



COMPLEXO ESCOLAR PRIVADO  
TCHILOCA

## Internet das Coisas (IoT) e Redes de Computadores



Docente

---

Luanda, 2024

COMPLEXO ESCOLAR PRIVADO  
TCHILOCA

**Internet das Coisas (IoT) e Redes de Computadores**

**Integrantes do Grupo**

Nº	Nome	Classificação
01	Cristina Makuela	
02	Evandro Forma	
03	Joaquim Mandulo	
04	Lucineide Quitanda	
05	Marcolino Lucas	
06	Marcolino Lucas	

Curso: Gestão dos Sistemas Informáticos

Classe: 12ª

Sala: Nº 09

Grupo: Nº 02

Luanda, 2024

# Epígrafe

“O Conhecimento é a arma mais poderosa que um Homem pode ter”  
(Jeth Weber)

# Resumo

O presente artigo explora a relação entre a Internet das Coisas (IoT) e as redes de computadores, destacando os conceitos, tecnologias e aplicações práticas dessa integração. São abordados os protocolos, infraestrutura de redes, segurança, privacidade e os impactos no cotidiano e em diferentes setores econômicos. A pesquisa também apresenta os desafios futuros, as tendências de mercado e os avanços tecnológicos que possibilitam o crescimento do IoT.

**Palavras-chave:** Internet das Coisas, Redes de Computadores, IoT, Segurança, Aplicações Tecnológicas.

# Objetivos

## Objetivo Geral

Analisar a integração entre a Internet das Coisas (IoT) e as redes de computadores, destacando os aspectos técnicos, aplicações práticas e desafios associados, com foco em suas contribuições para a transformação digital em diversos setores da sociedade.

## Objetivos Específicos

1. Investigar os fundamentos teóricos da IoT e seu relacionamento com as redes de computadores.
2. Identificar as principais tecnologias, protocolos e arquiteturas que viabilizam a comunicação em ambientes IoT.
3. Avaliar os desafios relacionados à segurança e à privacidade no uso de dispositivos IoT interconectados.
4. Explorar aplicações práticas da IoT em setores como saúde, agricultura, indústria e cidades inteligentes.
5. Apontar as tendências futuras e as implicações sociais, econômicas e ambientais da expansão da IoT.

# Índice

Epígrafe .....	3
Resumo .....	4
Objetivos .....	5
Objetivo Geral .....	5
Objetivos Específicos .....	5
Introdução .....	6
Fundamentação Teórica .....	7
Exemplos de Aplicações Práticas .....	7
Redes de Computadores .....	8
Conceito Básico e Componentes Principais .....	8
Função das Redes no Suporte à IoT .....	8
Segurança e Privacidade .....	9
Desafios de Segurança em IoT .....	9
Vulnerabilidades Específicas de Dispositivos IoT .....	9
Exemplos de Ataques em Dispositivos Conectados .....	9
Proteção de Dados .....	10
Criptografia e Autenticação em IoT .....	10
Boas Práticas para Garantir Privacidade .....	10
Futuro da IoT e Redes de Computadores .....	11
Tendências e Inovações .....	11
Expansão do 5G e Impacto no IoT .....	11
Uso de Inteligência Artificial na IoT .....	11
Sustentabilidade e IoT .....	11
Soluções para Reduzir o Impacto Ambiental .....	11
Energias Renováveis e IoT .....	12
Conclusão .....	13
Referências Bibliográficas .....	14
Futuro da IoT e Redes de Computadores .....	14



# Introdução

A Internet das Coisas (IoT) representa uma revolução tecnológica baseada na interconexão de dispositivos por meio das redes de computadores. Com o avanço das tecnologias de comunicação, tornou-se possível conectar objetos do cotidiano a sistemas computacionais, promovendo automação e inteligência em diversas áreas. Este artigo visa discutir os fundamentos dessa convergência, bem como analisar suas aplicações, desafios e perspectivas.



# Fundamentação Teórica

A Internet das Coisas (IoT) refere-se à interconexão de dispositivos físicos que possuem sensores, software e outras tecnologias capazes de coletar e trocar dados pela internet. A IoT abrange uma vasta gama de dispositivos, desde eletrodomésticos simples até complexos sistemas industriais, todos conectados e comunicando-se entre si para melhorar a eficiência e a funcionalidade. O termo "Internet das Coisas" foi cunhado em 1999 pelo cientista da computação Kevin Ashton enquanto trabalhava na Procter & Gamble. Ashton propôs a ideia de conectar objetos físicos à internet usando a tecnologia de rádio frequência para melhorar a gestão de inventário e a eficiência operacional.

## Exemplos de Aplicações Práticas

### 1. Casas Inteligentes:

- **Termostatos Inteligentes:** Dispositivos como o Nest Learning Thermostat ajustam automaticamente a temperatura com base nas preferências dos moradores e na presença, resultando em economia de energia.
- **Assistentes Virtuais:** Dispositivos como Amazon Echo e Google Home permitem controlar luzes, eletrodomésticos e sistemas de segurança através de comandos de voz.

### 2. Saúde:

- **Dispositivos Vestíveis:** Relógios inteligentes e pulseiras fitness monitoram a frequência cardíaca, passos e sono, enviando dados para aplicativos que ajudam a melhorar a saúde e a forma física.
- **Monitoramento Remoto de Pacientes:** Dispositivos médicos conectados permitem que médicos monitorem condições de saúde dos pacientes em tempo real, possibilitando intervenções mais rápidas.

### 3. Indústria:

- **Manutenção Preditiva:** Sensores em máquinas industriais coletam dados sobre seu desempenho, permitindo a detecção de falhas antes que elas ocorram, reduzindo o tempo de inatividade e os custos de reparo.
- **Automatização da Produção:** Sistemas de IoT coordenam e controlam processos de fabricação, ajustando automaticamente as operações para maximizar a eficiência.

### 4. Agricultura:

- **Sensores de Solo:** Monitoram a umidade e os nutrientes do solo, ajudando os agricultores a otimizar a irrigação e a aplicação de fertilizantes, aumentando a produtividade e economizando recursos.
- **Drones Agrícolas:** Utilizados para monitorar campos, identificar pragas e doenças, e aplicar tratamentos de precisão, melhorando o rendimento das colheitas.

# Redes de Computadores

## Conceito Básico e Componentes Principais

Redes de computadores são sistemas interconectados que permitem a troca de dados e recursos entre dispositivos. Esses sistemas variam em escala desde redes locais pequenas (LANs) até grandes redes de longa distância (WANs), como a internet. Os componentes principais de uma rede de computadores incluem:

### 1. Dispositivos de Rede:

- **Roteadores:** Direcionam o tráfego de dados entre diferentes redes.
- **Switches:** Conectam dispositivos dentro de uma mesma rede e gerenciam a distribuição de dados para os dispositivos corretos.
- **Pontos de Acesso (APs):** Permitem conexões sem fio dentro de uma rede.

### 2. Meios de Transmissão:

- **Cabos de Par Trançado:** Utilizados em redes Ethernet, são compostos por pares de fios trançados que minimizam interferências eletromagnéticas.
- **Fibra Óptica:** Utiliza filamentos de vidro ou plástico para transmitir dados como pulsos de luz, oferecendo alta velocidade e baixa latência.
- **Sinais de Rádio:** Utilizados em redes sem fio (Wi-Fi), permitem a comunicação sem a necessidade de cabos físicos.

### 3. Protocolos de Comunicação:

- **TCP/IP (Transmission Control Protocol/Internet Protocol):** Conjunto de protocolos que formam a base da comunicação na internet.
- **HTTP/HTTPS (HyperText Transfer Protocol):** Utilizados para a transferência de páginas web.

## Função das Redes no Suporte à IoT

As redes de computadores desempenham um papel crucial no suporte à IoT, fornecendo a infraestrutura necessária para a conectividade e a troca de dados entre dispositivos. Elas permitem que os dispositivos IoT se comuniquem de forma eficaz, garantindo que os dados coletados sejam transmitidos de forma segura e eficiente para sistemas de processamento e análise.

### 1. Conectividade:

- Redes de computadores permitem que dispositivos IoT se conectem à internet e entre si, facilitando a transmissão de dados em tempo real.

### 2. Segurança de Dados:

- As redes implementam medidas de segurança, como criptografia e firewalls, para proteger os dados transmitidos e garantir a privacidade das comunicações.

### 3. Eficiência Operacional:

- A integração de dispositivos IoT em redes de computadores permite a automação de processos, melhorando a eficiência e reduzindo custos operacionais.

### 4. Escalabilidade:

- Redes de computadores permitem a fácil adição de novos dispositivos IoT, suportando o crescimento contínuo e a expansão de sistemas conectados.

As redes de computadores são, portanto, a espinha dorsal que sustenta a IoT, possibilitando uma interconexão eficiente e segura de dispositivos que transformam diversos setores da economia e da vida cotidiana.

## Segurança e Privacidade

### Desafios de Segurança em IoT

#### Vulnerabilidades Específicas de Dispositivos IoT

Dispositivos IoT apresentam várias vulnerabilidades que podem ser exploradas por cibercriminosos devido a suas características únicas e à falta de padrões de segurança robustos. Algumas dessas vulnerabilidades incluem:

1. **Capacidades Limitadas de Processamento e Armazenamento:** Muitos dispositivos IoT são projetados para serem compactos e eficientes, o que frequentemente resulta em capacidades limitadas de processamento e armazenamento. Isso pode impedir a implementação de medidas de segurança avançadas, como criptografia robusta e detecção de intrusões.
2. **Atualizações de Firmware e Software Inadequadas:** A falta de atualizações regulares de firmware e software pode deixar dispositivos IoT vulneráveis a ataques. Muitos fabricantes não oferecem suporte contínuo, resultando em dispositivos desatualizados e suscetíveis a explorações conhecidas.
3. **Autenticação Fraca:** Senhas padrão fracas ou fáceis de adivinhar são uma vulnerabilidade comum em dispositivos IoT. Usuários muitas vezes não alteram as senhas padrão, facilitando o acesso não autorizado.
4. **Falta de Criptografia:** Muitos dispositivos IoT transmitem dados sem criptografia, permitindo que atacantes interceptem e leiam as informações transmitidas.
5. **Exposição à Rede:** Dispositivos IoT frequentemente estão conectados à internet ou a redes internas sem as devidas proteções, tornando-os alvos fáceis para invasões.

#### Exemplos de Ataques em Dispositivos Conectados

1. **Botnets de IoT:** Um dos ataques mais conhecidos é a criação de botnets a partir de dispositivos IoT comprometidos. Exemplos incluem o botnet Mirai, que utilizou câmeras de segurança e roteadores infectados para realizar ataques de negação de serviço distribuído (DDoS) massivos.
2. **Roubo de Dados:** Em 2017, um brinquedo conectado chamado CloudPets foi alvo de um ataque que resultou no vazamento de 2,2 milhões de mensagens gravadas por crianças e seus pais, devido à falta de segurança na comunicação entre o dispositivo e a nuvem.
3. **Sequestro de Dispositivos:** Dispositivos IoT como câmeras de segurança e termostatos têm sido alvos de ataques onde os invasores assumem o controle do dispositivo, espionando os usuários ou exigindo resgates para devolver o controle.

## Proteção de Dados

### Criptografia e Autenticação em IoT

Para mitigar as vulnerabilidades e proteger os dados em dispositivos IoT, a implementação de criptografia e autenticação é essencial. Aqui estão algumas das práticas e tecnologias utilizadas:

#### 1. Criptografia de Dados:

- **Criptografia Simétrica:** Utiliza a mesma chave para encriptar e descriptar os dados. É eficiente, mas o gerenciamento seguro das chaves pode ser um desafio.
- **Criptografia Assimétrica:** Utiliza um par de chaves (pública e privada) para encriptar e descriptar dados. Apesar de ser mais lenta, oferece maior segurança na transmissão de chaves.

#### 2. Autenticação Forte:

- **Autenticação Multifatorial (MFA):** Requer múltiplas formas de verificação, como senha, token e biometria, para acessar o dispositivo.
- **Certificados Digitais:** Utilizados para verificar a identidade de dispositivos e garantir que apenas dispositivos autenticados possam se comunicar na rede.

3. **Protocolo TLS (Transport Layer Security):** Protocolo amplamente utilizado para garantir que os dados transmitidos entre dispositivos IoT e servidores sejam criptografados e protegidos contra interceptações.

### Boas Práticas para Garantir Privacidade

1. **Alteração de Senhas Padrão:** Os usuários devem alterar senhas padrão para combinações fortes e únicas para cada dispositivo.
2. **Atualizações Regulares de Firmware e Software:** Fabricantes devem fornecer atualizações regulares para corrigir vulnerabilidades de segurança, e os usuários devem garantir que seus dispositivos estejam sempre atualizados.
3. **Isolamento de Redes IoT:** Configurar uma rede separada para dispositivos IoT pode limitar o impacto de um ataque, impedindo que dispositivos comprometidos afetem outros sistemas críticos.
4. **Monitoramento Contínuo:** Implementação de sistemas de monitoramento para detectar comportamentos anômalos nos dispositivos IoT, possibilitando respostas rápidas a possíveis ataques.
5. **Educação e Conscientização do Usuário:** Ensinar os usuários sobre as melhores práticas de segurança e a importância da proteção de seus dispositivos IoT pode reduzir significativamente o risco de vulnerabilidades exploradas.

A segurança e a privacidade são fundamentais para o sucesso da IoT, garantindo que os benefícios dessa tecnologia não sejam superados pelos riscos associados a falhas de segurança. Implementar medidas robustas de criptografia, autenticação e boas práticas pode ajudar a mitigar os desafios e proteger dados sensíveis.

# **Futuro da IoT e Redes de Computadores**

## **Tendências e Inovações**

### **Expansão do 5G e Impacto no IoT**

A expansão das redes 5G está transformando o panorama da Internet das Coisas (IoT). Com velocidades de download que podem alcançar até 10 Gbps e latências menores que 1 milissegundo, o 5G possibilita uma comunicação quase instantânea entre dispositivos. Esta tecnologia é particularmente vital para aplicações em tempo real, como veículos autônomos, que dependem de respostas rápidas para garantir a segurança e a eficiência.

Além disso, o 5G suporta uma densidade muito maior de dispositivos conectados por área, permitindo que um número significativo de dispositivos IoT opere simultaneamente sem degradação da qualidade do serviço. Isso é essencial para o crescimento de cidades inteligentes, onde milhares de sensores e dispositivos coletam e transmitem dados continuamente. Com a expansão do 5G, espera-se que a IoT se torne ainda mais integrada ao nosso cotidiano, facilitando avanços em áreas como saúde, logística, manufatura e agricultura.

### **Uso de Inteligência Artificial na IoT**

A integração da inteligência artificial (IA) com a IoT está moldando o futuro da tecnologia. A IA pode processar e analisar grandes volumes de dados coletados por dispositivos IoT em tempo real, extraindo insights valiosos e permitindo decisões automatizadas. Por exemplo, em cidades inteligentes, algoritmos de IA podem analisar dados de tráfego para otimizar os semáforos, reduzindo congestionamentos e melhorando a eficiência do transporte urbano.

Na área da saúde, a IA pode monitorar continuamente os sinais vitais dos pacientes por meio de dispositivos IoT, detectando anomalias precocemente e alertando os profissionais de saúde para intervenções imediatas. Na indústria, a manutenção preditiva usa IA para prever falhas em equipamentos com base nos dados coletados por sensores, minimizando o tempo de inatividade e os custos de reparo.

A combinação de IoT e IA não só aumenta a eficiência e a automação, mas também abre novas possibilidades para inovações que antes eram inimagináveis.

## **Sustentabilidade e IoT**

### **Soluções para Reduzir o Impacto Ambiental**

A IoT pode desempenhar um papel crucial na promoção da sustentabilidade e na redução do impacto ambiental. Sensores IoT podem monitorar e otimizar o uso de recursos naturais, como água e energia, reduzindo o desperdício e melhorando a eficiência. Por exemplo, sistemas de irrigação inteligentes ajustam automaticamente a quantidade de água com base na umidade do solo e nas condições climáticas, economizando água e melhorando o rendimento das culturas.

Além disso, dispositivos IoT podem monitorar a qualidade do ar e detectar poluentes, ajudando as cidades a implementar estratégias eficazes para reduzir a poluição. Na gestão de resíduos, sensores em lixeiras inteligentes podem otimizar as rotas de coleta de lixo, reduzindo o consumo de combustível e as emissões de gases de efeito estufa.

## **Energias Renováveis e IoT**

A IoT também está impulsionando o uso de energias renováveis. Painéis solares e turbinas eólicas equipados com sensores IoT podem monitorar continuamente sua eficiência e desempenho, ajustando automaticamente os ângulos e operações para maximizar a produção de energia. Além disso, redes elétricas inteligentes (smart grids) utilizam dispositivos IoT para equilibrar a oferta e a demanda de energia, integrando fontes de energia renovável de forma mais eficaz e reduzindo a dependência de combustíveis fósseis.

Os dispositivos IoT também são fundamentais para a gestão de baterias e sistemas de armazenamento de energia, garantindo que a energia renovável seja armazenada e utilizada de maneira eficiente. Isso não só melhora a sustentabilidade, mas também contribui para uma maior resiliência energética.

Com o avanço contínuo da tecnologia, a IoT tem o potencial de promover práticas mais sustentáveis e reduzir significativamente o impacto ambiental, ao mesmo tempo em que apoia a transição para uma economia verde.

## Conclusão

A Internet das Coisas (IoT), apoiada pelas redes de computadores, está transformando a forma como interagimos com a tecnologia, permitindo uma comunicação eficiente entre dispositivos e promovendo automação e inteligência em diversos setores. Sua aplicação prática em áreas como saúde, agricultura, indústria e cidades inteligentes demonstra como essa integração tem o potencial de melhorar a eficiência, reduzir custos e criar soluções sustentáveis. No entanto, para que esses benefícios sejam plenamente realizados, é essencial superar desafios relacionados à segurança, privacidade e interoperabilidade dos dispositivos.

Além disso, o futuro da IoT é promissor, com a integração de tecnologias emergentes, como o 5G e a inteligência artificial, possibilitando novas aplicações e avanços significativos. A IoT também desempenha um papel crucial na sustentabilidade, promovendo práticas ecológicas e otimizando recursos. Contudo, o sucesso dessa transformação digital requer esforços contínuos em pesquisa, regulamentação e conscientização para garantir que as inovações sejam acessíveis, seguras e benéficas para a sociedade como um todo.

## Referências Bibliográficas

**Della Rovere, L., & Florian, F.** (2022). "Estudo sobre Segurança e Privacidade na Internet das Coisas (IoT)." *RECIMA21 - Revista Científica Multidisciplinar*. ISSN 2675-6218.

1. **ENISA** (2015). "Security and Resilience of Smart Home Environments: Good Practices and Recommendations." *European Union Agency for Cybersecurity*.
2. **ENISA** (2017). "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures." *European Union Agency for Cybersecurity*.
3. **ENISA** (2018). "Good Practices for Security of Internet of Things in the context of Smart Manufacturing." *European Union Agency for Cybersecurity*.
4. **ENISA** (2018). "Towards secure convergence of Cloud and IoT." *European Union Agency for Cybersecurity*.
5. **ENISA** (2019). "IoT Security Standards Gap Analysis Mapping of existing standards against requirements on security and privacy in the area of IoT." *European Union Agency for Cybersecurity*.
6. **ENISA** (2019). "Industry 4.0 Cybersecurity: Challenges e Recommendations." *European Union Agency for Cybersecurity*.
7. **Araujo, A. R.** (2023). "Métodos e Técnicas de Segurança para Dispositivos IoT: Uma Revisão Sistemática da Literatura." *Instituto Federal de Educação, Ciência e Tecnologia da Paraíba*.
8. **Manoel da Silva, I.** (2024). "Privacidade e Segurança na Era da IoT em Residências: Possibilidades e Desafios." *FATEC Americana*.
9. **Barros, G. F.** (2021). "Internet das Coisas: a busca do conceito e as perspectivas futuras sobre sua aplicabilidade." .

## Futuro da IoT e Redes de Computadores

11. **Santos, B. P., Silva, L. A. M., Celes, C. S. F. S., Neto, J. B. B., Peres, B. S., Vieira, M. A. M., Vieira, L. F. M., & Goussevskaia, O. N.** (2023). "Internet das Coisas: da Teoria à Prática." *Universidade Federal de Minas Gerais*.
12. **Kurose, J. F., & Ross, K. W.** (2005). "Computer Networking: A Top-Down Approach Featuring the Internet, 3rd Edition." *Addison-Wesley*.
13. **Peterson, L., & Davie, B.** (2003). "Computer Networks: A Systems Approach, 3rd Edition." *Morgan Kaufmann*.
14. **Donahoo, M. J., & Calvert, K. L.** (2000). "TCP/IP Sockets in C: Practical Guide for Programmers." *Morgan Kaufmann*.
15. **Stevens, W. R.** (1998). "Unix Network Programming: Networking APIs: Sockets and XTI (Volume 1), 2nd Edition." *Prentice Hall PTR*.

<https://copilot.microsoft.com/chats/X4VsRwMxDY8rK48YkTGaC>. (2024/11/19)