

Inglês instrumental

Class 7

Gilmar Gomes do Nascimento

Instituto Federal do Amazonas
Campus Boca do Acre

18 de fevereiro de 2026





What is the IoT?

The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data.

IoT devices—also known as “smart objects”—can range from simple “smart home” devices like smart thermostats, to wearables like smartwatches and RFID-enabled clothing, to complex industrial machinery and transportation systems. Technologists are even envisioning entire “smart cities” predicated on IoT technologies.



Smart devices

IoT enables these smart devices to communicate with each other and with other internet-enabled devices. Like smartphones and gateways, creating a vast network of interconnected devices that can exchange data and perform various tasks autonomously. This can include:

- monitoring environmental conditions in farms
- managing traffic patterns with smart cars and other smart automotive devices
- controlling machines and processes in factories
- tracking inventory and shipments in warehouses



Ubiquity I

The potential applications of IoT are vast and varied, and its impact is already being felt across a wide range of industries, including manufacturing, transportation, healthcare, and agriculture. As the number of internet-connected devices continues to grow, IoT is likely to play an increasingly important role in shaping our world. Transforming the way that we live, work, and interact with each other.



Ubiquity II

In an enterprise context, IoT devices are used to monitor a wide range of parameters such as temperature, humidity, air quality, energy consumption, and machine performance. This data can be analyzed in real time to identify patterns, trends, and anomalies that can help businesses optimize their operations and improve their bottom line.



Why is IoT important?

IoT is important for business for several reasons. Here are the core benefits of IoT:

- Improved efficiency
- Data-driven decision-making
- Cost-savings
- Enhanced customer experience



Improved efficiency

By using IoT devices to automate and optimize processes, businesses can improve efficiency and productivity. For example, IoT sensors can be used to monitor equipment performance and detect or even resolve potential issues before they cause downtime, reducing maintenance costs and improving uptime.



Data-driven decision-making

IoT devices generate vast amounts of data that can be used to make better-informed business decisions and new business models. By analyzing this data, businesses can gain insights into customer behavior, market trends, and operational performance, allowing them to make more informed decisions about strategy, product development, and resource allocation.



Cost-savings

By reducing manual processes and automating repetitive tasks, IoT can help businesses reduce costs and improve profitability. For example, IoT devices can be used to monitor energy usage and optimize consumption, reducing energy costs and improving sustainability.



Enhanced customer experience

By using IoT technology to gather data about customer behavior, businesses can create more personalized and engaging experiences for their customers. For example, retailers can use IoT sensors to track customer movements in stores and deliver personalized offers based on their behavior.



The technologies that make IoT possible



Sensors and actuators: Sensors are devices that can detect changes in the environment, such as temperature, humidity, light, motion, or pressure. Actuators are devices that can cause physical changes in the environment, such as opening or closing a valve or turning on a motor. These devices are at the heart of IoT, as they allow machines and devices to interact with the physical world. Automation is possible when sensors and actuators work to resolve issues without human intervention.



Connectivity technologies: To transmit IoT data from sensors and actuators to the cloud, IoT devices need to be connected to the internet. There are several connectivity technologies that are used in IoT, including wifi, Bluetooth, cellular, Zigbee, and LoRaWAN.



Cloud computing: The cloud is where the vast amounts of data that is generated by IoT devices are stored, processed, and analyzed. Cloud computing platforms provide the infrastructure and tools that are needed to store and analyze this data, as well as to build and deploy IoT applications.



Big data analytics: To make sense of the vast amounts of data generated by IoT devices, businesses need to use advanced analytics tools to extract insights and identify patterns. These tools can include machine learning algorithms, data visualization tools and predictive analytics models.



Security and privacy technologies: As IoT deployments become more widespread, IoT security and privacy become increasingly important. Technologies such as encryption, access controls and intrusion detection systems are used to protect IoT devices and the data they generate from cyberthreats.



Examples of IoT applications

- Healthcare
- Manufacturing
- Retail
- Agriculture
- Transportation



Healthcare

In the healthcare industry, IoT devices can be used to monitor patients remotely and collect real-time data on their vital signs, such as heart rate, blood pressure and oxygen saturation. This sensor data can be analyzed to detect patterns and identify potential health issues before they become more serious. IoT devices can also be used to track medical equipment, manage inventory and monitor medication compliance.



Manufacturing

Industrial IoT devices can be used in manufacturing to monitor machine performance, detect equipment failures and optimize production processes. For example, sensors can be used to monitor the temperature and humidity in a manufacturing facility, ensuring that conditions are optimal for the production of sensitive products. IoT devices can also be used to track inventory, manage supply chains and monitor the quality of finished products. Industrial IoT is such an expansive new technology space, that it is sometimes referred to by its own abbreviation: IIoT (Industrial IoT).



In the retail industry, IoT devices can be used to track customer behavior, monitor inventory levels and optimize store layouts. For example, sensors can be used to track foot traffic in a store and analyze customer behavior, allowing retailers to optimize product placement and improve the customer experience. IoT devices can also be used to monitor supply chains, track shipments and manage inventory levels.



Agriculture

IoT devices can be used in agriculture to monitor soil conditions, weather patterns and crop growth. For example, sensors can be used to measure the moisture content of soil, ensuring that crops are irrigated at the optimal time. IoT devices can also be used to monitor livestock health, track equipment and manage supply chains. Low-power or solar-powered devices can often be used with minimal oversight in remote locations.



Transportation

In the transportation industry, IoT devices can be used to monitor vehicle performance, optimize routes, and track shipments. For example, sensors can be used to monitor the fuel efficiency of connected cars, reducing fuel costs and improving sustainability. IoT devices can also be used to monitor the condition of cargo, ensuring that it arrives at its destination in optimal condition.



Risks and challenges in IoT I

IoT offers many benefits, but it also poses several risks and challenges. Here are some of the most significant ones:

Security and privacy risks: As IoT devices become more widespread, security and privacy become increasingly important. Many IoT devices are vulnerable to hackers and other cyberthreats, which can compromise the security and privacy of sensitive data. IoT devices can also collect vast amounts of personal data, raising concerns about privacy and data protection.



Risks and challenges in IoT II

Interoperability issues: IoT devices from different manufacturers often use different standards and protocols, making it difficult for them to perform what's called "machine to machine" communication. This can lead to interoperability issues and create silos of data that are difficult to integrate and analyze.



Risks and challenges in IoT III

Data overload: IoT devices generate vast amounts of data, which can overwhelm businesses that are not prepared to handle it. Analyzing this data and extracting meaningful insights can be a significant challenge, especially for businesses that lack the necessary analytics tools and expertise.



Risks and challenges in IoT IV

Cost and complexity: Implementing an IoT system can be costly and complex, requiring significant investments in hardware, software, and infrastructure. Managing and maintaining an IoT system can also be challenging, requiring specialized skills and expertise.



Risks and challenges in IoT V

Regulatory and legal challenges: As IoT devices become more widespread, regulatory, and legal challenges are emerging. Businesses need to comply with various data protection, privacy and cybersecurity regulations, which can vary from country to country.



How should businesses approach IoT? I

Managing IoT devices can be a complex and challenging task, but there are several best practices that businesses can follow to ensure that their IoT devices are secure, reliable, and optimized for performance. Here are some tips for managing IoT devices:



How should businesses approach IoT? II

Plan your IoT strategy: Before deploying any IoT devices, businesses should have a clear understanding of their objectives, use cases and desired outcomes. This can help them choose the right devices, IoT platforms and technologies, and ensure that their IoT strategy is aligned with their business goals.



How should businesses approach IoT? III

Choose secure IoT products: Security is a critical consideration for IoT solutions, as they can be vulnerable to cyberattacks. Businesses should choose devices that are designed with security in mind and implement appropriate security systems, such as encryption, authentication, and access controls.



How should businesses approach IoT? IV

Monitor and maintain devices: IoT devices need to be monitored and maintained regularly to ensure that they are performing optimally and are not vulnerable to security threats. This can involve monitoring device health and performance, updating firmware and software and conducting regular security audits and predictive maintenance.



How should businesses approach IoT? V

Manage data effectively: IoT devices generate vast amounts of real-world data, which can be challenging to manage and analyze. Businesses should have a clear data management strategy in place, including data storage, analysis, and visualization. To ensure that they can extract meaningful insights from the data that is generated by their IoT devices.



How should businesses approach IoT? VI

Build an ecosystem: IoT devices are often part of a larger ecosystem that includes other devices, platforms, and technologies. Businesses should have a clear understanding of this ecosystem and ensure that their IoT devices can integrate effectively with other systems and technologies.



The future of IoT I

The future of IoT is promising, with many exciting developments for businesses on the horizon. Here are some of the trends and predictions for the future of IoT:



The future of IoT II

The number of IoT devices is expected to continue to grow rapidly, with estimates suggesting that there will be tens of billion IoT devices in use over the next few years. This growth will be driven by increased adoption across industries, as well as the development of new use cases and applications.



The future of IoT III

Edge computing is becoming increasingly important for IoT, as it allows data to be processed and analyzed closer to the source of the data, rather than in a centralized data center. This can improve response times, reduce latency and reduce the amount of data that needs to be transferred over IoT networks.



The future of IoT IV

Artificial intelligence and machine learning: are becoming increasingly important for IoT, as they can be used to analyze vast amounts of data that is generated by IoT devices and extract meaningful insights. This can help businesses make more informed decisions and optimize their operations.



The future of IoT V

Blockchain technology is being explored as a way to improve security and privacy in the IoT. Blockchain can be used to create secure, decentralized networks for IoT devices, which can minimize data security vulnerabilities.



The future of IoT VI

Sustainability is becoming an increasingly important consideration for IoT, as businesses look for ways to reduce their environmental impact. IoT can be used to optimize energy usage, reduce waste and improve sustainability across a range of industries.



The future of IoT VII

The future of IoT is exciting, with many new developments and innovations on the horizon, with providers of devices offering attractive pricing, as the cost of IoT device production declines. As the number of IoT devices continues to grow, businesses need to be prepared to adapt to new technologies and embrace new use cases and applications. Those that are able to do so will be positioned to reap the benefits of this transformative technology.



Referências Bibliográficas I

-  IBM. **What is Internet of Things.** Disponível em:
<https://www.ibm.com/think/topics/internet-of-things>. Acesso em: 18 fev. 2025.

