito aos resíduos produzidos nas residências, Songdo possui um sistema de reciclagem avançado, no qual mecanismos de aspiração direcionam os resíduos para uma rede subterrânea de túneis que os leva até o centro de processamento. Além disso, a cidade possui um sistema de aproveitamento de água, com uma extensa rede de canos que evita o uso de água potável nos vasos sanitários.

Songdo também oferece uma rede de ciclovias, uma escola internacional e câmeras que monitoram o fluxo de veículos que atravessam a ponte de acesso à cidade. Vale ressaltar que Songdo é uma ilha, com um projeto que se inspira na cidade de Nova Iorque e nos canais de Veneza.

Essas iniciativas mostram o compromisso de Songdo em se tornar uma cidade inteligente, proporcionando uma qualidade de vida aprimorada para seus habitantes por meio de soluções tecnológicas inovadoras.

**Figura 4 - Parque central de Songdo - Coreia do Sul**

Fonte: Spiegel ausland

## 4. Material e métodos

Para realizar esse trabalho, foram utilizados artigos científicos, livros e relatórios sobre tecnologias da informação e cidades inteligentes e sustentáveis, além de dados de pesquisas e estudos relacionados a esse tema.

Primeiramente, foi realizada uma revisão bibliográfica para entender as principais tecnologias da informação utilizadas em cidades inteligentes e sustentáveis, bem como os benefícios e desafios do uso dessas tecnologias. Em seguida, foram analisados dados de pesquisas e estudos para identificar as principais tendências e desafios relacionados ao uso dessas tecnologias.

Após a análise dos dados, foram identificados os principais desafios relacionados à implantação de tecnologias de TI em cidades inteligentes e sustentáveis e foram propostas estratégias para minimizar esses desafios. Por fim, com base em todo o material utilizado, foram elaboradas recomendações para a implantação de tecnologias de TI em cidades inteligentes e sustentáveis, com o objetivo de orientar gestores públicos, empresas e cidadãos na adoção dessas tecnologias de maneira eficaz e sustentável.

## 5. Considerações finais

Este trabalho teve como objetivo entender o papel das tecnologias da informação na construção de cidades inteligentes e sustentáveis, a partir da análise das principais tecnologias utilizadas e dos desafios para sua implantação.

Os objetivos específicos foram definidos para analisar as tecnologias de TI, identificar os principais desafios para a sua implementação na construção de cidades e propor recomendações para a implantação correta dessas tecnologias. Verificou-se que as tecnologias de TI podem contribuir significativamente para a construção de cidades

sustentáveis e inteligentes, mas é necessário abordar adequadamente questões como custos, privacidade, desigualdade e dependência tecnológica.

A hipótese do trabalho de que o uso de tecnologias de TI pode contribuir para a criação de cidades sustentáveis se confirmou, desde que esses desafios sejam adequadamente abordados.

Portanto, a resposta ao problema de pesquisa é que as tecnologias de TI podem ser utilizadas para a construção de cidades sustentáveis e inteligentes, desde que sejam considerados os desafios mencionados.

Os instrumentos de coleta de dados utilizados permitiram uma avaliação adequada dos temas abordados.

Para futuras pesquisas, é importante continuar explorando as tecnologias de TI utilizadas na construção de cidades sustentáveis e inteligentes, considerando fatores sociais, econômicos e políticos. Além disso, pode-se estudar o impacto dessas tecnologias na qualidade de vida dos cidadãos e na efetividade das políticas públicas.

## 6. Projetos futuros

Em pesquisas futuras, pode-se explorar a relação entre as tecnologias de TI e o Objetivo de Desenvolvimento Sustentável 9: Indústria, Inovação e Infraestrutura, que busca promover o desenvolvimento de infraestrutura resiliente, a industrialização inclusiva e sustentável, além da promoção da inovação e tecnologias limpas. A pesquisa pode enfatizar a importância dessas tecnologias para a realização desse objetivo, bem como discutir as estratégias necessárias para superar os desafios enfrentados na implementação dessas tecnologias em diferentes contextos urbanos.

## Referências

ABANDA, F. H. et al. Smart Grid Technologies for Sustainable Urban Development: Insights from Smart City Initiatives. Sustainable Cities and Society, v. 49, p. 101605, 2019.

ACS, G. et al. Urban Governance in the Era of Smart Cities: Institutionalization and Policy Learning in the Urban Living Lab. Journal of Urban Technology, v. 25, n. 3, p. 59-78, 2018.

ALMEIDA, E. C.; SANTORO, F. M. Smart Cities: Fundamentos, Tecnologias e Aplicações. São Paulo: Novatec Editora, 2017.

BATTY, M. The New Science of Cities. MIT Press, 2013.

BIEKER, T.; EDLER, D. Smart Mobility: Opportunities and Challenges of the Digitalization of Transportation. Technological Forecasting and Social Change, v. 104, p. 168-178, 2017.

CARAGLIU, A.; DEL BO, C.; NIJKAMP, P. Smart Cities in Europe. Journal of Urban Technology, v. 16, n. 2, p. 65-82, 2009.

CHEN, Y.; ZHANG, Y.; LU, Y. Smart city research: A review of the literature. Journal of Cleaner Production, v. 228, p. 946-965, 2019.

GIFFINGER, R. et al. Smart cities: Ranking of European medium-sized cities. Vienna University of Technology, Centre of Regional Science, 2007.

NAM, T.; PARDO, T. A. Conceptualizing smart city with dimensions of technology, people, and institutions. In: Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, p. 282-291, 2011.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Objetivos de Desenvolvimento Sustentável. Disponível em: https://nacoesunidas.org/pos2015/. Acesso em: 03 maio 2023.

SILVA, V. F. S. Tecnologias de informação e comunicação na construção de cidades inteligentes e sustentáveis: uma revisão sistemática. Revista Brasileira de Gestão Urbana, v. 11, n. 2, p. 266-282, 2019.

UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS. Sustainable Development Goals. Disponível em: https://sdgs.un.org/goals. Acesso em: 03 maio 2023.

ZORPAS, A. A. et al. Smart Technologies for Solid Waste Collection Monitoring: A Review. Waste Management, v. 77, p. 447-460, 2018.

RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

# As míticas histórias: contos e histórias

**Marcos Ferreira Guedes da Costa**
FATEC Itatiba, marcos.costa43@fatec.sp.gov.br

**RESUMO**

Este artigo traz em seu bojo experiências vividas por alunos do curso de Gestão da Produção Industrial da FATEC de Itatiba, por ocasião do aprendizado na disciplina de *Ética e Direito Empresarial*, na qual estudamos um pouco da normalidade ética, cujos comportamentos evoluem na medida em que construímos uma civilização que paute, cada vez mais, pelo respeito, ao diverso, nos variados *locus* nos quais os relacionamentos humanos se expressam. Antes de adentrarmos propriamente no ensino da ética, ramo da filosofia destinado ao ensino da moral, fez-se necessário explicar os fatos que antecederam o nascimento da *filosofia.* Assim, ao tomarem conhecimento dos fenômenos míticos, especialmente aqueles nascidos na Antiguidade Clássica, despertaram interesse em conhecer alguns *mitos universais*, reconhecendo sua presença no imaginário até os dias de hoje. Ao propor atividades que os fizessem reviver suas experiências com criaturas *mitológicas*, os discentes produziram inusitados contos que os fizeram reviver as experiências vividas com seres extraordinários que povoaram suas mentes em algum tempo de suas vidas. E aqui estão reunidas nove histórias contadas com pormenores por cada um deles. Aos que se debruçarem sobre os pequenos textos, uma relaxante e agradável leitura.

**Palavras-Chave:** Crenças; Folclore; Mito; Vivências.

Data de Submissão: 09/10/2023

Data Aceito Publicação: 15/05/2024

# *The Mythical Stories: Tales and Narratives*

**ABSTRACT**

This article encompasses the experiences lived by students from the Industrial Production Management course at FATEC in Itatiba during the learning process of the Ethics and Business Law subject. In this course, we studied ethical normality, where behaviors evolve as we build a civilization increasingly based on respect for diversity in the various loci where human relationships take place. Before delving into the teaching of ethics, a branch of philosophy dedicated to teaching morality, it was necessary to explain the events that preceded the birth of philosophy. Thus, upon learning about mythical phenomena, especially those from Classical Antiquity, the students became interested in exploring some universal myths, recognizing their presence in the collective imagination to this day. By proposing activities that allowed them to relive their experiences with mythological creatures, the students produced unusual tales that made them relive their encounters with extraordinary beings that once populated their minds. Here, nine stories are gathered, each told in detail by the students. To those who immerse themselves in these short texts, we wish you a relaxing and pleasant read.

**Key Words:** Beliefs; Folklore; Myth; Experiences.

***A tarefa proposta***

Ao ser designado pela coordenação do curso de *Tecnologia da Produção Industrial* para estar à frente da disciplina *Ética e Direito Empresarial*, inserida na grade do 4º semestre do curso de duração total de sete períodos, conheci um grupo de nove alunos cursantes os quais, por meio de breves conversas, fui conhecendo e interagindo com suas realidades. Fiquei agradavelmente surpreso em saber que a grande maioria, exceção feita a uma aluna, com seus poucos dezoito anos de idade, encontra-se formalmente inserida no mercado de trabalho, desenvolvendo diversas atividades nas indústrias do Município de Itatiba, envolvendo a produção de fármacos, componentes eletrônicos, ferramentaria e outros serviços de metalurgia, sendo um único deles pertencente ao setor de serviços de educação, desenvolvendo a atividade de auxiliar administrativo em nossa unidade.

Disse-lhes sobre a importância da participação de todos na composição dos 34,6% da produção do *Produto Interno Bruto* nacional, enfatizando a necessidade de conciliarmos nossas atividades laborais com as acadêmicas objetivando, com nossos esforços, ampliar nossa empregabilidade, buscando trabalhos com maiores exigências e conhecimentos, cujas certificações, a exemplo da conclusão de um curso superior de tecnólogo, são a porta de entrada para conquistarmos responsabilidades mais complexas e, em consequência, melhores remunerações.

A proposta da disciplina foi, inicialmente, a de ensinar-lhes as virtudes cardeais da prudência, da temperança, justiça e fortaleza, fundamentais para a compreensão dos comportamentos adotados nos mais diversos *locus:* nos relacionamentos domésticos, na sociedade civil, e nos ambientes corporativos. Com efeito, para adentrarmos ao precioso estudo da ética, ramo da filosofia que investiga as relações comportamentais de nós, humanos, no mundo civilizado, foi preciso explicar-lhes como nasceu a filosofia. Para isso, socorri-me de alguns textos de fácil compreensão, extraídos da plataforma *aprenda mais*, do Ministério da Educação do Governo Federal, cujo modelo do *site* de aprendizado, muito parecido com a plataforma *Mooc- EAD* do Centro Paula Souza, foi de fácil manuseio.

Contando a plataforma com mais de uma centena de cursos nas diversas áreas do conhecimento, com direito a certificações a serem inseridas em seus currículos acadêmicos, inscrevemo-nos *on-line* para termos acesso aos textos e demais referências bibliográficas, a fim de servirem como fontes de leitura, pesquisa e aprimoramento das reflexões feitas em sala de aula.

Eis que nos deparamos com o estudo do Mito.

Ao estudarmos a origem da *mitologia*, ilustrando nossas aulas com narrações dos contos mitológicos da civilização *Greco-Romana*, a exemplo do mito da sereia, interessaram-se pelo assunto, acrescentando ao aprendizado de todos, inclusive o docente, contando muito do que conheciam: as fantásticas histórias das criaturas imaginárias por eles conhecidas. Ao final do bimestre, solicitei que elaborassem livres redações a respeito do tema, inserindo as realidades e experiências pessoais vividas com as figuras míticas e o modo como foram-lhe transmitidas. Surgiu assim, o caminho para a realização da tarefa.

Segue aqui, o enunciado e a questão proposta, cujos produtos foram os curiosos contos, escritos a partir da imaginação e da experiência de cada um.

Meus agradecimentos ao corpo discente pelo entusiasmo com o qual realizaram a avaliação. Não estranhem eventuais correções feitas na estética da apresentação, posto que a essência de cada conto foi respeitada e preservada por mim, professor orientador.

***A avaliação***

***Marchinha da Sereia***

*Sabe o que é que faz,*
*Sereia em alto-mar?*
*Depois que se penteia,*
*Põe-se a cantar*
*Passa um marinheiro,*
*Ouve o canto e vai atrás*
*Sabe o que é que faz,*
*Sereia em alto mar?*
*Devora o marinheiro,*
*E põe-se a cantar*
*Outro marinheiro,*
*Ouve o canto e vai atrás*
*Um por um vai devorando,*
*E os marujos pedem mais*
*E a sereia linda,*
*Fica ainda mais voraz!*

**O mito, modo de interação das comunidades antigas com o desconhecido universo sobrenatural, compõe-se de contos que relatam com imensa criatividade e riqueza de detalhes, acontecimentos misteriosos inexplicáveis à luz da razão humana. O mito da sereia na Grécia antiga, representava os perigos existentes no grande Mar Mediterrâneo. Singrado pelos argonautas, ousados e corajosos navegadores oriundos de uma sociedade que necessitava explorá-lo para sobreviver e interagir com outros povos situados ao longo de todas as margens litorâneas, muitos destes jovens marinheiros, por ele tragados, deixavam marcas nos corações maternos e nos corações das noivas cujos sonhos das núpcias seriam afogados em um mar de lágrimas. As lendárias *sirenas*, representações míticas femininas, com seus enfeitiçadores cantos, seduziam os infortunados marujos, os quais não resistiam se lançarem ao mar para serem devorados por estes monstros marinhos. Estes personagens mitológicos, criados pelo imaginário coletivo no mundo helênico, continuam a despertar a fantasia do homem hodierno, chegando alguns a afirmar com certeza a existência destas criaturas marinhas a vagarem pelos oceanos, chegando, inclusive a serem observadas e, acreditemos!, filmadas e fotografadas!**

**Com base na poesia de Helio Ziskind e no texto que discorre sobre o *mito da sereia*, elabore uma pequena redação contando alguma experiência pessoal que teve durante sua vida com narrativas contadas por adultos que o fizeram acreditar e temer algum ser mitológico.**
***As míticas histórias***

***Um conto de infância***

Nascida e criada em Botucatu, cidade do interior do Estado de São Paulo, mais conhecida pela *terra do Saci*, minha infância na crença da existência do *Saci Pererê.* Nas histórias contadas por meus avós e bisavós, atestavam que alguns homens criavam *sacis* nas serras botucatuenses.

Conhecido por suas travessuras e por pregar peças nas pessoas, o *Saci Pererê*, menino negro, com uma única perna, portando um gorro vermelho e baforando um cachimbo, reinava por onde passava: salgava a comida das panelas que estavam sobre o fogão, apagava os lampiões dos ambientes, escondia objetos e nem os indefesos cavalos dele escapavam. Era comum os cavaleiros depararem-se com as crinas de suas montarias caprichosamente trançadas.

Estas e outras lendas de nosso folclore estiveram sempre comigo e com meus amigos de tenra idade, graças ao interesse dos mais velhos de gastarem seu tempo desfrutando de nossas companhias. Enquanto divertiam-se ao contá-las, a nós, inocentes ouvintes, restava ficarmos com nossos medos.

***Paula Thaís dos Santos Oliveira***

---

***Pernas que te quero, meu pavor, e o Lobsomem***

Durante minha infância, cresci ouvindo fascinantes histórias contadas por adultos, que me fizeram acreditar e temer os seres mitológicos. Das inúmeras histórias, a que mais me marcou foi a do *lobisomem.*

Meu tio, um excelente narrador, habituou-se a relatar para mim e meus amigos, as façanhas de um ser temido, *meio lobo meio homem*, que habitava as matas. Reportava ser uma criatura amaldiçoada, um homem dotado de muitos pelos a cobrirem todo o seu corpo. Um enorme e feroz *lobo*, cujos uivos eram ouvidos à longa distância todas as noites em que despontava no alto céu, uma gigantesca *lua cheia.*

Certa ocasião, no período de minhas férias escolares, minha família resolveu viajar para a casa do *titio*. O mesmo que me amedrontava com seus assustadores contos. Contava com pouco mais de dez anos. Era muito novo, inocente e, sobretudo, medroso.

A casa, situada em um pequeno sítio da zona rural, era ladeada por grandes pastos, iluminados pontualmente pelo voo solitário de alguns vaga-lumes. Por todos os lados aquela escuridão parecia me engolir, o que foi aumentando cada vez mais o pavor de estar ali. Pretendíamos eu, meu irmão e dois amigos, chegar o mais rápido possível à casa de um vizinho, cujo norte da caminhada nos era dado por uma pequena chama de um lampião aceso ao longe.

A *lua cheia*, subindo ao céu, tornava aquele ambiente cada vez mais sinistro. De repente, um longo e sonoro uivo: ahuuuuuuuuuuuuuuuuuuuuuuu!

Com o coração disparado e o corpo se desequilibrando de tanto tremer, minhas pernas institivamente movimentaram-se, passando a impulsionar, em movimentos frenéticos e coordenados todo o meu corpo em direção àquela luz que ia crescendo à medida em que me aproximava da varanda do vizinho.

Não sei dizer se era mesmo o *lobisomem.* Tanto eu como as companhias de infortúnio não voltaram para conferir o que era. Só sei que nos amontoamos para dormirmos em um dos dois quartos daquela pequena tapera. Retornamos logo ao amanhecer.

No resto de nossas férias, nem para o pasto íamos, mesmo durante o dia. Antes do anoitecer nos recolhíamos para o quarto, com receio de escutarmos novamente aqueles assustadores uivos.

Se existe *lobisomem?* Não sei. Como disse, nunca voltei para conferir.

***Fredson Caio Araujo Sena***

---

***Coitados dos meus avós!***

Lobisomem. Um ser antropozoomorfo,- parte homem, parte lobo,- cuja maldita transformação se manifesta todas as noites de lua cheia.

Meus avós contavam-me muitas histórias envolvendo esta terrível criatura. A crença de que era real, o que fazia temê-lo ainda mais, se fortalecia toda vez que assistia, envolto em minhas cobertas no sofá da sala, filmes de terror nos quais o lobisomem era o protagonista da tela.

Sua descrição era apavorante: com olhos vermelhos e raivosos, dentes afiados, garras e com o corpo coberto de pelos, corria rapidamente pelas matas com suas quatro estranhas patas. Conseguindo ficar de pé sobre suas pernas traseiras, visitava sítios e residências com criações, a fim de se alimentar de galinhas e outros animais. Minha avó narrava com detalhes as estranhas situações ocorridas com ela e com meu falecido avô.

Em uma delas, disse que costumava acompanhar meu avô numa carroça na qual transportavam alguns grãos e materiais para alguns lugares nas redondezas. Eram locais afastados, grandes sítios e propriedades ladeadas por florestas e caminhos de terra. Certa noite, quando a lua cheia despontava, tendo ao fundo a escuridão celeste, saíram com a carroça em direção a um atalho cujo percurso alongava-se mata adentro. Em meio a um silêncio absoluto, quebrado por pequenos grunhidos de animais noturnos e pelo zumbido dos insetos, passaram a ouvir o som do que parecia ser um animal maior, cujo uivar podia ser ouvido a longa distância.

O farfalhar das folhas secas, como se tivessem sendo pisadas, denunciava que a desconhecida criatura se movia rapidamente em direção à carroça em que estavam, à espera de uma oportunidade para atacá-los. De repente, um terrível e ensurdecedor uivo dava conta de que estava muito perto deles. Meu avô, espreitando atentamente o perigo, empunhou ao ombro a espingarda que trazia consigo, mirando em direção ao som do uivo. A negritude da noite não permitia divisar qualquer coisa à sua frente. O grande animal, ao aproximar-se, fez com que meu avô enxergasse sua enorme silhueta, que em nada se parecia com um lobo comum. Suas formas medonhas causaram pânico na montaria que puxava a carroça, obrigando meu avô a desatrelá-la dos arreios, fazendo com que seu cavalo, após tombar o coche, disparasse tomando rumo incerto.

Ao perceber que se tratava de um *lobisomem*, o velho tratou de proteger sua velhinha, escondendo-se ambos sob a carroça virada para baixo. Apavorados e escondidos, puderam ver o lobisomem procurando a caça, momento em que começou a arranhar a madeira do veículo e a emitir uivos que soavam raivosamente. Meu avô, neste momento posicionou sua arma em direção ao monstro, efetuando dois disparos com sua arma calibre vinte e oito, cano duplo. Com habilidade suficiente para mais uma vez municiá-la, atirou novamente até que a terrível criatura ao se sentir as dores das feridas causadas ferido pelos tiros cessou o ataque, fugindo velozmente por aquela lúgubre mata. Meus avós permaneceram embaixo da carroça, assustados e em alerta, até o amanhecer.

Ainda hoje, toda vez que percebo o nascer do *plenilúnio noturno*, lembro das histórias sobre um ser meio homem, meio lobo, tendo muito receio de ser por ele unhado ou mordido e ser contaminado por tão terrorificante maldição!

Apesar do medo, guardo muitas saudades dos tempos de minha infância, marcados em minhas memórias de amor.

***Marcelo Adriano de Souza Perobelli***

---

***Quem vê cara, não vê coração***

Contrariamente ao que possamos imaginar, os mitos não somente podem como devem ser levados a sério. Os seres mitológicos são tesouros culturais a nos conectarem com o passado, convidando-nos a explorar o extraordinário. Eles refletem a diversidade da imaginação humana, permanecendo como fontes inesgotáveis de inspiração e reflexão a respeito do mundo que nos cerca.

A Caipora, conhecida como protetora das florestas e dos animais selvagens, era um ser que em minha infância me causa muito medo. Morava em um sítio bem isolado na zona rural, cercado por uma grande mata virgem. Temendo um dia com ela me deparar, pois minha mãe atestava fielmente sua existência e minha professora, ao repetir a história para seus alunos naquela pequena escola rural, incutiram em mim um temor muito grande,

o que impedia sequer me aproximar daquelas áreas repletas de madeiros enormes, cujas copas escureciam os caminhos interiores mesmo nos ensolarados dias.

Em meus pensamentos, a Caipora estaria sempre à espreita de uma desavisada alma a percorrer inocentemente as trilhas. Com seus pés virados para trás, sua pele esverdeada a se mimetizar em meio àquelas verdejantes folhas e com seus cabelos de fogo semelhantes ao não menos temível *boitatá*, sua terrível imagem nunca saiu de minha cabeça. Toda vez, ao escutar o noturno cantar do curiango sobre o mourão da cerca, aterrorizava-me ante ao que parecia ser o prenúncio da aparição daquela horripilante criatura.

Com o passar do tempo, continuei a ouvir a mesma história, o que me fez aos poucos "destravar" deste medo, perdendo inclusive o temor de entrar na mata, levado que fui por meus amigos a tomar um delicioso banho em uma pequena cachoeira que lá existia.

Mesmo por se tratar de uma lenda, agradeci muito por ela proteger os indefesos animais da floresta das maldades perpetradas pelos covardes caçadores com suas daninhas espingardas.

Esteticamente imperfeita para os padrões humanos, taxada convenientemente pelos malvados caçadores como vilã, muitos a continuarão julgando por sua aparência, esquecendo-se do bem que sempre fez e fará por nossas árvores e pelos coloridos passarinhos e mamíferos, fragílimos moradores da verdura de nossas matas.

Portanto, atentemos mais aos corações humanos. Esqueçamos das aparências, pois por trás delas sempre se esconderá um maldoso caçador.

***Lucas Mateus Estevão***

---

***Os corajosos contadores de história***

Nos inocentes anos de minha infância, ouvia muito meus pais e avós contarem várias lendas. Apesar de contos, processavam-se em minha mente de uma maneira muito convincente. *Sacis-Pererês, Botos amazônicos, Mulas sem cabeça, Curupira* e o mais temido deles: o *lobisomem.*

Meu querido avô, com o entusiasmo de um bom contista, sempre repetia para mim esta apavorante história. Tratava-se de um pobre homem, filho mais novo de uma família composta por sete irmãos, tendo recebido não se sabe como e nem por que, em seus poucos treze anos de vida , uma maldição que se manifestava todas as noites de lua cheia. Só por saber que os cabalísticos números "7" e "13", compunham a aterradora combinação, morria de medo durante as aulas de matemática que algum resultado dos exercícios fosse os finais destes dois números.

Segundo o contista, o menino, ao se transformar no tenebroso monstro, andava uivando pelas matas até o amanhecer. Seu uivar, penetrando pelas janelas das casas daquele isolado povoado, causavam pavor em quem os escutava, desencorajando até mesmo o mais temível morador a aventurar-se à noite pelos pastos nos quais, durante o dia, tangiam o gado até a cocheira para lhes tirar o leite do café da manhã e para fazer aqueles deliciosos queijos.

Era este o ambiente do sítio *Seabra* no qual morávamos. Uma grande extensão de terras, com diversas plantações e criações de animais. Os comentários a respeito deste famigerado monstro não se resumiam aos feitos por meu avô. Muitos diziam os terem visto próximo a criações, em busca de comida.

O costume de fazermos fogueiras para ao redor nos reunirmos com familiares e amigos, próximo a uma cabana onde se armazenavam as espigas de milho colhidas, possibilitava a todos travar conversas, cujas fantásticas narrações alimentavam em todos fantasias a revelavam verdades nas mentes de cada um dos ouvintes, não somente nós, as crianças, mas, creio eu, principalmente os adultos, em vista do tamanho realismo com que contavam as várias situações das aparições do *lobisomem.*

Em meio a toda esta magia, nas quais os participantes contavam com maestria seus feitos, pois os vários contistas, exaltando a valentia, escondiam ser em verdade uns covardes de uns medrosos *caguiras*, sempre o *lobisomem* corria de seus enfrentamentos. E eu, na minha santa ingenuidade de criança, perguntava-me: por que ninguém saía para o pasto nas noites de lua cheia?

Por este motivo, até hoje, nas noites iluminadas pela prenúncio da claridade do luar, também não saio quando vou para o sítio.

***Bruno Henrique Pereira Santos***

---

***O mito que tanto temia***

Quando de minha infância, lembro-me da casa na qual morava com minha família, cujos vizinhos eram, também, imigrantes japoneses. Meus avós, nascidos no Japão, emigraram para o Brasil no início do século passado. Habitavam a casa, eu, meus pais, minha irmã e minha avó paterna.

Todas as tardes, minha avó se reunia com suas amigas japonesas, como ela desembarcadas em Santos, destino da longa viagem oceânica. Em meio às conversas, presenciadas por mim e por minha irmã, minha avó reservava um tempo para desfrutar da agradável companhia das netas. "B*atiãn"* narrava com riqueza de detalhes, algumas histórias que para suas pequeninas *"sanseis"* eram aterrorizantes. Extraía seus contos das lendas e folclores mitológicos de seu longínquo e saudoso torrão.

Contava-nos a respeito da existência de uma criatura chamada *Oni:* um ser enorme avermelhado, com aparência humana, mas que tinha um rosto semelhante a um macaco, dotado de presas afiadíssimas na boca, e dois longos chifres pontudos e espiralados, semelhantes aos chifres de um dragão. Sua veste sumária, resumia-se a um pequeno *fundoshi:* uma espécie de tanga utilizada para cobrir as partes íntimas e que deixava as coxas desnudas. Portava em sua mão direita um porrete cravejado com pontas de ferro, nominado *Kanabõ.* Segundo "*batiãn", Oni* usava seu *Kanabõ* para torturar os pecadores no inferno e para castigar os seres humanos que não se comportavam adequadamente neste mundo.

Estas imagens, guardadas em nossas mentes de crianças, causavam-nos muito medo, fazendo-nos tremer a cada vez que ouvíamos *"batiãn"* narrar tão atemorizantes fatos.

Dentre as mais famosas histórias envolvendo o mito *Oni,* está a lenda japonesa conhecida por *Momotarô:* um menino que veio ao mundo dentro de um pêssego gigante. Ao enfrentar *Oni* com a ajuda de seus amigos, terminavam por vencer a árdua batalha, demonstrando coragem e persistência para que o mal sucumbisse ao triunfo do bem. Mesmo sabendo que *Oni* acabava sempre derrotado, permanecia em nossas mentes seu terrível semblante a nos amedrontar.

Passado o tempo, e à medida em que cresci, descobri que os *Onis* não se tratam de demoníacos vilões. Mais que criaturas mitológicas, representam os desafios a serem enfrentados e superados por nós. Aprendi também que a mitologia pode nos ensinar boas lições sobre a vida e a cultura de um povo, no caso, meus ancestrais nipônicos.

No ano de dois mil e seis tive a oportunidade de conhecer a terra de meus avós. Com carinho e muitas saudades deles, relembrei e senti novamente as emoções que me eram causadas ao ouvir estes terríveis contos. E os sentimentos, outrora de medo, transformaram-se em cândidas lembranças de ternura.

Obrigado, *"Batiãn",* por proteger suas netinhas das investidas do malvado *Oni.*

***Marcia Rumiko Yanagava Nakasato***

---

***Eu, minha mãe, e o Homem do Saco.***

Nasci e cresci em uma pequena cidade do interior de São Paulo, com cerca de treze mil habitantes. Naquele lugarejo, todos se conheciam. Foi neste pacato ambiente que, desde a minha infância, meu universo era povoado de histórias contadas pelos adultos, dentre as quais a do *Homem do Saco,* o que me fez acreditar e aprender a temê-lo. Não somente eu, mas muitos amigos daquela comunidade, amedrontavam-se com sua "existência" e sua fome por crianças.

A história era usada como um meio de garantir, pelo temor, a obediência aos adultos e, principalmente, a nossos pais. Minha mãe era uma *expert* em contar tais histórias de terror. Alertava-me constantemente para não falar com estranhos, não seguir ninguém desconhecido e nunca sair sozinho, especialmente à noite. O *Homem do Saco* era apresentado como uma figura sinistra que habitava os becos escuros e áreas isoladas da cidade, à espera de crianças desavisadas.

Um dia, ao questioná-la sobre a veracidade desta assustadora história, descobri que sua intenção ao me narrar, com riqueza de detalhes, a lenda do homem barbudo de cabelos longos, maltrapilho e que trazia consigo um saco no qual "guardava" meninos e meninas por ele capturados, em verdade o fazia para que eu mesmo me resguardasse dos perigos da vida, principalmente quanto ao risco de ser sequestrado. Minha mãe nunca escondeu seu medo, posto ser uma realidade e não um mito. Embora morássemos em um

lugar bem sossegado, sua preocupação comigo era constante. *O Homem do Saco*, com sua ânsia predatória por crianças foi de grande eficácia até mesmo à minha idade adulta, a fim de me conscientizar sobre os perigos do mundo real, para cautelosamente agir, sobretudo no trato com estranhos.

Embora desmistificado, o *Homem do Saco* fez-me compreender e valorizar, em meio a tantos medos e ansiedades, a intensidade do amor maternal a me guardar até hoje. Mamãe, ao me ensinar a virtude da prudência, desejava conscientizar-me e precaver-me a respeito das perigosas situações que se apresentariam a mim no decorrer de minha existência.

Ao vivenciar este *mito*, certamente o repetirei, visando proteger e resguardar meus futuros filhos. Por não ter causado *traumas* em minha personalidade, o *Mito do Homem do Saco*, contrariamente ao seu propósito aterrorizante, será a forma eficaz de proteger e garantir o bem-estar de minhas futuras crianças, assegurando a elas minha constante companhia e cumplicidade durante os preciosos e inocentes anos da infância.

Mamãe, obrigado pela gratuidade do seu amor. Amo-te muitíssimo, também!

Quanto a você, *Homem do Saco*, enfie-se dentro do saco e suma para sempre!

***Luiz Antonio Picco Junior***

---

***Os mitos***

Mitos são figuras que surgem no decorrer de nossas vidas, desde o momento em que interagimos com o mundo exterior, a começar pelas sensações auditivas e pela compreensão do significado das palavras transmitidas a nós por nossos pais e professores.

Mesmo que o tema proposto refira-se ao mito, dispenso, por ora, discorrer sobre o assunto. Prefiro comentar e, por que não, anunciar a Revelação Divina por meio da encarnação de seu Filho, Jesus Cristo.

Para os crentes nesta Verdade, Deus ofertou a nós o verbo encarnado, por meio de uma misteriosa concepção, inexplicável à inteligência humana, mas totalmente diferente dos mitos, estes sim, produtos da imaginação dos homens.

Morto na Cruz para remir os pecados de toda, repito, toda a humanidade, ainda há hoje uma multidão que o nega, o esbofeteia, o escarnece, e que manifesta um grande ressentimento para com aqueles que creem nele e na legião de anjos que o servem, seres reais invisíveis, os quais jamais devem ser confundidos com seres mitológicos. Agradeço a eles por acamparem ao redor de minha vida, e por me acompanharem até o derradeiro e eterno encontro com o Pai.

Falemos agora propriamente dos seres mitológicos, criados a partir das engenhosas imaginações humanas. Alguns deles, a exemplo da "*mula sem cabeça",* povoam a mente de crianças e até mesmo de adultos. A infeliz mulher, transformada neste aterrorizante quadrúpede em decorrência da maldição de ter se *deitado* com um sacerdote, galopa errantemente por escuros campos, anunciando sua macabra presença pelo ruído de suas ferraduras, pelo fogo solto pelas ventas, e por seu estridente relinchar, por vezes parecido com o soluçar humano. Ao leitor, afirmo nunca ter me amedrontado com este lendário ser, mesmo porque nunca morei na roça, tendo conhecido esta história quando estudava no primário.

Mas, peço segredo a respeito do que vou falar! Que vergonha! Que mico!

Já adolescente, estudante no ginásio, corria entre os colegas que uma loira aparecia nos banheiros das escolas. Tratava-se de uma bela jovem que cercava os rapazes que iam sozinhos ao banheiro, geralmente fora do intervalo, quando os professores permitiam a saída individual para o inesperado "*xixi*". Confesso que, por muitas vezes fiquei "*apertado"* na sala de aula por não ter coragem de descer sozinho rumo ao banheiro. Contava com quatorze anos e me pelava de medo da loira retirando os algodões de suas narinas por onde, segundo afirmavam, jorrava muito sangue.

Até hoje não sei se era mito ou verdadeiramente uma assombração. Só sei que durante todo o meu curso ginasial e colegial tive disciplina suficiente para não proferir a fatídica frase: "professor, posso ir ao banheiro?"

Hoje, como estudante do curso de Gestão da Produção Industrial na FATEC Itatiba, comporto-me como um adulto em sala, participando ativamente das aulas, sem qualquer *"aperto"* ou necessidade de sair antes do intervalo.

Quando vou ao banheiro, sempre há outros colegas utilizando as dependências. Pergunto a mim mesmo: será que a loira continua à espreita por aqui?

Que o benefício da dúvida ajude a evitar me deparar com a famigerada mulher!

E você? Deseja ir sozinho ao banheiro da escola?

Boa sorte!

***Junior Gomes Costa***

---

***A menina, o velho e o Saci Pererê***

Ainda pequena, não tive muitas experiências sobre o mundo da mitologia por ter sido criada em um ambiente cristão. Entretanto, quando no período de férias, ao passar

muitos dias na casa de meus avós, lembro da imagem de meu avô, sentado no banco da varanda a me contar uma história na qual existia, na roça, um negrinho a saltar com sua única perna, soltando uma fumaça inalada de seu fétido cachimbo, cuja cabeça se destacava por nela encimar um gorro vermelho que em meio à escuridão do campo, era visto tal qual a brasa do cachimbo.

Atenta a tudo o que dizia, sentada ao seu lado com os olhos arregalados – um misto de medo e curiosidade - suas palavras pintavam vívido quadro de um ser muito travesso a saltitar pelos caminhos para, por fim, após cometer traquinagens, esconder-se nos recônditos das matas mineiras. Enquanto falava, minha criativa imaginação penetrava e viajava em suas histórias, como fosse eu uma destemida menina a acompanhar o moleque Saci por seus caminhos. Cada relato trazia consigo um aviso velado: jamais deveríamos perturbar a ordem natural das coisas. O Saci, apesar de suas travessuras era, segundo meu avô, um guardião das matas das Minas Gerais. O primeiro aviso de sua aparição manifestava-se logo pela manhã, pelo movimento circular das folhas caídas ao chão, as quais erigiam-se em espirais provocadas por pequenos moinhos de vento. Nas noites escuras, caminhar pela roça era como percorrer um território mágico, onde cada sombra escondia segredos. Até mesmo a brisa suave era um sussurro do Saci, um lembrete sobre a fronteira entre o real e o imaginário, muito tênue e desconhecida.

Estas histórias contadas por meu avô, ajudaram a formar meu caráter, e a encantar-me não somente pela lenda, mas por seu olhar de ternura a mim dirigido a cada frase pronunciada. Por vezes, ao divisar a escuridão, meu coração palpitava e minha imaginação corria solta, sempre à espera de possibilidades ainda mais assombrosas. Este medo conferia a mim experiências temperadas com sabor único: uma mistura de adrenalina e respeito pelas coisas desconhecidas.

(In)Felizmente cresci. As aventuras do Saci-Pererê evoluíram de meros contos fantásticos para boas recordações de meu avô, um delicado homem, arqueado e sentado no banco da varanda à luz do lampião de querosene, a me contar as histórias que guardo eternamente nos escaninhos de minhas memórias.

Paralelamente a estas lúdicas narrações, meu avô me fez conhecer, também, a mais Bela História: a Palavra de Deus, que procuro, à medida em que amadureço, conhecer cada vez mais para melhor vivê-la sem medo, mas com muita alegria.

Obrigado vovô, por tanto carinho ofertado. Deus te guarde e proteja.

***Caroliny Fernandes Rodrigues***

---

## *O Lobisomem*

A lenda do *Lobisomem* é um mito mundialmente conhecido e se manifesta fortemente na cultura popular brasileira, dentre várias outras histórias do cancioneiro de nosso rico folclore.

Originário da mitologia greco-romana, cuja denominação *licantropo* significa *Lobo humano*, este ser mitológico foi largamente difundido na Europa, ensejando, além de diversos contos livrescos, uma farta produção cinematográfica cujo desfecho dos filmes focava a figura de um herói revestido com a simplicidade de um aldeão, disparando sobre o monstro um letal projétil confeccionado a partir da fundição de um argentino

*crucifixo,* do qual forjava-se a mortífera *bala de prata.* E ao esvair-se em sangue, junto com ele esvaía-se o encanto, revelando naquele cadáver, uma pobre e insuspeita criatura humana, cuja maldição se materializava nas noturnas sextas-feiras de lua cheia.

E ainda tem gente que pensa em curtir o seu *sextou!*

Contanto que não seja em uma clara noite de lua cheia, curta à vontade, sem esquecer dos perigos reais que rondam as madrugadas regadas a bebidas e outras *"cositas mas".*

E por falar em castelhano, ao referir-me ao *argentino crucifixo*, não pense ser o ostentado pelo *Bergolio.* Argentino quer dizer: feito de prata. Ou você acha que algum *hermano* teria coragem de enfrentar tão terrível criatura?

Voltemos, porém, ao que nos interessa: o aterrorizante e monstruoso ser das noites de luar.

Cresci ouvindo muitas histórias sobre *lobisomens*, muitas delas contadas por minha avó Benedita. Jurava ter visto o horripilante ogro quando, morando no sítio, contava dez anos de idade. Disse-me que numa bela noite de *lua cheia,* estando sozinha na casa, pois seus pais tinham ido com a charrete até o povoado comprar alguns enlatados, além de querosene e pavio para os lampiões, ouviu um barulho estranho vindo do galinheiro. Ao sair para ver o que causava a agitação das galinhas, cacarejando sonoramente como que estivessem em pânico, deparou-se com um ser enorme, peludo, com caninos protuberantes a sair pelos lábios, babando como fosse um cachorro louco. Observou também que tinha enormes pés humanos, sem pelos, com afiadas garras no lugar das unhas. Trazia em uma das mãos uma galinha dilacerada, como se já estivesse iniciado a devora.

Apavorada, fugiu para dentro de casa, fechando as janelas e colocando a tramela na porta, encolhendo-se ao lado do fogão de lenha enquanto rezava para que Nossa Senhora expulsasse aquele demônio do quintal. Não soube me dizer se foi por causa de suas preces ou pela chegada da charrete trazendo seus pais de volta ao sítio. Apenas disse ter certeza que o "*peludo",* como por vezes se referia ao monstro, foi embora da propriedade.

Por muito tempo, a história contada por minha avó muito me atemorizou. Em noites de *lua cheia,* não colocava o nariz fora de casa, nem para brincar com os amigos, ainda que morasse em uma rua iluminada por postes de luz.

O medo do *lobisomem* se foi. As saudades de minha avó, porém, permanecem para sempre, acompanhadas das não menos saudosas lembranças de minha linda infância.

***Willian Rodrigues Ibelino***

## *Conclusão*

Após a leitura destes inusitados casos, a mostrarem um pouco das histórias e experiências afetivas de seus escritores, percebemos que os mitos, produtos do imaginário humano, vivamente relembrados por cada contista, trouxeram-lhes boas recordações da infância e adolescência, em cujas memórias permanecem, indelevelmente gravados, não somente as imagens e ações das monstruosas criaturas mas, principalmente as doces

lembranças de pais, avós, tios e amigos, que com tanta ternura narraram e participaram destes inesquecíveis momentos de suas vidas. A vocês, alunos do curso de Gestão em Tecnologia da Produção Industrial, de nossa pequena e acolhedora FATEC de ITATIBA, com todo o carinho do professor Marcos Guedes.

***Referências***

CAMPBELL, Joseph, ***O Poder e o Mito***. Ed. Palas Athena, São Paulo, 2014

ELIADE, Mircea, ***Mito e Realidade.*** Editora Perspectiva, São Paulo, 2019

ROCHA, Everardo, ***O que é Mito?*** Ed. Brasiliense, São Paulo, 2016

*Plataforma aprendamais*: ***www.mec.gov.br – Curso de Filosofia I***

RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

# Uma revisão sistemática da literatura sobre a utilização de algoritmos de *Machine Learning* para realização de análise de sentimentos

**Stewart Evangelista Gonçalves**
Instituto Federal de Alagoas (IFAL), stewartegoncalves@gmail.com

**RESUMO**

A análise de sentimentos é uma técnica que visa mensurar comentários e notícias por meio de inteligência artificial, é crescente a popularização da área de machine learning a fim da realização dessa análise. O objetivo deste trabalho é investigar e mapear qual é a linguagem mais utilizada no ramo de machine learning, bem como quais algoritmos de NLP são mais utilizados para aplicação da análise de sentimento, e também encontrar qual algoritmo possui maior acurácia nesta aplicação. Como metodologia, foi elaborada uma Revisão Sistemática de Literatura - RSL, onde foram analisados 22 artigos das fontes: Google Scholar e Scielo. Tais estudos foram selecionados com base em critérios de inclusão e exclusão e também via String de busca. Foi observado que a linguagem mais utilizada é Python, já os algoritmos mais utilizados são Naive Bayes, Máquinas de Vetores de Suporte (SVM), Floresta aleatória (Random Forest) e Regressão Logística. Dentre eles, o algoritmo que apresentou maior acurácia ficou sob contexto entre SVM e Random Forest.

**Palavras-chave:** Análise de Sentimentos; Machine Learning; NLP.

Data de Submissão: 09/10/2023

Data Aceito Publicação: 15/05/2024

# *A Systematic Literature Review on the Use of Machine Learning Algorithms for Sentiment Analysis*

**ABSTRACT**

Sentiment analysis is a technique that aims to measure comments and news through artificial intelligence. The objective of this work is to investigate and map which is the most used language in the field of machine learning, as well as which NPL algorithms are most used for the application of sentiment analysis, and also to find which algorithm has the highest accuracy in this application. As a methodology, a Systematic Literature Review - RSL was elaborated, where 22 articles from the sources: Google Scholar and Scielo were analyzed. Such studies were selected based on inclusion and exclusion criteria and also via String search. It was observed that the most used language is Python, since the most used algorithms are Naive Bayes, Support Vector Machines (SVM), Random Forest and Logistic Regression. Among them, the algorithm that presented the highest accuracy was under context between SVM and Random Forest.

**Keywords:** Sentiment Analysis; Machine Learning; NLP.

## 1. Introdução

A análise de sentimentos é uma técnica que tem sido cada vez mais utilizada para extrair informações valiosas de dados não estruturados, como textos de mídias sociais, avaliações de produtos, entre outros. A aplicação de técnicas de análise de sentimentos pode permitir às empresas compreenderem melhor a opinião do público sobre seus produtos ou serviços, identificar problemas e oportunidades de melhoria, e desenvolver estratégias de marketing mais eficazes.

De acordo com Pang e Lee (2008), a análise de sentimentos é o processo de identificação e extração de informações subjetivas de fontes não estruturadas, tais como opiniões, sentimentos e emoções expressos em textos. Essas informações podem ser úteis para diversas áreas, incluindo negócios, política e saúde.

Recentemente o uso de técnicas de machine learning e processamento de linguagem natural (PLN) tornou-se popular para realizar análise de sentimentos em grandes conjuntos de dados de texto. Esta área se trata de problemas relacionados com a compressão e extração de informações a partir de documentos em textos escritos (Freitas, 2014). Algoritmos de aprendizado de máquina têm se mostrado eficazes na realização da análise de sentimentos, permitindo que as empresas possam analisar grandes volumes de dados de maneira eficiente e precisa.

Segundo Ethem Alpaydin (2010), no aprendizado de máquina utiliza-se um modelo definido com base em alguns parâmetros de dados. O aprendizado em si é a otimização dos parâmetros do modelo por meio de treinamento de dados ou de experiências passadas, podendo o modelo ser preditivo – prevendo o futuro de algum cenário –, descritivo – a fim de ganhar conhecimento com os dados –, ou ambos.

Kaur, Sehra S e Sehra K (2017) realizaram uma revisão sistemática de literatura sobre técnicas de análise de sentimentos em mídias sociais e encontraram que a abordagem de aprendizado de máquina é a mais utilizada na literatura, com destaque para algoritmos como Support Vector Machines (SVM), Redes Neurais Artificiais (ANN) e Árvores de Decisão.

Além disso, a análise de sentimentos tem sido amplamente aplicada em pesquisas de software, permitindo a identificação de problemas e tendências em diferentes fases do ciclo de vida do software. Mäntylä (2018) realizou um estudo empírico de análise de sentimentos em avaliações de usuários, bugs e pedidos de melhoria em projetos de software livre, identificando diferenças significativas nos sentimentos expressos em cada tipo de feedback.

Em suma, a análise de sentimentos tem se mostrado uma técnica valiosa para empresas e pesquisadores que desejam compreender melhor a opinião do público sobre produtos, serviços e outros assuntos. Com o uso de técnicas avançadas de aprendizado de máquina, é possível automatizar o processo de análise de sentimentos, tornando-o mais rápido e eficiente.

## 2. Metodologia

Para realização desta revisão sistemática de literatura, foram selecionados artigos que tivessem como foco algoritmos e técnicas utilizadas na análise de sentimentos em

relação a frases e textos. Esta pesquisa utiliza-se de caráter exploratório, pois busca-se um aprofundamento em trabalhos acadêmicos já publicados. Foram excluídos os artigos que não estavam em português ou inglês, que não estavam disponíveis na íntegra, ou que tinham pouca relevância para o tema da revisão.

A presente RSL foi dividida em três fases: Planejamento, condução e documentação, seguindo o protocolo proposto por Kitchenham e Charters (2007).

No período de planejamento, foi realizado o preenchimento do protocolo de RSL, assim, definindo alguns pontos como: objetivo, string de busca, fontes de dados, critérios de inclusão e exclusão. Foi elaborada também as questões de pesquisas, além de definir as fontes de dados que seriam utilizadas na pesquisa.

Na condução iniciou-se a pesquisa bibliográfica de fato, utilizando a string definida no passo acima e exercendo alguns filtros de melhorias, foi obtido fontes literárias preciosas para a relevância do trabalho em questão. Todo esse passo foi elaborado com o objetivo de responder às questões de pesquisas definidas.

Na fase de documentação, foram respondidas as questões pesquisadas, assim resultando no relatório final.

## 2.1. Planejamento

### 2.1.1. Questões de pesquisa

Seguindo o objetivo da RSL, temos a necessidade de encontrar estudos acadêmicos que possuam algoritmos de machine learning que realizem a análise de sentimentos em comentários ou notícias, a fim de criar uma base teórica para desenvolvimento de um estudo posterior. Visando o objetivo, foram definidas três questões de pesquisa:

Questão 1 (Q1) – Quais são as linguagens de programação mais frequentemente utilizadas na implementação de análise de sentimentos?

Questão 2 (Q2) – Quais são os algoritmos de Aprendizado de Máquina mais comumente utilizados na análise de sentimentos?

Questão 3 (Q3) – Dentre os algoritmos de machine learning mais utilizados no contexto de análise de sentimentos, quais apresentam melhores dados de acurácia em comparações entre si?

### 2.1.2. Fontes de dados

A fonte de dados escolhida primeiramente foi o *Google Scholar*, pela facilidade de utilização e por conter conteúdos de outras plataformas, após isso, a fim de realizar uma busca mais elaborada, foram utilizadas outras fontes, como no quadro a seguir:

**Quadro 1. Fontes de dados selecionadas**

| Fonte de dados | Link |
|---|---|
| *Google Scholar* | https://scholar.google.com |
| *Scielo* | https://www.*Scielo*.org |

### 2.1.3. Critérios de inclusão e exclusão

De acordo com Vom Brocke (2009), o processo de inclusão e exclusão deve ser transparente para que a revisão possua credibilidade, assim, temos no Quadro 2, uma série de critérios utilizados no refinamento da fonte, visando a facilidade de uma possível replicação por alguém que venha a se basear neste trabalho.

**Quadro 2. Critérios de inclusão e exclusão**

| Critérios de inclusão | Critérios de exclusão |
|---|---|
| Tccs, monografias, artigos. | Não deixa explícito o algoritmo |
| Publicado entre 2018 e 2023 | Não aborda análise de sentimentos |
| Informar algoritmo | Análise de sentimentos facial, não textual |
| Explicitar base de dados utilizada | Livros |
| Base pública | Indisponíveis e repetidos |

## 2.2. Condução

### 2.2.1. Busca dos trabalhos

Para conseguir encontrar artigos relevantes para o trabalho proposto, fez-se necessária a criação de uma *String* de busca, onde a mesma passou por um processo de refinamento, procurando torná-la mais específica e condizente com o que queremos, e assim ficou:

*(“Machine Learning”or “Deep Learning” or NLP or “aprendizagem de máquina") and ("análise de sentimento”) and (algorithms or algoritmo")*

### 2.2.2. Estratégia de seleção

A pesquisa inicial resultou em 60 trabalhos provenientes de ambas as fontes utilizadas. Ao aplicarmos o primeiro critério de seleção de trabalhos publicados após 2018, o número de resultados reduziu para 42. Dessa forma, prosseguimos com o processo de filtragem, utilizando critérios de inclusão (CI) e critérios de exclusão (CE).

Após a aplicação dos CI e CE sobraram 22 estudos que se adequaram ao objetivo final desta RSL. A Tabela 1 mostra a quantidade de estudos selecionados por fonte de dados.

**Tabela 1. Quantidade de trabalhos selecionados por fonte**

| Fonte de dados | Qtd de resultados | Qtd após seleção |
|---|---|---|
| Google Scholar | 42 | 22 |
| Scielo | 0 | 0 |

A planilha detalhada com título dos trabalhos, autores, ano, base de dados, algoritmos utilizados e uma breve análise da conclusão pode ser acessada no seguinte link: https://tinyurl.com/ybtfab3y

## 3. Resultados

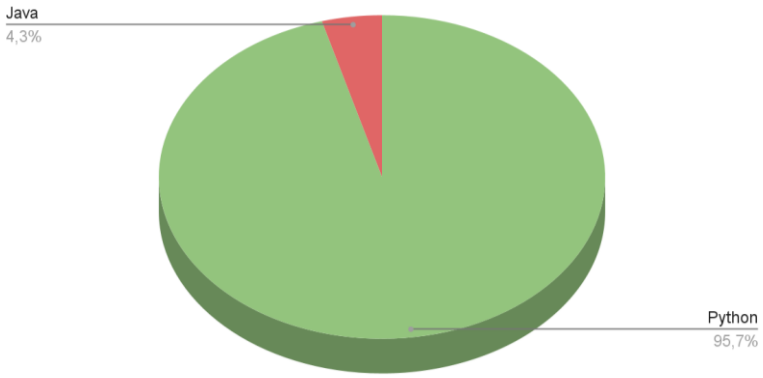
Com base na investigação e análise dos estudos realizados, foi possível responder às perguntas de pesquisa propostas e alcançar o objetivo da revisão sistemática da literatura. A seguir, cada questão será abordada e respondida com base nos dados obtidos a partir dos estudos selecionados.

**Q1 – Quais são as linguagens de programação mais frequentemente utilizadas na implementação de análise de sentimentos?**

No total, foram analisados 22 trabalhos com aplicações práticas de análise de sentimentos, um dos pré-requisitos da seleção, foi que dentro dos artigos tivessem exemplificações e trechos de códigos utilizados nos algoritmos, a fim de avaliar de fato a linguagem adotada, sem suposições.

O foco da questão é identificar qual linguagem está sendo mais utilizada no momento, para replicação em um trabalho futuro, por isso é tão importante que os artigos sejam novos e atualizados.

**Figura 1. Linguagens de programação mais utilizadas**



Presente em 95,7% dos trabalhos analisados como a linguagem mais utilizada para implementação da análise de sentimentos, o Python demonstra predominância para atividades envolvendo *Data science*, já que possui um uso intuitivo para computação quantitativa e analítica, além de contar com um grande banco de dados de bibliotecas voltadas para inteligência artificial e *machine learning.*

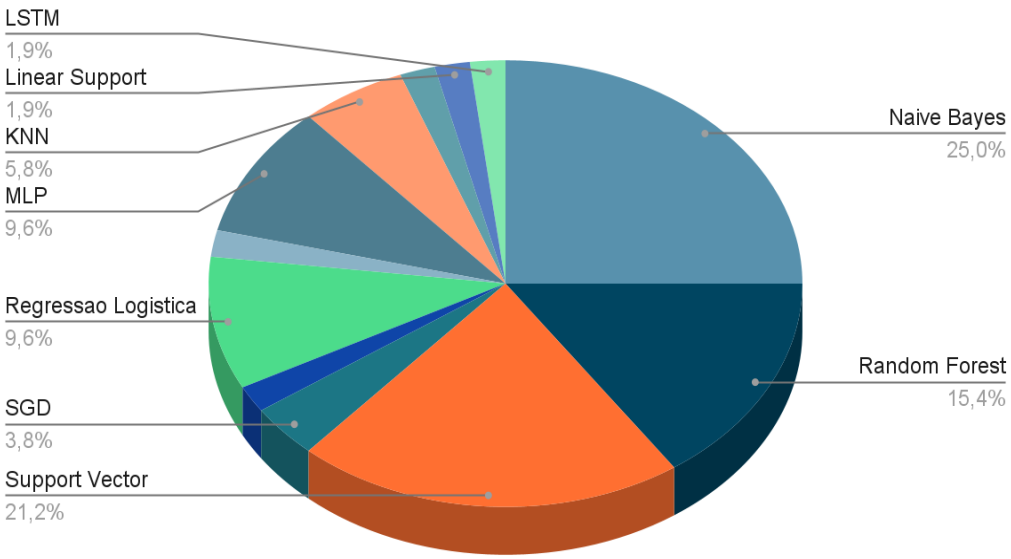
**Quadro 3. Linguagens mais utilizadas na implementação de análise de sentimentos**

| Linguagem | Refs dos artigos |
|---|---|
| Python | [A01], [A02], [A03], [A04], [A05], [A06], [A07], [A08], [A10], [A11], [A12], [A13], [A14], [A15], [A16], [A17], [A18], [A19], [A20], [A21], [A22]. |
| Java | [A09] |

**Q2 – Quais são os algoritmos de Aprendizado de Máquina mais comumente utilizados na análise de sentimentos?**

Dos 22 artigos analisados, cada um apresentou sua particularidade e diversidade em técnicas, fomentando a pluralidade de respostas. Foram mapeados todos os algoritmos de classificação utilizados em todos os trabalhos, considerando que alguns trabalhos possuem mais de um algoritmo em seu corpo, em caso de existir no trabalho estudado algum tipo de comparação entre os modelos.

**Figura 2. Algoritmos tradicionais mais utilizados**



Conforme o gráfico acima, percebe-se que três algoritmos possuem maior predominância em utilizações, que são: *Naive Bayes, Support Vector Machine* (SVM) e *Random Forest*, respectivamente.

O *Naive Bayes* ganha pontos por possuir diversas aplicações e por sua simplicidade aliada aos bons resultados que gera. Já o SVM é eficaz na classificação de dados complexos e separáveis por hiperplanos, o que é muito útil quando há um grande número de atributos e a separação das classes é clara. Por sua vez, o *Random Forest* é baseado em conjunto de árvores de decisão. Ele cria várias árvores independentes e, em seguida, combina suas previsões para obter um resultado final.

Observa-se que cada técnica possui suas vantagens e desvantagens, e a escolha de qual técnica utilizar depende do objetivo da análise e dos dados disponíveis.

**Quadro 4. Algoritmos tradicionais mais utilizados**

| Algoritmos | Refs dos artigos | Número de citações |
|---|---|---|
| *Naive Bayes* | [A01], [A02], [A04], [A05], [A06], [A07], [A08], [A09], [A10], [A15], [A18], [A20], [A21] | 13 |
| *Random Forest* | [A01], [A06], [A08], [A09], [A10], [A14], [A15], [A20] | 8 |
| *Support Vector Machines* (SVM) | [A02], [A03], [A06], [A08], [A09], [A10], [A12], [A15], [A18], [A19], [A20] | 11 |
| SGD | [A02], [A08] | 2 |
| XGBoost | [A02] | 1 |
| Regressão Logística | [A03], [A05], [A06], [A08], [A15] | 5 |
| LGBM | [A05] | 1 |
| MLP | [A05], [A08] [A11], [A16], [A20] | 5 |
| KNN | [A06], [A08], [A12] | 3 |
| *Decision Tree* | [A15] | 1 |

| | | |
|---|---|---|
| *Linear Support Vector Classification* (LSVC) | [A21] | 1 |
| LSTM | [A22] | 1 |

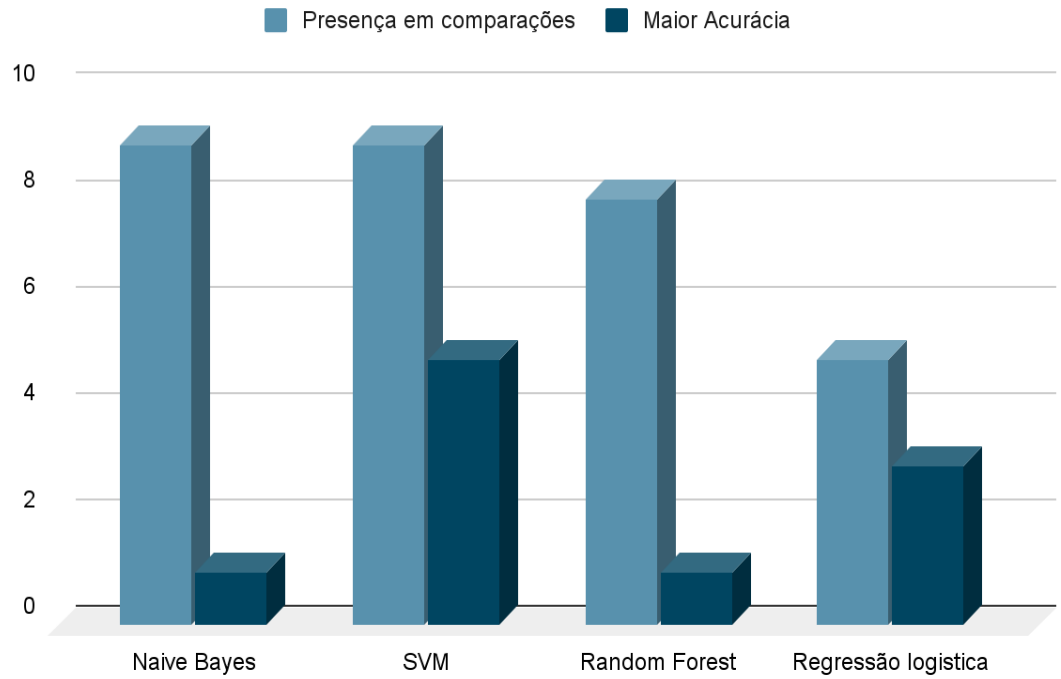
**Q3 – Dentre os algoritmos de *machine learning* mais utilizados no contexto de análise de sentimentos, quais apresentam melhores dados de acurácia em comparações diretas?**

Apesar de termos inúmeros algoritmos de *machine learning*, separamos os mais utilizados com base na questão anterior, e partimos para uma análise em busca da melhor acurácia.

Para essa questão foi adicionado mais um critério de inclusão: apenas trabalhos que exercem comparação de algoritmos. Com isso, dos 22 trabalhos utilizados em questões anteriores, restaram apenas 11.

Para encontrar essa resposta, utilizamos uma métrica de valor agregado sob a presença, ou seja, anota-se quantas vezes o algoritmo aparece em algum tipo de comparação, após isso, é necessário encontrar em quantos desses trabalhos o algoritmo foi tido como o de maior acurácia pelo pesquisador do estudo.

**Figura 3. Algoritmos NLP com maior presença e sua acurácia**



Nota-se no gráfico que o *Naive Bayes* aparece em 9 dos 11 artigos, mas apesar de sua enorme participação, ele foi considerado o de melhor acurácia em apenas 1 dos artigos em que esteve presente. Realizando uma divisão de **presença/maior acurácia**, ficamos com uma porcentagem de 11,11%.

Já o SVM, presente também em 9 artigos, consegue ser muito mais efetivo que o anterior, temos maior acurácia em 5, calculando sua porcentagem obtemos que em 55% das vezes em que ele está sendo comparado, o mesmo consegue ter maior acurácia que os outros métodos.

O *Random Forest* vem um pouco mais atrás, pois está presente em 8 artigos e é considerado o mais efetivo em apenas 1, obtendo a taxa de 12,5% após ter a presença em comparações de algoritmos dividida pela maior acurácia.

O algoritmo de Regressão Logística aparece como uma grande surpresa, apesar de ser pouco utilizado se comparado aos outros, ele apresenta um cálculo de 3 vitórias em 5 participações, ou seja, em 60% das vezes em que está envolvida em comparações, ela lidera com a melhor acurácia.

**Quadro 5. Linguagens mais utilizadas na implementação de análise de sentimentos**

| Linguagem | Presente em | Número de citações | Maior acurácia |
|---|---|---|---|
| SVM | [A02], [A03], [A06], [A08], [A09], [A10], [A14], [A15], [A20] | 9 | [A02], [A06], [A09], [A10], [A14] |
| Regressão logística | [A03], [A05], [A06],[A08], [A15] | 5 | [A03], [A05], [A08] |
| Naive Bayes | [A01], [A02], [A05][A06], [A08], [A09][A10], [A15], [A20] | 9 | [A01] |
| Random Forest | [A01], [A06], [A08], [A09], [A10], [A14], [A15], [A20] | 8 | [A20] |

## 4. Conclusão

Os resultados dos estudos analisados mostraram que o python é predominantemente utilizado quando se trata de linguagem de programação voltada para uso em machine learning, é justificável, visto que suas bibliotecas facilitam o trabalho dos desenvolvedores da área.

Com relação aos algoritmos de classificação mais utilizados para aplicação da análise de sentimentos, apesar da existência de inúmeros métodos, alguns acabam se destacando pela sua facilidade de implementação, outros por sua capacidade produtiva e outras qualidades, mas nota-se que há uma certa preferência por alguns como: Naive Bayes, SVM, Random Forest e Regressão logística.

Também foi visto que apesar da popularidade de alguns modelos, quando levamos em conta principalmente sua acurácia, alguns modelos podem não ser tão bons quanto parecem, já outros aparecem como uma grande surpresa, com números de acurácia muito bons.

Desta forma, essa revisão sistemática de literatura mostrou o que tem de mais atual no meio acadêmico na área de machine learning para elaboração de análise de sentimento utilizando algoritmos de machine learning.

**Referências:**

ALPAYDIN, E. **Introduction to Machine Learning**. MIT Press, 2010. Disponível em: <http://nuir.nkumbauniversity.ac.ug/xmlui/bitstream/handle/20.500.12383/1421/Introduction%20to%20Machine%20Learning,%20Second%20Edition%20(Adaptive%20Computation%20and%20Machine%20Learning)%20(%20PDFDrive%20).pdf?sequence=1>. Acesso em: 19/05/2023.

FREITAS, Cláudia. Sobre a construção de um léxico da afetividade para o processamento computacional do português. **Revista Brasileira de Linguística Aplicada**, Rio de Janeiro, v. 13, n. 4, p. 1031-1059, dez. 2013. Disponível em: <https://doi.org/10.1590/S1984-63982013005000024>. Acesso em: 19/05/2023.

KAUR, J.; SEHRA, S. S.; SEHRA, S. K. A systematic literature review of sentiment analysis techniques. **International Journal of Computer Sciences and Engineering**, v. 5, n. 4, p. 22-28, 2017.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. In: **Technical report**, Ver. 2.3 EBSE TechnicalReport EBSE. [S.l.]: Epidemiol. Serv. Saúde, 2007.

MÄNTYLÄ, Mika; GRAZIOTIN, Daniel; KUUTILA, Miikka. The evolution of sentiment analysis—A review of research topics, venues, and top cited papers. **Computer Science Review**, v. 27, p. 16-32. fev. 2018. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S1574013717300606>. Acesso em: 21/05/2023.

PANG, Bo; LEE, Lillian. Opinion mining and sentiment analysis. **Foundations and Trends in Information Retrieval**, v. 2, n. 1-2, p. 1-135, jul. 2008. Disponível em: <https://www.nowpublishers.com/article/Details/INR-011>. Acesso em: 19/05/2023.

VOM BROCKE, J. *et al*. Reconstructing the giant: On the importance of rigour in documenting the literature search process. *In*: Proceedings of the 17th European Conference on Information Systems, 2009, Verona. ***Anais eletrônicos*** [...] Verona, 2009, p. 1-13. Disponível em: <https://www.researchgate.net/publication/259440652_Reconstructing_the_Giant_On_the_Importance_of_Rigour_in_Documenting_the_Literature_Search_Process>. Acesso em: 25/05/2023.

RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

# Os Impactos da Inteligência Artificial (IA) na Enfermagem

**Djones Braz de Araujo Costa**
Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro – IFRJ,
djones.braz@gmail.com
**Flávia dos Santos Alves**
Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro – IFRJ

**RESUMO**

Este estudo examina como a Inteligência Artificial (IA) afeta as práticas de enfermagem. Ele aborda as suas aplicações na área de saúde. A revisão de pesquisas mostra que a IA está se tornando cada vez mais importante na enfermagem para fins como diagnóstico de enfermagem precoce, monitoramento de pacientes, otimização de processos hospitalares e tomada de decisões clínicas. Além dos benefícios claros, como a melhoria da eficácia e precisão dos cuidados em saúde, o estudo também enfatiza as questões éticas relacionadas à supervisão humana e à proteção dos dados. A pesquisa aborda os problemas da IA na enfermagem, como a necessidade de treinamento adequado e adaptação aos contextos clínicos e abordagem terapêutica. Assim, este artigo fornece uma visão abrangente dos avanços e desafios da IA na enfermagem, destacando seu potencial transformador no campo da assistência à saúde.

**Palavras-Chave:** Inteligência Artificial; Enfermagem; Saúde; Tomada de Decisão; Ética.

Data de Submissão: 09/10/2023

Data Aceito Publicação: 15/05/2024

# The Impacts of Artificial Intelligence (AI) in Nursing

**ABSTRACT**

This study examines how Artificial Intelligence (AI) affects nursing practices. It addresses its applications in the health sector. The research review shows that AI is becoming increasingly important in nursing for purposes such as early diagnosis, patient monitoring, optimizing hospital processes, and clinical decision-making. In addition to clear benefits such as improving the effectiveness and accuracy of healthcare, the study also emphasizes ethical issues related to human oversight and data protection. The research addresses the problems of AI in nursing, such as the need for adequate training and adaptation to clinical contexts. Thus, this article provides a comprehensive overview of the advances and challenges of AI in nursing, highlighting its transformative potential in the field of healthcare.

**Key Words:** Artificial Intelligence; Decision Making; Ethic; Health; Nursing.

## 1. Introdução

A Inteligência Artificial (IA) está transformando o mundo da saúde. Tem o potencial de melhorar os cuidados de enfermagem e médicos e por extensão a toda equipe multidisciplinar. A inteligência artificial (IA), que consiste em sistemas de aprendizado de máquinas e algoritmos sofisticados, está rapidamente se tornando uma ferramenta vital para enfermeiros e outros profissionais de saúde. A maneira como os enfermeiros fazem diagnósticos de enfermagem, tratamentos e acompanhamento de pacientes está mudando devido à sua capacidade de analisar grandes quantidades de dados, identificar padrões complexos e tomar decisões baseadas em evidências.

No entanto, essa mudança trouxe consigo vários desafios e questões éticas que devem ser considerados com cuidado. As preocupações sobre a confiabilidade das decisões automatizadas, a privacidade dos dados dos pacientes e como isso afeta o relacionamento enfermeiro-paciente surgem à medida que a IA se torna mais comum nas práticas de enfermagem.

Logo, essa mudança trouxe consigo vários desafios e questões éticas que devem ser considerados com cuidado.

## 2. Revisão da Literatura

### 2.1 Definição de Inteligência Artificial (IA)

Uma área da ciência da computação conhecida como inteligência artificial (IA) se concentra no desenvolvimento de sistemas de computadores capazes de realizar tarefas que normalmente exigiriam a inteligência humana. A IA envolve algoritmos e técnicas de aprendizado de máquinas que permitem que os sistemas processem dados, identifiquem padrões, tomem decisões e, em alguns casos, aprendam e se adaptem com base em experiências anteriores (Guimarães, 2020).

### 2.2 Breve histórico da IA na saúde

Os primeiros sistemas de apoio à decisão clínica desenvolvidos nas décadas de 1960 e 1970 representam o início da história da IA na saúde. No entanto, devido ao aumento da disponibilidade de dados de saúde eletrônicos e ao desenvolvimento de algoritmos avançados, a IA começou a se tornar mais importante no campo da saúde nos últimos anos. Essa tendência tem sido particularmente evidente na enfermagem, onde a IA está sendo usada para melhorar os resultados dos pacientes e otimizar processos.

### 2.3 Aplicações da IA na Enfermagem

Na enfermagem, a IA pode ajudar na tomada de decisões em prescrição de cuidados e na automação de tarefas administrativas. Exemplos incluem sistemas de triagem automatizada, monitoramento contínuo de pacientes, assistência na interpretação de exames e até mesmo robôs de enfermagem que podem auxiliar na administração de medicamentos (Silva et al., 2018).

### 2.4 Vantagens da utilização da IA na Enfermagem

As vantagens da implementação da IA em enfermagem são substanciais. A IA pode tornar os diagnósticos de enfermagem mais precisos, os erros médicos menores e os processos clínicos e de cuidados mais rápidos, permitindo que os enfermeiros se concentrem em tarefas mais complexas e centradas no paciente. Isso pode levar a uma assistência mais eficaz e eficiente (Oliveira et al., 2021).

### 2.5 Desafios e preocupações éticas

No entanto, os avanços da IA na enfermagem também apresentam problemas. Precisamos nos preocupar com questões como a privacidade dos dados dos pacientes, a confiabilidade das decisões automatizadas, a responsabilidade legal e os efeitos no relacionamento enfermeiro-paciente. O equilíbrio entre a automação e o cuidado humano é uma questão crítica (Topol, 2019).

### 2.6 Estudos anteriores relacionados ao tema

Estudos anteriores examinaram uma variedade de aspectos da IA na enfermagem. O estudo examinou como eles podem melhorar os cuidados de saúde e os problemas éticos e práticos associados. Além disso, conferências acadêmicas, como a International Conference on Computational Science and Its Applications (2019), têm proporcionado um fórum para discutir o progresso e os desafios da IA na enfermagem (Amisha et al., 2019). Esse trabalho fornece uma visão geral das principais questões relacionadas à IA na enfermagem, enfatizando como ela pode mudar a prática de enfermagem e quais questões precisam ser levadas em consideração.

## 3. Metodologia

### 3.1 Descrição da abordagem metodológica

A metodologia utilizada neste estudo é uma revisão bibliográfica sistemática. A revisão bibliográfica é uma ferramenta amplamente reconhecida para a análise crítica e síntese de pesquisas existentes, permitindo uma compreensão abrangente do tópico em questão (Chen et al., 2019).

### 3.2 Descrição das fontes de dados

Esta revisão foi baseada em artigos de revistas científicas, conferências, livros, sites de órgãos reguladores de saúde e portais de notícias de saúde. Essas fontes foram escolhidas porque eram relevantes para o assunto de enfermagem da IA.

### 3.3 Critérios de seleção de estudos ou casos

Os critérios de seleção para inclusão dos estudos na revisão bibliográfica foram os seguintes:

1. **Relevância:** O uso da IA na enfermagem deve ser o foco de estudos.

2. **Atualidade:** Para garantir que abranja os desenvolvimentos mais recentes, a literatura considerada deve ser datada a partir de 2017.
3. **Qualidade:** Os estudos revisados por pares e publicados em fontes confiáveis devem ter prioridade.

### 3.4 Procedimentos de análise de dados

Para analisar os dados, seguimos os seguintes procedimentos:

1. Identificar e selecionar fontes relevantes usando padrões definidos.
2. Ter uma leitura cuidadosa e uma síntese dos principais resultados e conclusões encontrados em cada fonte.
3. Agrupar os resultados em categorias como usos da IA na enfermagem, vantagens, desafios e questões éticas.
4. Analisar e comparar estudos selecionados para identificar tendências e lacunas na literatura.
5. Discutir cuidadosamente os resultados e como eles afetam a enfermagem.

Esta revisão bibliográfica utilizará uma metodologia que permitirá uma análise aprofundada dos efeitos da IA na enfermagem. Isso criará uma base sólida para a discussão e os resultados deste estudo.

## 4. Resultados:

Uma revisão abrangente da literatura sobre os efeitos da Inteligência Artificial (IA) na enfermagem encontrou muitos resultados importantes. Esses resultados destacam o quanto a IA está se tornando cada vez mais importante na prática de enfermagem e na forma como afeta a qualidade dos cuidados de saúde.

### 4.1 Aplicações da IA na Enfermagem

A ampla aplicação da IA na enfermagem é um dos principais resultados desta revisão. A automação de tarefas administrativas, o suporte à tomada de decisões clínicas, o monitoramento contínuo e a triagem de pacientes são alguns dos vários campos da assistência à saúde que usam a IA para melhorar. Por exemplo, sistemas de triagem automatizada podem identificar pacientes que precisam de atenção imediata com base em sintomas e histórico médico (Oliveira et al., 2021). Ao direcionar recursos para os pacientes que mais precisam, essas ferramentas podem aumentar a eficiência dos hospitais.

### 4.2 Vantagens da Utilização da IA na Enfermagem

Esta revisão também mostrou os benefícios da implementação da IA na enfermagem. A inteligência artificial demonstrou ser capaz de reduzir os erros médicos e tornar os diagnósticos clínicos mais precisos. Por meio da análise de grandes conjuntos de dados, a IA pode identificar padrões sutis que os profissionais de saúde humanos

podem perder, contribuindo para diagnósticos mais precisos e tratamentos personalizados (Topol, 2019).

### 4.3 Exemplos de Sucesso na Aplicação de IA na Enfermagem

Existem muitos exemplos de aplicação bem-sucedida da IA na enfermagem. O uso de algoritmos de aprendizado de máquina para prever a deterioração clínica em pacientes hospitalizados é um caso notável. Esses sistemas monitoram continuamente sinais vitais e históricos médicos, alertando enfermeiros e médicos sobre mudanças significativas no estado do paciente, permitindo intervenções precoces (Silva et al., 2018).

A utilização da IA para a interpretação de exames médicos, como radiografias e exames de imagem, é outro exemplo bem-sucedido. Algoritmos de visão computacional treinados podem identificar anomalias com precisão e rapidez, acelerando o processo de diagnóstico (Chen et al., 2019).

### 4.4 Discussão sobre como a IA está sendo usada na prática

A IA está sendo amplamente usada na enfermagem em vários contextos. Em hospitais, sistemas de gerenciamento de enfermagem alimentados por I.A. ajudam a alocar enfermeiros com base na carga de trabalho e na complexidade do atendimento. Isso melhora a distribuição de recursos e a qualidade do cuidado ao paciente (Guimarães, 2020).

Outra área de aplicação é a gestão de medicamentos. Robôs de enfermagem equipados com IA podem administrar medicamentos de forma precisa e consistente, reduzindo erros de medicação (Carvalho, 2019). Além disso, a IA é usada na triagem de pacientes em unidades de emergência, priorizando casos mais críticos com base em dados clínicos e históricos médicos (Oliveira et al., 2021).

É importante lembrar que a IA não substitui enfermeiros, mas os ajuda. Os enfermeiros ainda são muito importantes para avaliar o bem-estar emocional dos pacientes, comunicar e fornecer cuidados holísticos.

### 4.5 Desafios e Preocupações Éticas

A aplicação da IA na enfermagem apresenta benefícios e questões éticas. A proteção dos dados dos pacientes é um grande problema. A IA depende de uma grande quantidade de informações pessoais de pacientes, o que levanta preocupações sobre o armazenamento seguro e o acesso a esses dados (Chen et al., 2019).

Além disso, a confiabilidade das decisões automatizadas é uma preocupação crítica. Os sistemas de IA devem ser altamente precisos e, em casos de diagnóstico incorreto ou tomada de decisões inadequadas, questões de responsabilidade legal surgem (Topol, 2019).

A supervisão humana também é importante. Embora a IA possa realizar tarefas complexas, a supervisão humana continua sendo necessária para garantir que os pacientes estejam seguros e para interpretar os detalhes do tratamento. O equilíbrio entre a

automação e a intervenção humana é uma área de foco em estudos futuros (Guimarães, 2020).

### 4.6 Resultados Estatísticos

Muitos estudos, em termos de dados estatísticos, fornecem evidências quantitativas de melhorias na precisão dos diagnósticos e no atendimento ao paciente. Por exemplo, um estudo recente demonstrou que a adoção de sistemas de monitoramento de pacientes baseados em IA resultou em uma redução de 25% nas taxas de mortalidade hospitalar (Oliveira et al., 2021).

### 4.7 Conclusão dos Resultados

Cada vez mais, a IA está se tornando um componente essencial da enfermagem e da assistência à saúde em geral. Isso aumenta a precisão dos diagnósticos, a eficiência clínica e a qualidade do atendimento. No entanto, questões éticas, preocupações com a privacidade dos dados e a necessidade de supervisão humana continuam sendo importantes.

Esses resultados mostram o quão importante é uma abordagem equilibrada para a integração da IA na enfermagem, que leva em consideração tanto as vantagens quanto os problemas. O uso consciente da IA na enfermagem pode melhorar significativamente a assistência médica, fornecendo cuidados mais eficientes e eficazes.

## 5. Discussão

Os resultados desta revisão bibliográfica incluem uma análise minuciosa dos principais resultados e seus efeitos na prática de enfermagem. O foco desta revisão é as implicações, problemas e questões éticas que surgem com a crescente integração da Inteligência Artificial (IA) na área de saúde, particularmente na enfermagem.

### 5.1 Interpretação dos Resultados

Os resultados desta revisão mostram que a IA está se tornando cada vez mais importante na enfermagem e ajudando a melhorar significativamente a qualidade dos cuidados de saúde. A eficácia da IA na otimização de processos clínicos e na redução de erros é demonstrada por sua aplicação bem-sucedida na triagem de pacientes, monitoramento contínuo, interpretação de exames e administração de medicamentos. Além disso, a IA pode identificar padrões clínicos complexos e fornecer insights valiosos, complementando as habilidades dos enfermeiros (Topol, 2019).

Ainda assim, é importante lembrar que a IA não é um substituto para os enfermeiros; em vez disso, atua como um auxiliar valioso. Os enfermeiros continuam desempenhando um papel vital na avaliação do bem-estar emocional dos pacientes, na comunicação e na prestação de cuidados individualizados e holísticos (Guimarães, 2020).

### 5.2 Discussão sobre as Implicações dos Resultados

Os resultados têm vários significados e afetam a prática de enfermagem e na assistência à saúde em geral. A IA na enfermagem pode ajudar a fazer diagnósticos mais precisos, tratamentos mais personalizados e melhores resultados para os pacientes. A IA também pode permitir que as enfermeiras se concentrem mais no atendimento direto aos pacientes, reduzindo o trabalho administrativo.

### 5.3 Abordagem dos Desafios e Limitações da IA na Enfermagem

A IA tem vantagens na enfermagem, mas também tem desvantagens. As preocupações éticas são particularmente importantes. Problemas de privacidade e segurança surgem com a coleta e uso de dados de pacientes. A proteção dos dados do paciente é de extrema importância, e os sistemas de IA devem ser projetados para garantir o sigilo das informações (Chen et al., 2019).

A confiabilidade das decisões automatizadas deve ser abordada também. Para garantir a precisão de suas ações, a IA deve ser treinada com conjuntos de dados representativos e monitorada continuamente. Erros na tomada de decisões clínicas podem ter consequências graves (Topol, 2019).

Outra preocupação significativa é a supervisão humana. Embora a IA possa realizar tarefas complexas, a intervenção humana é necessária para entender os detalhes do atendimento e tomar decisões moralmente e contextualmente adequadas. Portanto, a automação não deve ser implementada de forma a substituir completamente o julgamento humano (Guimarães, 2020).

### 5.4 Reflexão sobre as Questões Éticas Envolvidas

Ao falar sobre IA na enfermagem, é importante pensar na ética. Princípios como transparência, responsabilidade, equidade e justiça são parte da ética da IA. Os profissionais de saúde devem ser capazes de entender como a tomada de decisões automatizadas funciona. Além disso, a responsabilidade legal deve ser estabelecida em casos de erros ou falhas (Chen et al., 2019).

Uma preocupação ética fundamental é a equidade. Para evitar discriminação e preconceito, os sistemas de IA devem ser treinados com dados diversos e representativos. É fundamental garantir que a IA não fomente a desigualdade.

### 5.5 Comparação com Estudos Anteriores

Esta revisão bibliográfica apoia-se em pesquisas anteriores sobre os avanços da IA na enfermagem. Esta revisão bibliográfica apoia pesquisas anteriores sobre os avanços da IA na enfermagem. Da mesma forma, o estudo de Chen et al. (2019) enfatizou a importância da ética na IA em saúde, especialmente no que diz respeito à privacidade e à equidade.

A revisão atual também oferece uma visão completa dos avanços, problemas e consequências éticas da IA na enfermagem, melhorando nossa compreensão.

### 5.6 Considerações sobre a Discussão

A IA está se tornando cada vez mais importante no campo da enfermagem e da assistência à saúde. Seu potencial é inegável para otimizar processos e melhorar a qualidade dos cuidados. No entanto, é difícil lidar com questões éticas, proteger a privacidade dos dados dos pacientes e equilibrar a automação com o cuidado humano.

A discussão neste tópico enfatiza a importância de adotar uma abordagem sensata e responsável para a incorporação da IA na enfermagem. Os enfermeiros são essenciais para monitorar e entender as ações da IA para garantir que o cuidado ao paciente permaneça no centro da assistência à saúde.

Portanto, a capacidade de abordar esses problemas é crucial para o futuro da enfermagem e da IA. Se conseguirmos fazê-lo, a IA poderá ser usada como uma ferramenta valiosa e ética na prestação de cuidados de saúde de alta qualidade.

## 6. Considerações Finais

### 6.1 Resposta às Questões de Pesquisa

As questões de pesquisa levantadas neste estudo foram abordadas de maneira abrangente:

1. **Quais são as aplicações da IA na Enfermagem?** A automação de tarefas administrativas, apoio à tomada de decisões clínicas e monitoramento contínuo de pacientes são algumas das aplicações da IA na enfermagem.
2. **Quais são as vantagens da utilização da IA na Enfermagem?** A melhoria da precisão diagnóstica, a redução dos erros médicos e a otimização de processos clínicos são alguns dos benefícios.
3. **Quais são os desafios e preocupações éticas associados à IA na Enfermagem?** Problemas como a privacidade dos dados, a confiabilidade das decisões automatizadas e a necessidade de supervisão humana estão entre as preocupações. A transparência, a responsabilidade, a equidade e a justiça são questões éticas.

### 6.2 Implicações Práticas e Recomendações

Este estudo tem consequências significativas no campo da enfermagem e da assistência à saúde em geral. Quando usada de forma ética e responsável, a IA pode ser uma ferramenta útil para melhorar a qualidade dos cuidados.

Recomenda-se que as instituições de saúde tenham políticas e diretrizes claras sobre como usar a IA na enfermagem, considerando privacidade, segurança de dados e responsabilidade legal. Além disso, os enfermeiros devem ser treinados adequadamente para entender e monitorar as ações da IA.

Por fim, a IA pode ajudar na enfermagem melhorando a eficiência e a qualidade dos cuidados de saúde. No entanto, questões éticas e desafios práticos devem ser considerados ao fazê-lo. Os profissionais de saúde, os pesquisadores e os formuladores

de políticas são responsáveis por garantir que o uso da IA na enfermagem seja ético. Eles devem se concentrar no equilíbrio entre a automação e o cuidado humano.

**Referências**

AMISHA et al. Artificial Intelligence in Healthcare: Past, Present and Future. In: International Conference on Computational Science and Its Applications, 2019, p. 3-18. DOI: 10.1007/978-3-030-24307-0_1.

CARVALHO, P. V. R. Enfermagem e Inteligência Artificial: Perspectivas Futuras. Editora Atheneu, 2019.

CHEN, J. H. et al. Artificial Intelligence in Health Care: Anticipating Challenges to Ethics. Journal of Medical Internet Research, v. 21, n. 12, p. e16184, 2019. DOI: 10.2196/16184.

CONSELHO FEDERAL DE ENFERMAGEM (COFEN). Inteligência Artificial e o Exercício da Enfermagem, 2021. Disponível em: http://www.cofen.gov.br/inteligencia-artificial-e-o-exercicio-da-enfermagem_83736.html.

GUIMARÃES, A. R. Inteligência Artificial na Saúde. Editora Manole, 2020.

HEALTHCARE IT NEWS. Artificial Intelligence in Nursing: How Tech is Transforming the Role, 2020. Disponível em: https://www.healthcareitnews.com/news/artificial-intelligence-nursing-how-tech-transforming-role.

JIANG, F. et al. Artificial Intelligence in Healthcare: Past, Present, and Future. In: International Joint Conference on Artificial Intelligence, 2017, p. 51-57. DOI: 10.24926/jai.2017.5717.

OLIVEIRA, R. S. et al. Aplicações da Inteligência Artificial na Prática de Enfermagem: Uma Revisão Integrativa. Revista Brasileira de Enfermagem, v. 74, n. 3, p. e20190520, 2021. DOI: 10.1590/0034-7167-2019-0520.

SILVA, M. A. et al. O Papel da Inteligência Artificial na Tomada de Decisões em Enfermagem. Revista de Enfermagem UFPE Online, v. 12, n. 3, p. 872-879, 2018. Disponível em: http://www.revista.ufpe.br/revistaenfermagem/index.php/revista/article/view/14473.

TOPOL, E. J. High-Performance Medicine: The Convergence of Human and Artificial Intelligence. Nature Medicine, v. 25, n. 1, p. 44-56, 2019. DOI: 10.1038/s41591-018-0300-7.

RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

# A Segurança da Informação: uma observação sobre os aspectos técnicos, humanos, sociais e jurídicos conhecidos

**Anderson Julianelli do Nascimento**
Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro – IFRJ
**Djones Braz de Araujo Costa**
Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro – IFRJ,
djones.braz@gmail.com

**RESUMO**

Este artigo visa discutir o impacto dos aspectos técnicos, humanos, sociais e legais na área da Segurança da Informação como um todo. Buscaremos a compreensão sobre como esses fatores afetam a segurança dos dados digitais e como podemos nos preparar para minimizar os efeitos causados pelos riscos e ameaças aos quais estamos sujeitos em nosso dia a dia. Analisaremos também se o Brasil está preparado para atuar em casos de incidentes e o que vem fazendo para coibir os ataques cibernéticos. Já quanto à parte jurídica, por se tratar de uma matéria nova e que se modifica constantemente, observamos o estágio de adaptação da legislação brasileira à realidade atual. Por fim, concluímos sugerindo a adoção de métodos e padrões de combate a ataques cibernéticos.

**Palavras-Chave**: Segurança da Informação; Ameaças; Ataques; Melhores Práticas.

Data de Submissão: 17/10/2023

Data Aceito Publicação: 15/05/2024

# Information Security: an observation on the known technical, human, social and legal aspects.

**ABSTRACT**

This article aims to discuss the impact of technical, human, social and legal aspects in the area of Information Security as a whole. We will seek to understand how these factors affect the security of digital data and how we can prepare to minimize the effects caused by the risks and threats to which we are subject in our daily lives. We will also analyze whether Brazil is prepared to act in cases of incidents and what it has been doing to curb cyber attacks. As for the legal part, as it is a new matter that is constantly changing, we observe the stage of adaptation of Brazilian legislation to the current reality. Finally, we will conclude by suggesting the adoption of methods and standards to combat cyber attacks.

**Key Words:** Best practices; Information security; Threats; Attacks.

## 1. Introdução

Este artigo propõe analisar as modificações nas ferramentas aplicadas para garantir a segurança da informação, considerando o desenvolvimento das técnicas e das tecnologias num recorte de 60 anos, de 1957 a 2017. Ao longo desse artigo, pretende-se também apontar como o comportamento humano e social impacta diretamente os sistemas cibernéticos, tanto para métodos de invasão como para procedimentos de defesa. Todavia, não podemos deixar de destacar os esforços empregados na elaboração de legislações específicas sobre ameaças cibernéticas e as aplicações das sanções cabíveis a estes criminosos.

O artigo pretende observar três frentes bem experimentadas, são elas: a visão tecnológica, o comportamento humano e social e as ferramentas legais disponibilizadas para o combate desses crimes. Em conjunto, essas frentes formam uma tríade bastante sólida capaz de nos dar informações relevantes sobre o comportamento destes criminosos e também de nós, usuários. Por conseguinte, estes dados serão analisados e, com base nestas análises, serão sugeridas novas metodologias de defesa, técnicas de prevenção, tecnologias para mitigação de ataques cibernéticos, políticas de segurança e dispositivos legais para dirimir inconveniências causadas por este tipo de infração.

Dentre a imensa variedade de dados que trafega pelo ciberespaço, destacamos as transações bancárias, responsáveis por inúmeros negócios, e que estão sujeitas a todos os tipos de ameaças imagináveis. Devemos estar sempre atentos e preparados para todo tipo de ameaça que possamos vir a sofrer, empregando todas as ferramentas conhecidas e atuando no desenvolvimento de novas ferramentas.

O tema escolhido para este artigo científico tem a sua relevância social, pois atualmente o mundo inteiro está conectado, ou seja, vivemos num cenário globalizado em que a rapidez e a facilidade para se comunicar com outras pessoas, empresas, governos, entre outros, e essa realidade se deve à concepção da internet. Essa rede global que interliga a todos sem distinção e que em um período tão curto, se comparado à revolução industrial, alcançou um patamar imensurável e indispensável para todos nós, haja vista que hoje seria impossível pensarmos em não haver trocas de informações em tempo real.

## 2. Fundamentação teórica

### 2.1. Os fundamentos de segurança da informação

Para entendermos o que tratamos como segurança da informação, primeiramente, devemos entender que a internet que conhecemos hoje está em constante transformação devido a velocidade dos avanços tecnológicos. Permitindo assim, em um futuro próximo, o surgimento da Web Semântica ou como a maioria dos especialistas estão chamando, Internet 3.0. Essa nova forma de uso da internet que está por vir, será capaz de organizar e usufruir de todo conhecimento adquirido e disponível na rede mundial de uma forma mais inteligente, onde dados de fontes distintas serão embaralhados de maneira imediata a partir de dados acessados e conectados entre si.

Garantir a segurança da informação em ambiente digital constitui, cada vez mais, uma preocupação à escala mundial, seja por parte de organismos públicos, privados,

universidades, empresas e até pelos cidadãos, de forma individual ou coletiva. (PEREIRA, 2005, p.67).

Deste modo, com as possibilidades que surgirão a partir dessa nova internet, deveremos prestar mais atenção nos conteúdos disponibilizados na rede. A maneira como usamos essas informações e a segurança que deveremos empregar em nossas redes terão um papel cada vez mais importante no cenário cibernético.

Em seu artigo científico Canongia & Mandarino (2009) nos esclarecem que, em março de 2009 ocorreu a reunião da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), preocupados com os rumos que a nova sociedade da informação está tomando recentemente. Dentre os vários pontos explicitados nesta reunião, destaca-se a discussão sobre a cultura de segurança como um vetor estratégico das nações, onde os seguintes aspectos foram evidenciados:

- Cada parte envolvida tem um importante papel para assegurar a segurança em função de suas competências, e devem ser sensibilizados sobre os riscos associados à segurança de sistemas e redes de informação;
- As questões de segurança devem ser objeto de preocupação e responsabilidade de todos os atores, seja governamental, empresarial, e de outros (pesquisa e terceiro setor).

Segundo a International Communications Union (ITU), cybersecurity significa basicamente prover proteção contra acesso, manipulação, e destruição não autorizada de recursos críticos e bens. Para a promoção da cybersecurity, a ITU considera as seguintes áreas como foco principal:

a. Áreas de elevada atenção: Combate ao crime cibernético, Criação em nível nacional de CERTs/CSIRTs (*Computer Emergency Response Teams/Computer Security Incident Response Teams*); Aumento da cultura de segurança cibernética e suas atividades; e Promoção da educação;
b. Áreas com menos atenção: Pesquisa e Desenvolvimento; Avaliação e monitoramento; e Atendimento às pequenas e médias empresas (PMEs). (SUND, 2008).

Na esfera pública do Brasil, dois conceitos são empregados e dão sustentação à abordagem da segurança cibernética, são eles:

> [...] "infraestrutura crítica da informação", bem como "ativos de informação". Para o governo federal brasileiro, considera-se "infraestrutura crítica da informação" o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. E, complementarmente, consideram-se "ativos de informação", os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios, e as pessoas que a eles têm acesso. (BRASIL, Portaria n. 34.2009).

Os "Princípios para a Governança e Uso da Internet no Brasil", criado em fevereiro de 2009, pelo Comitê Gestor da Internet no Brasil (CGI.br), tem o objetivo de normatizar a estabilidade, a segurança e a funcionalidade globais da rede. No entendimento do CGI.br, esses três pontos devem ser preservados de forma ativa através

de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

Para assegurarmos uma boa segurança da informação, devemos nos ater as suas principais propriedades, a confidencialidade - é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las; integridade – é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas e, disponibilidade – é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisem.

## 2.2. A importância da segurança cibernética e a prevenção de riscos e ameaças

Um dos primeiros princípios para um bom serviço de segurança digital é o controle de acesso. Além disso, outros princípios são fundamentais para minimizar o risco de incidentes, sendo eles:

> **Autenticação** é o serviço de segurança que pode ser utilizado para assegurar que as pessoas que acessam a rede sejam autorizadas;
> **Confidencialidade** é o serviço de segurança que pode ser utilizado para assegurar que os dados, o software e as mensagens não sejam expostos a partes não-autorizadas;
> **Integridade** é o serviço de segurança que pode ser utilizado para assegurar que partes não-autorizadas não modifiquem os dados, o software e as mensagens;
> **Não-repúdio** é o serviço de segurança que pode ser utilizado para assegurar que as entidades envolvidas em uma comunicação não possam negar sua participação nesta comunicação. Especificamente, a entidade que envia não pode negar que tenha enviado uma mensagem (não-repúdio como prova de origem) e a entidade receptora não pode negar ter recebido uma mensagem [não-repúdio como prova de entrega] (BURNETT & PAINE, 2002, p.279).

Inúmeros autores, como os citados por Pereira (2005) em seu artigo, quando abordam a segurança da informação digital fazem uma primeira distinção entre a segurança física e a lógica. CARNEIRO (2002), quando discorre sobre segurança física da informação digital, propõe a sua subdivisão em 3 subgrupos: de pessoal, de equipamentos e de instalações.

## 2.3. Os aspectos legais e normativos da segurança da informação

Um documento digital só terá validade jurídica se cumprir com alguns requisitos, como os que já são feitos aos documentos tradicionais. Tanto para os documentos digitais quanto para os tradicionais são exigidas verificações de sua autenticidade, da integridade e da tempestividade. Para garantir a identificação e autenticidade das pessoas que assinam estes documentos eletrônicos, foram criadas as Autoridades Certificadoras, que intermediam a relação entre usuários por meio de um sistema cifrado de comunicação assimétrica. A medida provisória no. 2.200, de 28 de junho de 2001, dispõe sobre a infraestrutura de Chaves Públicas Brasileiras – ICP – Brasil, que instituiu o Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira (CG ICP-Brasil), e cuja função é de autoridade gestora de políticas de certificação digital, ao qual garantirá a segurança e demais aspectos apresentados sobre os documentos digitais.

Atualmente, podemos nos pautar em padrões internacionais de segurança cibernética, como as normas ISO/IEC, específicas para as áreas de segurança da informação, para tentar dirimir ou até mesmo minimizar os efeitos causados por incidentes e/ou ataques sofridos diariamente. Pereira (2005) informa em seu artigo que:

> A norma ISO/IEC 17799 é relativa à segurança da informação e procura contribuir para a segurança das organizações, dos seus colaboradores, instalações e, sobretudo, dos sistemas de informação, sendo o seu título 'Tecnologias da Informação – Código de prática para a gestão da segurança da informação'". PEREIRA (2005, p.75).

## 2.4. Segurança cibernética: práticas e políticas adotadas no brasil

A Administração Pública Federal (APF), o Gabinete de Segurança Institucional da Presidência da República (GSIPR), por meio de seu Departamento de Segurança da Informação e Comunicação (DSIC), desenvolveram em colaboração com vários órgãos da APF e seus representantes, e em conjunto ao Comitê Gestor de Segurança da Informação (CGSI), um conjunto de normas que visam garantir a segurança da informação e comunicações para o governo. Além disso, as normas também estão focadas em impulsionar a criação de grupos de trabalhos técnicos e na formação de recursos humanos capazes de tratar temas relativos à segurança cibernética.

A publicação da Instrução Normativa IN GSIPR No. 01/2008, possui relevância quanto ao tema segurança da informação, pois disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indiretamente. O documento define que "Segurança da Informação e Comunicações (SIC) são as ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações", trazendo consigo uma nova ideia de inovação e ampliação do entendimento tradicionalmente adotado na segurança da informação.

Podemos identificar parâmetros e valores principais na SIC com relação aos conceitos descritos na IN GSIPR No.01/2008, são eles:

> **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade; integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
> **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada; e,
> **Autenticidade:** propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou *entidade*. (GSIPR, No.01/2008).

Destacamos também as seguintes publicações com relação ao desenvolvimento e implantação da SIC em órgão e entidades da APF, são elas:

- **NC 03/IN 01/DSIC/GSIPR** - "Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal", Portaria No. 29, publicada no D.O.U de No. 125, em 03 de julho de 2009;

- **NC 04/IN 01/DSIC/GSIPR** - "Gestão de Risco de Segurança da Informação e Comunicações – GRSIC nos Órgãos e Entidades da Administração Pública Federal", Portaria No. 37, publicada no D.O.U de No. 156, em 17 de agosto de 2009; e,
- **NC 05/IN 01/DSIC/GSIPR** - "Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos Órgãos e Entidades da Administração Pública Federal", Portaria No. 38, publicada no D.O.U No. 156, em 17 de agosto de 2009.

Diante de todo exposto, vimos que nosso país possui os instrumentos e mecanismos necessários para o desenvolvimento de nossa segurança da informação e comunicações. O Brasil possui normatizações próprias, adequadas à realidade de nosso país, e com reconhecimento internacional, capaz de atender qualquer eventualidade que possa surgir com relação às ameaças virtuais.

## 3. Considerações finais

Este artigo tem a intenção de discutir questões sobre Segurança da Informação abordando seus aspectos técnicos, humanos, sociais e legais e demonstrando como cada um destes influencia o desenvolvimento de novas técnicas e metodologias.

Durante a reflexão, detectamos que a nossa legislação ainda está em fase inicial, em se tratando especificamente de leis para combate aos crimes digitais. Contudo, temos que reconhecer que o primeiro passo no sentido de regulamentar esses crimes cometidos na esfera tecnológica já foi dado com a sanção da Lei 12.737/2012 (Lei Carolina Dieckman), a qual discorre sobre a tipificação criminal de delitos informáticos.

Além disso, devemos também uma parcela de atenção à nossa legislação penal em vigor, pois esta encontra-se desatualizada com relação à realidade dos dias atuais. Nosso código penal data da década de 40, portanto, não condiz com a realidade atual. É necessária uma grande reforma jurídica com a criação de leis específicas para o combate aos crimes digitais. Sem dispositivos legais que considerem o novo cenário virtual, atualmente adaptamos as leis existentes aos crimes cometidos na esfera digital.

## Referências

ABREU, Karen Cristina Kraemer. História e usos da Internet. Artigo Científico. Disponível em: <http://www.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf>. Acesso em: 16 agosto 2018.

BRASIL, Decreto n. 6.605, de 14 de outubro de 2008. O Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil exerce a função de autoridade gestora de políticas de certificação digital. Disponível em: <https://www.iti.gov.br/comite-gestor>. Acesso em: 25 out 2018.

_____, Decreto n. 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa e dá outras providências. Disponível em: <http://www.fab.mil.br/portal/defesa/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 18 de agosto de 2018.

_____, Fundamentos de Segurança da Informação. Disponível em: <https://www.cert.br/docs/palestras/certbr-egi2014.pdf>. Acessado em: 24 setembro 2018.

_____, Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 25 out 2018.

_____, Segurança Cibernética: onde estamos e onde deveríamos estar? Disponível em: < https://www.cert.br/docs/palestras/certbr-painel-telebrasil2018.pdf>. Acessado em: 24 setembro 2018.

_____, Gabinete de Segurança Institucional da Presidência da República (GSIPR). Lei n. 10.683, de 28 de maio de 2003. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.683.htm>. Acesso em: 18 de agosto de 2018.

_____, Norma Complementar 03/IN01/DISC/GSIPR. Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgão e Entidades da Administração Pública Federal. Diário oficial da União, n. 125, 03 jul 2009. Disponível em: < http://dsic.planalto.gov.br/legislacao/nc_3_psic.pdf>. Acesso em: 18 de agosto de 2018.

_____, Norma Complementar 04/IN01/DISC/GSIPR. Gestão de Risco de Segurança da Informação e Comunicações – GRSIC nos Órgão e Entidades da Administração Pública Federal. Diário oficial da União, n. 156, 17 ago 2009. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf> Acesso em: 18 de agosto de 2018.

_____, Norma Complementar 05/IN01/DISC/GSIPR. Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais nos Órgão e Entidades da Administração Pública Federal. Diário oficial da União, n. 156, 17 ago 2009. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_05_grsic.pdf> Acesso em: 18 de agosto de 2018.

_____, Portaria n. 34, de 05 de agosto de 2009. Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Diário oficial da União, n. 149, 06 ago 2009. Disponível em: <http://www.mctic.gov.br/mctic/opencms/legislacao/portarias/migracao/Portaria_CGSIPR_n_34_de_05082009.html> Acesso em: 25 de agosto de 2018.

_____, Portaria n. 35, de 06 de agosto de 2009. Institui Grupo de Trabalho de Criptografia, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Diário oficial da União, n. 150, 07 ago 2009. Disponível em: < http://www.transportes.gov.br/images/Portaria_223-2009.LLX.pdf> Acesso em: 25 de agosto de 2018.

BURNETT, Steve; PAINE, Stephen. Criptografia e Segurança: O Guia Oficial RSA. Rio de Janeiro: Campus, 2002.

CANONGIA, Claudia; MANDARINO JR., R. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

CARNEIRO, Alberto. Introdução à Segurança dos Sistemas de informação. Lisboa: FCA Editores, 2002. In: PEREIRA, Pedro Jorge Fernandes. Segurança da informação digital. Cadernos BAD 1. 2005. Lisboa: BAD. p.66-80, 2005.

DEPARTMENT OF HOMELAND SECURITY (DHS). National Infrastructure Protection Plan: partnering to enhance protection and resiliency. EUA: DHS, 2009. p.12.

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. A SEGURANÇA DOS DOCUMENTOS DIGITAIS. 2011. Artigo Científico – Postado em: 03 mar 2011. No site: Portal de e-governo, inclusão digital e sociedade do conhecimento. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/seguran%C3%A7a-dos-documentos-digitais>. Acessado em: 16 ago 2018.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). Global Cybersecurity Agenda (GCA): framework for international cooperation. Switzerland: ITU, 2007. p.10. In: _____. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

LYRA, Maurício Rocha. Segurança e Auditoria em Sistemas de Informação. 2 ed. Rio de Janeiro: Ciência Moderna, 2017.

MANDARINO JR., R. Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro. 2009. Monografia aprovada no Curso de Especialização em Gestão de Segurança da Informação e Comunicações. Brasília: Universidade de Brasília – UNB/Departamento de Ciência da Computação, jun 2009. p.29. In: _____. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). Guidelines for the security of information systems and networks: towards a culture of security. Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 july 2002. Paris: OECD, 2002. 28p. In: _____. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

_____, Recommendation of the council on the protection of critical information infrastructure: Adopted as a Recommendation of the OECD Council at its 1172th Session on 30 april 2008. Seoul, jun. 2008. In: _____. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

PEREIRA, Pedro Jorge Fernandes. Segurança da informação digital. Cadernos BAD 1. 2005. Lisboa: BAD. p.66-80, 2005.

SILVA, D. R. P. da; STEIN, Lilian Milnitsky. Segurança da informação: uma reflexão sobre o componente humano. 2007. Artigo Científico – Ciência & Cognição, 2007. Vol.10. p. 46-53. Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Porto Alegre-RS, 2007.

SUND, Christine. Promoting a culture of Cybersecurity. In: ITU REGIONAL CYBERSECURITY FORUM FOR EASTERN AND SOUTHERN AFRICA, Lusaka, 25-28 Aug 2008, Lusaka: ITU, 2008. In: _____. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

# Arquitetura *Zero Trust*: boas práticas de gestão de riscos de segurança da informação.

**Eduardo Nascimento**
FATEC Americana
**João Emmanuel S'Alkmin Neves**
FATEC Americana, joao.neves11@fatec.sp.gov.br

**RESUMO**

O presente artigo discorre sobre o modelo ZTA, cuja abordagem consiste na confiança zero, no que tange à gestão de riscos de segurança da informação. A revisão bibliográfica permite a disseminação do conceito, e a compreensão detalhada dos princípios e da composição da arquitetura Zero Trust. Acompanhada da análise de boas práticas encontradas atualmente, evidencia-se as vantagens e os benefícios de sua implantação, e ainda se apresentam as dificuldades, desde a aceitação de um novo paradigma por parte de gestores, quanto a mobilização para a introdução de uma nova cultura e estratégia, sem negligenciar o investimento necessário para colocar este modelo em prática. Ao final do trabalho as considerações sobre os desafios futuros e algumas sugestões, afinal o modelo não encerra em si mesmo, é adaptado e adaptável às necessidades e às particularidades de cada corporação, quanto ao acesso aos dados, exigindo a melhoria contínua de sua estrutura e processos.

**Palavras-chave:** Arquitetura; Confiança zero; Gestão de riscos; Organizações; Segurança de rede.

Data de Submissão: 14/11/2023

Data Aceito Publicação: 15/05/2024

# Zero Trust Architecture: best practices for managing information security risks.

**ABSTRACT**

This article discusses the ZTA model, whose approach consists of zero trust, regarding information security risk management. The bibliographic review allows the dissemination of the concept, and a detailed understanding of the principles and composition of the Zero Trust Architecture. Accompanied by the analysis of good practices currently found, the advantages and benefits of its implementation are highlighted, and difficulties are still presented, since the acceptance of a new paradigm by managers, to the mobilization for the introduction of a new culture and strategy, without neglecting the investment necessary to put this model into practice. At the end of the work, considerations about future challenges and some suggestions, after all the model does not close in itself, it is adapted and adaptable to the needs and particularities of each corporation, in terms of access to data, requiring continuous improvement of its structure and processes.

**Keywords:** Architecture; Enterprises; Network security; Risks Management; Zero trust.

## 1 INTRODUÇÃO

No cenário atual, com a rápida evolução digital, as organizações enfrentam o desafio de protegerem seus dados e sistemas sensíveis contra ameaças cibernéticas, que se tornam proporcionalmente cada vez mais frequentes e sofisticadas.

Segundo dados da Fortinet (2023), no ano de 2022 houve mais de 360 bilhões de tentativas de ciberataques somente na América Latina e Caribe, sendo o México o país com maior número, 187 bilhões de tentativas, seguido do Brasil com 103 bilhões.

Os modelos tradicionais de segurança da informação, nos quais predomina a implantação de sistemas de defesa em perímetro, revelam-se inadequados diante do avanço dos métodos de ataques.

Por essa razão, um número cada vez maior de organizações começa a adotar novas formas de abordagem na segurança de seus ativos, com medidas efetivas e abrangentes, que buscam desenvolver o Sistema de Gestão de Segurança da Informação (SGSI) e, consequentemente, melhorar os processos de mitigação de riscos e ameaças, oriundas tanto do ambiente externo quanto interno, bem como da infraestrutura de tecnologia da informação. Assim, desponta como uma solução adequada e estratégica, a *Zero Trust Architecture* (ZTA).

Este artigo discorre sobre a implantação crítica da Arquitetura *Zero Trust* como um novo modelo e paradigma, uma mudança de mentalidade e de gestão de riscos de segurança da informação, ao trazer os princípios e as estratégias fundamentais concernentes à estrutura ZTA. Utiliza-se da revisão bibliográfica sobre o tema, e tem como objetivo geral, contribuir com ideias para as organizações protegerem seus dados e sistemas de maneira eficaz. Como objetivo específico, apresenta três casos reais de empresas renomadas, trazendo o que há de mais novo na área, com a finalidade de confrontar teoria e prática, comprovar os fatos, justificando pesquisas substanciais e fomento a um assunto tão emergente.

## 2 ZERO TRUST: CONCEITOS, PRINCÍPIOS E COMPOSIÇÃO

Em uma rede na qual a estrutura delimita sua segurança em perímetro, com a utilização de um conjunto de ativos de segurança como *firewall*, servidores de autenticação como RADIUS, pela aplicação do protocolo 802.1X etc., presume-se que todo acesso autorizado por estes filtros sejam de origem confiável e podem, a partir de então, obterem acesso a toda rede de acordo com o nível de permissão definido pelo servidor. Porém, autorizado o acesso, ignora-se qualquer ação que possa gerar vulnerabilidades e trazer riscos ou ameaças como consequência, seja intencionalmente ou não.

Nessa medida, pensando na possibilidade de invasão da rede e na obtenção de acesso aos ativos de tecnologia da informação, quando um atacante consegue permear as defesas e conseguir acesso, ele tem a possibilidade de movimento lateral dentro da rede – o que não é detectado pelas defesas perimetrais já que o acesso foi autorizado – e, assim, tentar elevar seu nível de permissão até que consiga acesso como administrador da rede.

Isso se tornou um grande problema para as organizações, já que os processos gerenciais para a manutenção de uma rede segura passaram a requerer maior cuidado e esforço contínuo de planejamento e gestão. Além disso, devido à disseminação da

computação em nuvem, dos dispositivos móveis e do trabalho remoto e, especialmente, na atual situação em que os dados e informações se tornaram ativos mais valiosos e o mundo cada vez mais global e digital, o modelo de defesa por perímetro mostrou-se inadequado, para não dizer obsoleto.

Partindo destas adversidades criou-se o conceito de desperimetralizar e, em seguida, o termo "confiança zero" na segurança cibernética passou a ser adotado como um novo paradigma de arquitetura e gerenciamento dos ativos de tecnologia da informação.

Na norma NIST 800-207 da *National Institute of Standards and Technology*, Rose et al (2020), descreve a arquitetura de confiança zero (ZTA) como um plano de segurança cibernética empresarial que utiliza conceitos de confiança zero e abrange relacionamentos de componentes, planejamento de fluxo de trabalho e políticas de acesso. Uma empresa de confiança zero é a infraestrutura de rede (física e virtual) e as políticas operacionais que estão em vigor para a empresa como produto de um plano de arquitetura de confiança zero (ROSE *et al*, 2020).

Entende-se como confiança zero, ou *Zero Trust* (ZT), o processo que desenvolve um conjunto de ideias e princípios com o intuito de reduzir a incerteza na aplicação de decisões que restringem e limitam o acesso a sistemas e serviços de informação dentro de um ambiente de rede que possa estar comprometido (ROSE *et al*, 2020).

Esse processo parte, basicamente, da solicitação de acesso a um recurso (sistema, dados ou aplicação) onde a origem é uma zona não confiável, que por sua vez passa por um ponto de decisão de políticas a serem atribuídas e possa ter acesso a um recurso dentro de uma zona implicitamente confiável. A NIST apresenta um modelo abstrato que ajuda a compreender como se dá o acesso a uma zona *Zero Trust*.

A partir deste conceito, baseia-se a confiança zero no princípio de "nunca confiar, sempre verificar", ou seja, a confiança nunca deve ser automaticamente assumida ou presumida por qualquer usuário, dispositivo ou sistema, independentemente da sua localização na rede e do seu nível de permissão de acesso; ao contrário, deve ser enfatizada a verificação contínua da identidade e da conduta de segurança antes da concessão de acesso aos recursos.

Rose *et al* (2020) esclarecem que, uma arquitetura de confiança zero é projetada e implantada com adesão aos seguintes princípios básicos, a saber:

a. **Todas as fontes de dados e serviços computacionais são considerados recursos.** Uma rede pode ser composta por múltiplas classes de dispositivos e ter dispositivos pequenos que enviam dados para agregadores/armazenamento, software como serviço (SaaS), sistemas que enviam instruções para atuadores e outras funções.
b. **Toda comunicação é protegida independentemente da localização da rede**. A confiança não deve ser concedida automaticamente com base no fato de o dispositivo estar na infraestrutura de rede corporativa. Toda comunicação deve ser feita da maneira mais segura disponível, protegendo a confidencialidade e a integridade e fornecendo autenticação da fonte.
c. **O acesso a recursos empresariais individuais é concedido por sessão.** A confiança no solicitante é avaliada antes que o acesso seja concedido. O acesso também deve ser concedido com o mínimo de privilégios necessários para concluir a tarefa. A

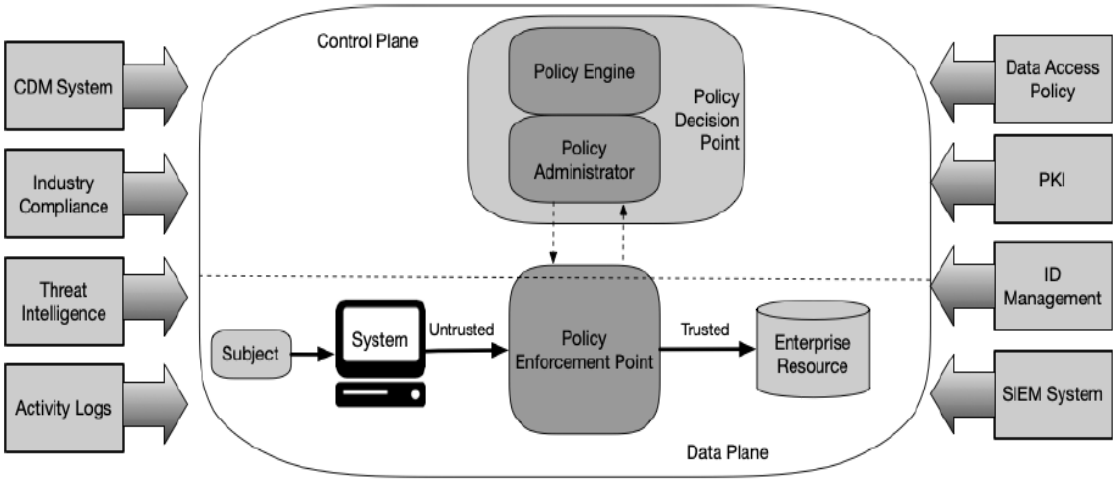
autenticação e a autorização para um recurso não serão concedidas automaticamente a um recurso diferente.

d. **O acesso aos recursos é determinado por políticas dinâmicas, incluindo o estado observável da identidade do cliente, da aplicação/serviço e do ativo solicitante, e englobar outros atributos comportamentais e ambientais**. A organização define como será feita a proteção de seus recursos e membros e delimita o acesso a eles, conforme suas necessidades de acesso. Para confiança zero, a identidade do cliente pode incluir a conta do usuário (ou identidade de serviço) e quaisquer atributos associados concedidos pela empresa. A solicitação do estado do ativo pode incluir características do dispositivo, como versões de software instaladas, localização da rede, hora/data da solicitação, comportamento observado anteriormente e credenciais instaladas. Os atributos comportamentais incluem análises automatizadas de assuntos, análises de dispositivos e desvios medidos dos padrões de uso. Essas regras e atributos são baseados nas necessidades do processo de negócios e no nível aceitável de risco.
e. **A empresa monitora e mede a integridade e a postura de segurança de todos os ativos próprios e associados**. Nenhum ativo é inerentemente confiável. A empresa avalia a postura de segurança do ativo ao avaliar uma solicitação de recurso. Uma empresa que implemente uma ZTA deve estabelecer um diagnóstico e mitigação contínuos (CDM) ou sistema semelhante para monitorar o estado de dispositivos e aplicativos e aplicar *patches*/correções conforme necessário. Os ativos descobertos como subvertidos, com vulnerabilidades conhecidas e/ou não gerenciados pela empresa podem ser tratados de maneira diferente. Isto também se aplica a dispositivos associados, por exemplo, dispositivos de propriedade pessoal, que podem ter permissão para acessar alguns recursos, mas não outros, e requerem um sistema robusto de monitoramento.
f. **Toda autenticação e autorização de recursos são dinâmicas e rigorosamente aplicadas antes que o acesso seja permitido**. Este é um ciclo constante de obtenção de acesso, verificação e avaliação de ameaças, adaptação e reavaliação contínua da confiança na comunicação. Espera-se que uma empresa que implemente uma ZTA possua sistemas de gerenciamento de identidade, credenciais e acesso, e de gerenciamento de ativos em funcionamento, incluindo o uso de autenticação multifator, e o monitoramento contínuo com possível reautenticação e reautorização durante as transações do usuário, a fim de se alcançar um equilíbrio entre segurança, disponibilidade, usabilidade e eficiência de custos.
g. **A empresa coleta o máximo de informações possível sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as utiliza para melhorar sua postura de segurança**. A empresa deve coletar dados sobre a postura de segurança de ativos, tráfego de rede e solicitações de acesso, processar esses dados e usar o conhecimento obtido para melhorar a criação e aplicação das políticas (ROSE *et al*, 2020).

Existem ainda vários componentes lógicos que constituem uma implantação ZTA em uma empresa. Esses componentes podem ser operados como um serviço local ou por meio de um serviço baseado em nuvem (ROSE *et al*, 2020).

A seguir, o esquema de arquitetura ZTA e as considerações quanto aos componentes lógicos que contemplam a sua estrutura.

**Figura 1 - Modelo *Zero Trust* do NIST 800-207 e seus componentes lógicos.**




**Fonte: ROSE *et al*, 2020.**

Os componentes apresentados correspondem a uma estrutura principal de controle (*Control Pane*) contendo o Mecanismo de Política ou *Policy Engine* (PE), responsável pela decisão final de concessão de acesso a um recurso para determinado sujeito, utilizando políticas organizacionais, entradas e fontes externas, e o Administrador de Políticas ou *Policy Administrator* (PA), destinado a estabelecer e/ou interromper a comunicação dos recursos, gerando uma sessão específica de autenticação/autorização de um cliente para com o recurso organizacional. O PA está diretamente ligado ao PE e depende deste para conceder ou negar acesso solicitado pelo Ponto de Aplicação de Políticas (ROSE *et al*, 2020).

O Ponto de Aplicação de Políticas ou *Policy Enforcement Point* (PEP) é responsável por habilitar, monitorar e eventualmente finalizar a conexão entre o sujeito e o recurso, além de repassar requisições ao Administrador de Políticas (PA) e deste receber atualizações de políticas. É o componente que está entre o Sistema (não confiável) e os Recursos Organizacionais (confiáveis) (idem, 2020).

Juntamente com os componentes principais da ZTA, há uma série de fontes de dados que provêm políticas e regras de entrada que dão suporte às decisões de concessão de acesso. São compostas pelo Sistema Contínuo de Diagnósticos e Mitigação (CDM), Sistema de Conformidade de Indústria, *Feeds* de Inteligência Sobre Ameaças, *Logs* de Atividade da Rede e Sistema, Políticas de Acesso a Dados, Infraestrutura de Chave Pública Corporativa (PKI), Sistema de Gestão de Identidade (ID) e Sistema de gerenciamento de informações e eventos de segurança (SIEM) (ibidem, 2020).

Para Rose *et al* (2020), uma empresa pode implementar uma arquitetura ZTA de diversas maneiras, de acordo com os seus fluxos de trabalho, variando conforme os componentes utilizados e a principal fonte de políticas e regras para a organização, podendo variar também conforme a abordagem *Zero Trust* que se pretenda implementar, ou ainda utilizando uma solução que contemple uma ou duas abordagens, ou de forma

completa, com as três abordagens existentes, que incluem a governança aprimorada de identidade, a microsegmentação lógica e a segmentação baseada em rede.

## 3 PROCEDIMENTOS METODOLÓGICOS

Como metodologia para a produção deste artigo adotou-se a pesquisa bibliográfica, exploratória e de abordagem qualitativa.

Partindo-se da revisão da literatura sobre o tema, tão em voga atualmente, quanto ainda carente de publicações, foram consultados manuais técnicos e artigos científicos, assistidos vídeos e palestras que abordam o assunto, analisados exemplos de empresas que utilizam a arquitetura ZTA e oferecem plataformas para a sua implantação.

Segundo Marconi e Lakatos (2003), a pesquisa bibliográfica não é mera repetição do que já foi escrito sobre determinado assunto, propiciando examiná-lo sob um novo enfoque, chegando-se a considerações inovadoras.

Não se optou por um estudo de caso específico, mas por encontrar boas práticas no mercado, revelar a vantagem competitiva e os benefícios que a arquitetura ZTA promovem, já que o conceito é relativamente novo e o assunto mostra-se relevante dentro das corporações e no mundo cada vez mais conectado e ávido por informações.

A pesquisa exploratória tem como propósito desenvolver, esclarecer e até transformar conceitos e ideias, e apresenta menor rigidez no planejamento; é orientada no sentido de favorecer uma visão geral, aproximativa, acerca de determinados fatos (GIL, 1999). Malhotra (2001) complementa que, este tipo tem como características um processo de pesquisa flexível e não-estruturado, uma amostra pequena e não-representativa, a observação informal, uma análise de dados qualitativa, constatações experimentais e resultados, geralmente, seguidos por outras pesquisas futuras.

A abordagem qualitativa foi escolhida para explicar a origem, a premissa, as relações e a mudança que este paradigma traz para a questão do gerenciamento de riscos, investigando diretamente a situação, obtendo dados descritivos, enfatizando mais o processo que o produto; o interesse do pesquisador ao estudar a Arquitetura *Zero Trust* é verificar como se manifesta nas atividades, nos procedimentos e nas interações cotidianas, induzindo as consequências (observam-se os dados e se supõe).

## 4 RESULTADOS E DISCUSSÃO

A arquitetura *Zero Trust* possui uma abordagem que vai além da concepção física, mobiliza mudanças na estrutura e no desenvolvimento dos processos, alcançando um valor estratégico para as organizações. Consequentemente, seu modelo traz benefícios quando aplicado de maneira integral e abarcando tudo aquilo que compõe ativos da empresa.

Torna-se, assim, um componente crucial para a mitigação de vulnerabilidades, riscos e ameaças, pois estrutura todo o contexto dentro de uma empresa no processo de proteção, monitoramento e análise de identidades, acessos e dados. Além disso, atua no processo de melhoria contínua, corrigindo pontos fracos e aperfeiçoando pontos fortes, tendo como base o estabelecendo de métricas de níveis de criticidade dos ativos.

Dando subsídios à fundamentação teórica, nesse momento apresenta-se casos reais de boas práticas de implementação da arquitetura ZT por organizações. Far-se-á a análise das empresas **AWS**, **Google** e **Microsoft**.

A *Amazon Web Services* (AWS) possui soluções de serviços e recursos que podem ser usados para implementar uma arquitetura *Zero Trust*. Gooden (2023) destaca esses serviços:

**a.** **AWS *Identity and Access Management* (IAM):** fornece controles de autenticação e autorização para usuários, grupos e recursos, incluindo *single-sign-on* (SSO), autenticação multifator (MFA), entre outros;
**b.** **AWS *Network Access Control Lists* (ACLs):** permite que se controle o tráfego de rede entre recursos, é uma solução aplicada à microsegmentação, auxiliando a empresa a isolar e proteger dados e sistemas críticos de acessos não autorizados;
**c.** **AWS *CloudTrail*:** registra todas as solicitações de API, o que pode ser usado no controle do armazenamento *cloud*, na detecção e remediação de atividades suspeitas;
**d.** **AWS *Security Hub*:** responsável por centralizar e automatizar buscas, fornecendo uma visão geral de sua postura de segurança e ajuda a identificar vulnerabilidades.

Ele também indica uma abordagem em fases para a implementação de uma arquitetura *Zero Trust*. As principais etapas são: identificação de todos os ativos que precisam ser protegidos, incluindo dados, sistemas e aplicativos; implementação de controles de autenticação e autorização rigorosos para garantir que apenas usuários e dispositivos autorizados possam acessar recursos; segmentação de rede em micro perímetros, limitando o acesso a recursos confidenciais; implementação de controles de acesso granulares para cada recurso; e monitoramento e análise do tráfego da rede para detectar atividades suspeitas.

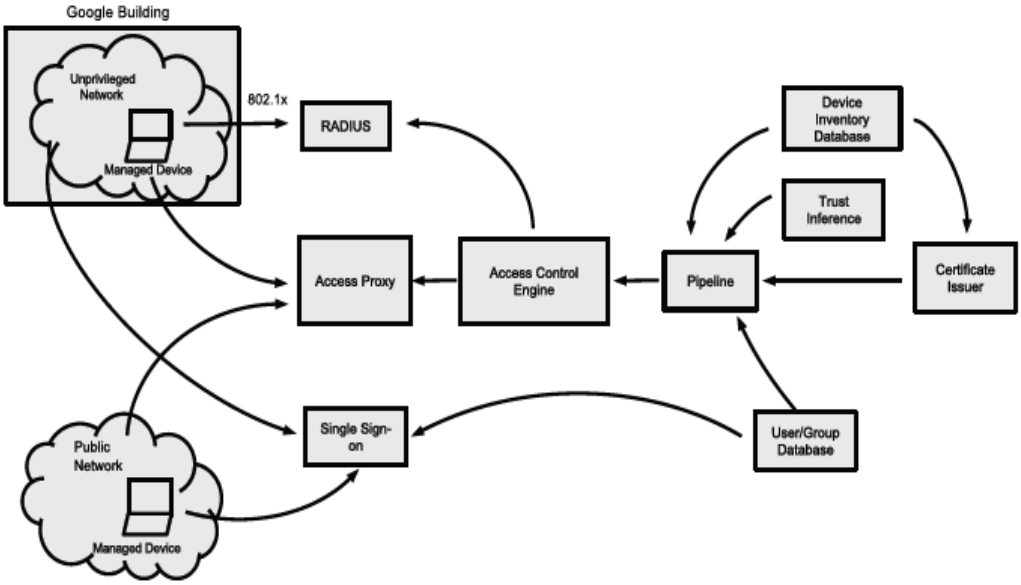
Gooden (2023) relaciona os próximos passos após a implementação e concepção de um modelo *Zero Trust*: implementar o plano adotado, implantar efetivamente a ZTA, realizar avaliações regulares de segurança e otimizar continuamente o ambiente de nuvem e os controles de segurança.

Além da abordagem e dos serviços disponíveis, a AWS orienta e fornece recursos para auxiliar as organizações a implementarem uma arquitetura ZT, bem como fornece serviços de consultoria e implantação que podem ajudar as organizações a otimizarem o processo.

A segunda empresa, a Google, foi uma das empresas pioneiras em adotar *Zero Trust* em sua infraestrutura, com o desenvolvimento da *BeyondCorp Enterprise*. Essa ferramenta destina-se à capacitação das empresas para adoção da abordagem *Zero Trust*, reunindo informações sobre um usuário, levando em conta o contexto de qual dispositivo e local este usuário está localizado e, assim, possibilitando que uma empresa tome decisões de acesso e aplique as políticas de segurança adequadas.

Em todo processo de verificação são analisadas ameaças, fluxos de conexões e acesso, e realizadas aplicações de políticas baseadas em identidade e contexto, como se observa na figura abaixo.

**Figura 2 – Componentes e fluxo de acesso da *BeyondCorp Enterprise***




**Fonte: WARD, R; BEYER, B., 2014.**

A arquitetura *Zero Trust* da Google baseia-se em três pilares principais: autenticação forte, na qual usuários e dispositivos devem ser autenticados de forma segura antes de serem autorizados a acessar recursos; controle de acesso baseado em risco, ou seja, o acesso é concedido de acordo com o usuário, dispositivo ou requisição; e na visibilidade e análise, que requer que as empresas tenham uma visão de todos os seus ativos e do tráfego para poderem detectar e responder às ameaças.

Entre as tecnologias utilizadas pela *BeyondCorp Enterprises*, alinhadas aos pilares descritos acima, estão a gestão de identidade e acesso (IAM), usada para gerenciar identidades e credenciais de usuários; a gestão de dispositivos, destinada à verificação da segurança e a conformidade dos dispositivos; a microsegmentação, usada para dividir a rede em pequenas áreas, o que dificulta para os atacantes se moverem lateralmente; a inteligência de ameaças, aplicada na identificação e resposta a ameaças em tempo real; e a autenticação forte, com a autenticação multifator (MFA), que consiste na utilização de duas ou mais formas de autenticação, como uma senha, um código de verificação ou impressão digital, a autenticação baseada em identidade, baseada em informações sobre o usuário, como seu cargo ou departamento, para determinar seu nível de acesso, e a autenticação baseada em dispositivo, para determinar se ele é seguro.

Há ainda o controle de acesso baseado em risco, que engloba uma variedade de fatores que determinam o nível de risco de uma requisição de acesso, como a identidade do usuário (usuários com acesso a informações confidenciais ou sistemas críticos são considerados de alto risco), o dispositivo do usuário (dispositivos não seguros ou não

conformes são considerados de alto risco), e tempo e local da solicitação (solicitações de acesso de fora da organização ou em horários incomuns são consideradas de alto risco).

Quanto à visibilidade e análise, utiliza uma série de ferramentas e técnicas que permitem visualizar todos os seus ativos e tráfego, incluindo o monitoramento de rede, registrando todo o tráfego, a inteligência de ameaças, identificando ameaças conhecidas e emergentes, e análise de comportamento anormal, que identifica atividades suspeitas.

A implementação da arquitetura *Zero Trust* pela *BeyondCorp Enterprises* segue um processo gradual que se divide em três etapas fundamentais. A primeira, a planificação, consiste em definir os objetivos de segurança e identificar os recursos e tecnologias necessários para implementá-los. Em seguida, a implantação, fase na qual a organização deve implantar a infraestrutura e as políticas de segurança necessárias para a arquitetura. E, por último, a operação e gerenciamento, para monitorar e gerenciar a arquitetura *Zero Trust* de forma a garantir que ela funcione como o esperado.

Ao implementar as boas práticas conforme apresentado pela *BeyondCorp*, a empresa apresenta alguns benefícios para as organizações como a redução dos riscos de ataques, a melhoria da segurança em trabalho remoto e redução de custos de segurança, eliminando a necessidade de VPNs e de outras tecnologias tradicionais.

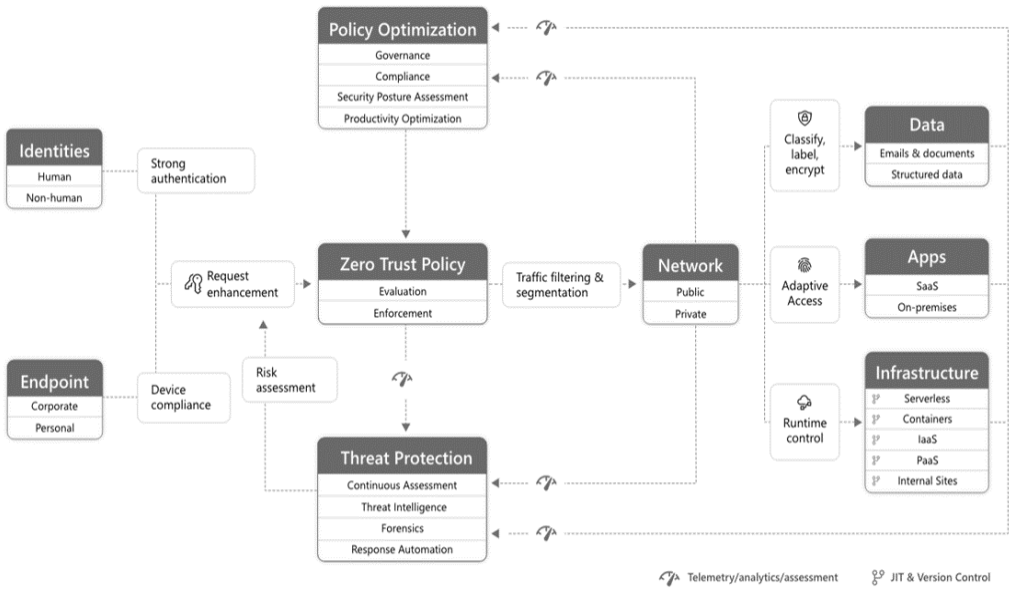
Em 2020, com a pandemia atingindo o mundo todo e o isolamento social, as organizações se viram obrigadas a adotar a estratégia *Zero Trust*, já que pela quantidade de funcionários atuando remotamente, redes privadas virtuais (VPNs) foram violadas ou sobrecarregadadas. A transformação digital tornou-se fator crucial para a sustentabilidade dos negócios (MICROSOFT, 2021).

Com a adoção do modelo *Zero Trust*, a Microsoft ajudou organizações do mundo todo a desenvolverem suas implantações de ZT para comportar as transições para o trabalho remoto e, após o controle da pandemia, com o sistema de trabalho híbrido, em paralelo a uma crescente intensidade e sofisticação dos ataques cibernéticos.

Dentro deste contexto, a Microsoft desenvolveu uma arquitetura baseada em princípios que guiam o modelo *Zero Trust*, que compreendem:

a. **Verificar explicitamente:** sempre tomar decisões de segurança usando todos os dados disponíveis, como localização, identidade, integridade do dispositivo, recurso, classificação de dados e anomalias;
b. **Usar acesso com menos privilégios:** limitar o acesso com o modelo *just-in-time* e *just-enough-access,* apenas o suficiente (JIT/JEA), e políticas adaptativas baseadas em risco.
c. **Assumir violação:** reduzir ao máximo o raio de ação de ataques utilizando microssegmentação, criptografia final de ponta a ponta, monitoramento contínuo e detecção e resposta automatizada a ameaças.

**Figura 3 – Componentes da arquitetura *Zero Trust* da Microsoft**




Fonte: MICROSOFT, 2021.

Partindo de um modelo de maturidade, a empresa define três etapas para que uma organização questione e analise ao aplicar a arquitetura *Zero Trust*, começando pelo primeiro estágio, no qual deve-se questionar se há redução de riscos em senhas com a adoção de métodos fortes como a autenticação multifator (MFA) e a adoção de *single-sign-on* (SSO) para o acesso a aplicações na nuvem (MICROSOFT, 2021). Em seguida, o processo mais significativo e que envolve questionamentos mais avançados, como se há a utilização de análises em tempo real para avaliar o comportamento dos usuários e a integridade dos dispositivos, se é possível fazer relação entre os sinais de segurança dentre os seus pilares *Zero Trust* para detectar ameaças e agir rapidamente e se é possível encontrar e corrigir de forma proativa as vulnerabilidades como configurações incorretas e *patches* ausentes para reduzir os vetores de ameaça (idem, 2021).

Por fim, com o avanço da maturidade, objetivando metas de otimização do processo, questionar se é possível aplicar dinamicamente políticas após a concessão do acesso para a proteção contra violações, se o ambiente está protegido usando a detecção automatizada de ameaças e respostas para reagir mais rapidamente às ameaças avançadas, e se há análise da produtividade e sinais de segurança para que auxiliem a direcionar o usuário na melhora de sua experiência e compreensão (ibidem, 2021).

É importante salientar que a arquitetura *Zero Trust* é um modelo dinâmico e, como já dito anteriormente, de melhoria contínua. Por esta razão, em sua implementação, a Microsoft espera que as organização obtenham como resultados: uma mudança de conceito de proteção dos pilares individuais com as políticas e controles corretos para a unificação de todos os setores, estabelecendo uma integração mais profunda, uma aplicação consistente e uma proteção holística; a inteligência contra ameaças, a resposta automatizada e a priorização dos incidentes; os processos de software e *DevOps* verificando explicitamente a integridade da segurança de aplicativos e *softwares* usando testes externos; o aumento da eficiência no gerenciamento da postura de segurança ao

simplificar a sua complexidade; e a adaptação e a expansão do *Zero Trust*, para resolver a escassez de competências em TI, a capacidade do pessoal e reforçar a postura de segurança (MICROSOFT, 2021).

## 5 CONSIDERAÇÕES FINAIS

Ao analisar os casos de boas práticas apresentados, alinhados com os princípios teóricos e conceitos da arquitetura *Zero Trust* entende-se que, ao aderir aos princípios fundamentais da ZTA, as organizações podem estabelecer uma estrutura de segurança robusta frente ao cenário de ameaças dinâmico e em evolução.

Vale ressaltar que a implementação destes princípios requer uma abordagem abrangente que combine tecnologia, processos e pessoas para alcançar uma confiança zero, além da mentalidade aberta para se construir uma postura de segurança resiliente.

Por ser um modelo que traz um novo paradigma para a segurança, para a visão e a cultura organizacional, alguns desafios podem se fazem presentes ao implementá-lo, como a dificuldade de compreensão das estratégias *Zero Trust*, sendo fundamental clareza na comunicação com as partes interessadas e sinergia com as necessidades do negócio.

O custo de implementação pode ser outro desafio, principalmente quando envolvem empresas de pequeno e médio porte que, mesmo em soluções aplicadas a uma infraestrutura mais simples e reduzida, torna-se inviável com menor orçamento.

Outros fatores que desafiam a sua implementação dizem respeito aos impedimentos ou mudanças que podem ocorrer mesmo com uma compreensão clara da estratégia, durante o processo, como a falta de fornecedores que possam entregar uma solução completa da arquitetura.

Nesse sentido, deve-se considerar que ao adotar o modelo *Zero Trust* é preciso analisar quais soluções ofertadas no mercado abrangem toda a estrutura, e caso não possua alguns componentes, que estes possam ser integrados a soluções de terceiros sem impactar negativamente desempenho e custos.

Contudo é necessário também atentar-se a essas soluções que atuam somente em partes específicas (gerenciamento da nuvem, gerenciamento de identidade, análise de transações etc.). A adição de ferramentas diversas para uma só arquitetura pode gerar uma complexidade na infraestrutura que irá dificultar o gerenciamento, o que diverge do modelo ideal.

É indispensável, portanto, que ao se pensar em soluções para implantação da arquitetura *Zero Trust*, que agreguem em um só sistema todos os ativos da empresa e o gerenciamento de toda a rede, para que deste modo haja simplicidade nos processos e otimização quanto ao gerenciamento de riscos de segurança da informação.

## REFERÊNCIAS

ARRUDA, L. G. S. de; GIOZZA, W. F.; NZE, G. D. A.; NUNES, R. R. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. In: **Revista Ibérica de Sistemas e Tecnologias de Informação**. Publicado em junho de 2023. Disponível em:

https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf

Acesso em: 07 de setembro 2023.

FORTINET. **Fortinet relata que a América Latina foi alvo de mais de 360 bilhões de tentativas de ataques cibernéticos em 2022.** Publicado em fevereiro de 2023. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent. Acesso em: 07 de outubro 2023.

GIL, A. C. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas,1999.

GOODEN, G. **AWS perspective guidance: embracing zero trust:** a strategy for secure and agile business transformation. Amazon Web Services Inc., 2023. Disponível em: https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/strategy-zero-trust-architecture/strategy-zero-trust-architecture.pdf. Acesso em: 01 de outubro 2023

GOOGLE. **BeyondCorp Enterprise.** Google, 2022. Disponível em**:** https://cloud.google.com/beyondcorp-enterprise?hl=pt-br. Acesso em: 03 de outubro 2023.

_____. **Implementing zero trust security with chrome enterprise and beyondcorp enterprise**. Disponível em: https://services.google.com/fh/files/misc/chrome_enterprise_and_beyondcorp_enterprise_technical_paper.pdf. Acesso em: 04 de outubro 2023.

MALHOTRA, N. **Pesquisa de marketing**. Porto Alegre: Bookman, 2001.

MARCONI, M.A.; LAKATOS. E.M. **Fundamentos da metodologia científica.** São Paulo: Atlas, 2003.

MICROSOFT. **Envolving zero trust:** how real-world deployments and attacks are shaping the future of zero trust strategies. Microsoft Co., 2021. Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT. Acesso em: 05 de outubro 2023.

PECK, J.; Beyer, B.; BESKE, C.; SALTONSTALL, M. Migrating to BeyondCorp: maintaining productivity while improving security. In: **Login**, vol. 42, nº 2, 2017. Disponível em https://www.usenix.org/publications/login/summer2017/peck. Acesso em: 04 de outubro 2023.

ROSE, S., BORCHERT, O., MITCHELL, S., & CONNELLY, S. Zero Trust Architecture. In: **Encyclopedia of Cryptography, Security and Privacy**. Springer Berlin Heidelberg: Stafford, 2020. Disponível em: https://doi.org/10.6028/NIST.SP.800-207. Acesso em: 14 de setembro 2023.

SEQUEIRA, J. **O paradoxo do Zero Trust: porque 60% das empresas têm dificuldades em maximizar os seus benefícios.** Publicado em 24 de fevereiro de 2023. Disponível em: https://www.computerworld.com.pt/2023/02/24/o-paradoxo-do-zero-trust-porque-60-das-empresas-tem-dificuldades-em-maximizar-os-seus-beneficios. Acesso em: 08 de outubro 2023.

TEERAKANOK, S.; UEHARA, T.; INOMATA, A. **Migrating to zero trust achitecture:** reviews and challenges. Volume 2021. Hindawi, 2021. Disponível em: https://doi.org/10.1155/2021/9947347. Acesso em: 03 de outubro 2023.

WARD, R; BEYER, B. BeyondCorp: a new approach to enterprise security. In: **Login**, vol 39, nº 6. Publicado em dezembro 2014. Disponível em:

https://www.usenix.org/system/files/login/issues/login_dec14_online.pdf. Acesso em: 07 de outubro 2023.