
# Problemas de Segurança na Internet das Coisas

Mestrado em Cibersegurança e Informática Forense

Arlindo Jorge de Jesus Ribeiro

Leiria, novembro de 2020


# Problemas de Segurança na Internet das Coisas

Mestrado em Cibersegurança e Informática Forense

Arlindo Jorge de Jesus Ribeiro

Dissertação realizada sob a orientação do Professor Doutor António Pereira e do Professor Doutor Luís Frazão

Leiria, novembro de 2020

# Originalidade e Direitos de Autor

A presente dissertação é original, elaborada unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

# Dedicatória

Ao meu filho Jorge Ribeiro, pela difícil provação pela qual teve de passar, no período mais difícil da sua vida e, pela qual teve de “lutar” para conseguir sobreviver. À minha esposa Irene Ribeiro, por todo o apoio prestado no momento mais difícil pelo qual passamos, nestes anos de casados.

Foi de facto um período muitíssimo difícil de conseguir conciliar, em termos de aulas e, de apoio à família, para conseguir concluir as aulas e este trabalho, na fase mais difícil da minha vida.

# Agradecimentos

Na conclusão deste percurso, agradeço a todos os que de forma direta ou indireta, contribuíram para o seu desenvolvimento e conclusão do trabalho.

Os meus sinceros agradecimentos, pelo apoio prestado ao longo de todo deste processo da elaboração da dissertação, ao Professor António Pereira e ao Professor Luís Frazão, pela exigência e rigor dos mesmos, permitindo elevar a qualidade do trabalho final.

O meu agradecimento, vai também para todos os professores do mestrado MCIF, que me permitiram enriquecer o meu percurso académico, bem o meu percurso profissional, em termos de conhecimentos na área da cibersegurança.

Um agradecimento à Escola Superior de Tecnologia e Gestão de Leiria e a todos os envolvidos na elaboração deste mestrado, pela forma como o mesmo foi concebido, permitindo conciliar a teoria com a prática, pelos meios e condições colocados, à disposição dos alunos.

Um agradecimento especial, também à organização onde estou a trabalhar, que pela sua dimensão a nível nacional e internacional, me proporcionou a possibilidade de interagir com uma multiplicidade de projetos nacionais e internacionais ao nível do IoT, IIoT, Smart Cities, Smart Buildings e, projetos em cibersegurança, permitindo a aquisição de um conhecimento exponencial dentro desta área, enriquecendo a dissertação, com este know-how.

Embora lhe tenha dedicado esta dissertação ao meu filho, não poderia deixar de lhe dar um especial agradecimento, pelo lutador que é, desejando-lhe muita saúde. Um especial obrigado à minha esposa, por todo apoio nos momentos mais difíceis deste percurso.

Agradeço também a todos os amigos e familiares, que forma direta ou indireta prestaram apoio de alguma forma, na persecução deste objetivo.

# Resumo

A massificação dos dispositivos, associados à Internet das Coisas (que teve a sua origem do termo em inglês *Internet of things*, ou *IoT)*, levou a que assistíssemos a uma explosão neste segmento. Esta expansão, tem associado um crescimento económico, pelos diferentes setores a que está associado (Indústria, Transportes, Telecomunicações, etc.), na perspetiva da analítica do que é possível obter com estes dispositivos e, o que é possível fazer com esses dados, mas por outro lado, tem também subjacente uma componente de insegurança de elevada magnitude.

A Internet das Coisas, engloba "coisas", como sensores, atuadores e outros dispositivos, que quando são concebidos, os seus "criadores", não tem em consideração as melhores práticas ao nível da segurança, no sentido de garantirem que estes dispositivos, são parte integrante da solução e não parte do problema.

A presente dissertação tem como objetivo o desenvolvimento de um modelo, que tem em consideração a dificuldade atual com que as organizações se deparam, ao ponto de não entenderem em que fase de evolução se encontram, na jornada da Industria 4.0. Este modelo tem o foco na Indústria 4.0, pela relevância que esta representa ao nível da economia dos países, bem como o "peso" que esta tem, na vertente da Internet das Coisas.

Para a elaboração deste modelo, foram feitas várias análises, aos modelos de arquitetura mais relevantes, que endereçam este setor, bem como a avaliação de diferentes modelos de maturidade. Este modelo vai permitir dotar as organizações no setor da indústria, com uma matriz de avaliação, que lhes vai anuir a adoção do modelo e integração dos seus resultados, na estratégia da organização.

O modelo agrega na sua avaliação, três dos principais atores nesta mudança de digitalização do chão de fábrica, permitindo aos CxO (Administradores, executivos, diretores) atuarem com celeridade na realização da avaliação e, com isso tomarem as devidas medidas, emanadas pelo modelo.

O resultado do modelo/simulador permitirá que, as organizações se possam tornar mais ágeis na resposta direta à concorrência, consigam ser céleres na tomada de decisão em termos do *time-to-market*, permitam focar a produção orientada ao cliente e também ajustar a produção, orientada à procura. Este modelo, tem em consideração as ameaças e vulnerabilidades que decorrem do fenómeno IoT aplicado à indústria pelo que, o modelo potencia a colaboração das tecnologias de operação com as tecnologias de informação, garantindo a implementação de uma solução, assente nas melhores práticas de segurança. Estas sinergias internas, vem permitir que a organização tenha economias de escala, resultando numa redução de custos de exploração e, num maior aumento da eficácia e da eficiência.

**Palavras-chave:** Internet das Coisas, Cibersegurança, Indústria 4.0, Industrial Internet of Things, Vulnerabilidades no IoT

# Abstract

The Internet-of-things devices massification, led us to witness an explosion in this segment. This expansion has associated an economic growth, due to the different sectors to which it is associated (Industry, Transportation, Telecommunications, etc.), in the perspective of the data analytics that can be obtained with these devices, and the information that can be obtained with these data, however, there is a high insecure component underlying.

The Internet of Things, encompasses “things”, such as sensors, actuators, etc. that when they are conceived, their “creators” do not take into account, the best practices in terms of security, in order to ensure that these devices, are an integral part of the solution and not of the problem.

This dissertation aims to develop a model, which takes into consideration the current difficulty that organizations face, to the point of not understanding what stage of evolution they are, in the journey of Industry 4.0. This model focuses on Industry 4.0, due to the relevance it represents in terms of the countries' economy, as well as the “weight” it has, in the Internet of Things world.

For the elaboration of this model, several analyzes were made, to the most relevant architectural models, that address this sector, as well as the evaluation of different maturity models. This model will allow organizations in the industry sector to be provided with an evaluation matrix, which will allow them to adopt the model and integrate their results into the organization's strategy.

In its evaluation, the model brings together three of the main players in this digitalization of the factory floor change, allowing CxO (Chief Executive Officer, Chief Information Officer, Chief Security Officer, etc.) to act quickly in carrying out the evaluation and with that, take the appropriate measures, issued by the model.

The result of the model/simulator will allow organizations to become more agile in responding directly to the competition, be able to be quicker in decision-making in terms of time-to-market, can focus on customer-oriented production and also adjust the production , to the demand-oriented. This model takes into account the threats and vulnerabilities that result from the IoT phenomenon applied to the industry. Therefore, the model enhances the collaboration of operating technologies with information technologies, guaranteeing the implementation of a solution, based on the best security practices. These internal synergies, allow the organization to have scale economies, resulting in a reduction in operating costs (OPEX) and a greater increase in effectiveness and efficiency.

**Keywords:** Internet-of-things, Cybersecurity, Industry 4.0, Industrial Internet of Things, IoT vulnerabilities.

# Índice

# Lista de Figuras

# Lista de tabelas

# Lista de siglas e acrónimos

| | |
|---|---|
| 6LoWPAN | IPv6 over Low Power Wireless Personal Area Network |
| APT | Advanced Persistent Threat |
| CEP | Complex Event Processing |
| CIA | Confidenciality, Integrity and Availability |
| CoAP | Constrained Application Protocol |
| CPS | Cyber Physical System |
| DCS | Distributed Control Systems |
| ENISA | European Union Agency for Cibersecurity |
| ERP | Enterprise Resource Planning |
| ESTG | Escola Superior de Tecnologia e Gestão |
| ESP | Event Stream Processing |
| FTP | File Transfer Protocol |
| HMI | Human Machine Interface |
| HVAC | Heating, Ventilating and Air Conditioning |
| I4.0 | Indústria 4.0 |
| ICT | Information and Communication Technology |
| ICS | Industrial Control System |
| IIoT | Industrial Internet of Things |
| IoT | Internet of Things |

| | |
|---|---|
| IP | Internet Protocol |
| LiDAR | Light Detection and Ranging |
| LWAN | Low Power Wide Area Network |
| NFC | Near Field Communications |
| NIST | National Institute of Standards and Technology |
| M2M | Machine to Machine |
| MES | Manufacturing Execution System |
| MQTT | Message Queue Telemetry Transport |
| PLC | Programmable Logic Controlleer |
| QR Code | Quick Response Code |
| RFID | Radio Frequency IDentification |
| SCADA | Supervisory Control and Data Aquisition |
| SCI | Sistemas de Controlo Industrial |
| SIMMI4.0 | System Integration Maturity Model Industry 4.0 |
| SIRI | Smart Industry Readiness Index |
| SIS | Safety Instrumented Systems |
| SOA | Service-Oriented Architecture |
| SOC | Security Operation Center |
| TIC’s | Tecnologias de Informação e Comunicações |
| TI’s | Tecnologias de Informação |

| | |
|---|---|
| TO’s | Tecnologias de Operação |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

# 1. Introdução

Internet das Coisas é um tema muito abrangente, pelo que não existe de facto uma única definição para a mesma, no entanto de acordo com o ITU[1], a Internet das Coisas é uma infraestrutura da sociedade de informação, que permite a realização serviços avançados, ao conectar (fisicamente e virtualmente) "coisas", com base em tecnologias de informação e comunicação, interoperáveis existentes e em evolução.

Em termos de âmbito, será importante reforçar que uma "coisa" será, um dispositivo como um sensor eletrónico, que recolhe dados e que pode ser conectado a uma rede de comunicações, como por exemplo uma rede corporativa, uma rede residencial, uma rede industrial ou diretamente ligado à internet de forma física, como por exemplo por cabo de rede ou por fibra, sendo possível ter esta "coisa" ligada por redes Wi-Fi, LTE, 4G, 5G, Bluetooth, RFID, comunicações rádio, etc.

Para manter este paralelismo de conhecimento, de forma coerente ao longo deste trabalho, todas as referências a "coisa", terão por base a descrição supracitada.

Numa perspetiva mais abrangente em termos de interpretação da Internet das Coisas, enquadra-se na possibilidade de fornecer qualquer serviço sobre a rede tradicional da Internet ao permitir comunicações de humanos-a-coisas, coisa-a-coisa ou, coisas-a-coisas [2].

A Internet das Coisas representa a interligação de entidades heterógenas, onde o termo entidades, está mapeado com humanos, sensores ou potencialmente qualquer coisa que possa necessitar e/ou disponibilizar serviços [3].

Assistimos a uma adoção massiva a nível global, transversal a todas as indústrias, segundo um estudo realizado pela Microsoft denominado *IoT Signals* [4]através de um *survey* a três mil decisores, onde é possível verificar a existência de elevados níveis de adoção de soluções no conceito IoT, por parte destes decisores, no curto e médio prazo. Verificamos que na Figura 1, os três setores com maior nível de adesão acima dos 85% são: o retalho, a indústria, os transportes, o governo e a saúde.

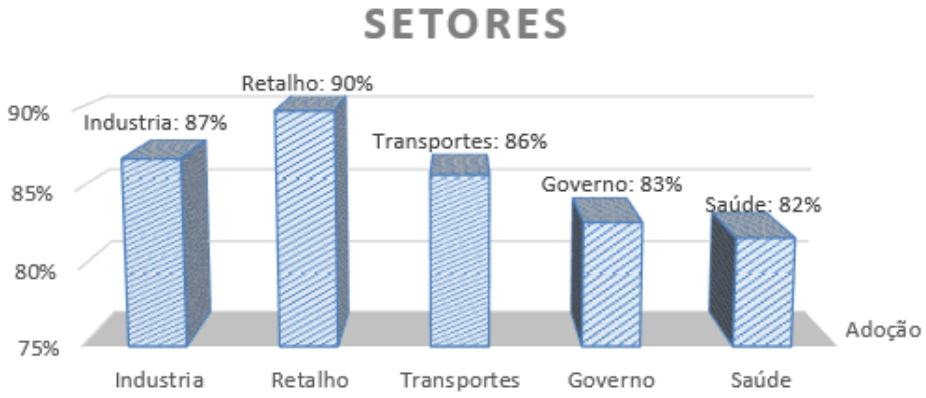



**Figura 1: Percentual de intenção de adoção IoT**
Fonte: Adaptado [4]

É possível também confirmar que os países que lideram esta corrida, acabam por ser os países mais industrializados, por forma a conseguirem ganhar vantagens competitivas a nível económico e financeiro. É possível constatar na Figura 2, que os países com maior nível de adoção, acima dos 85% são a Alemanha e China com 88% seguido pela Franca e os Estados Unidos com 87%.

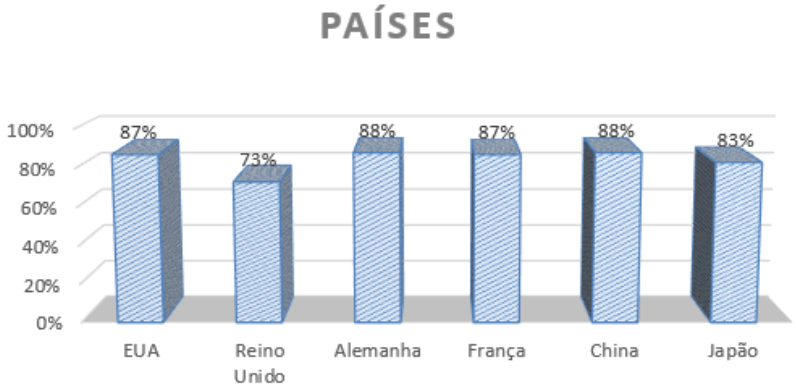



**Figura 2: Países que lideram na adoção do IoT**
Fonte: Adaptado [4]

Estes decisores e influenciadores IoT, nas suas áreas de negócio, vêem o IoT como um fator crítico de sucesso, sendo que as organizações que incorporam estas soluções IoT estão satisfeitas com os resultados obtidos.

## 1.1. Pertinência do tema

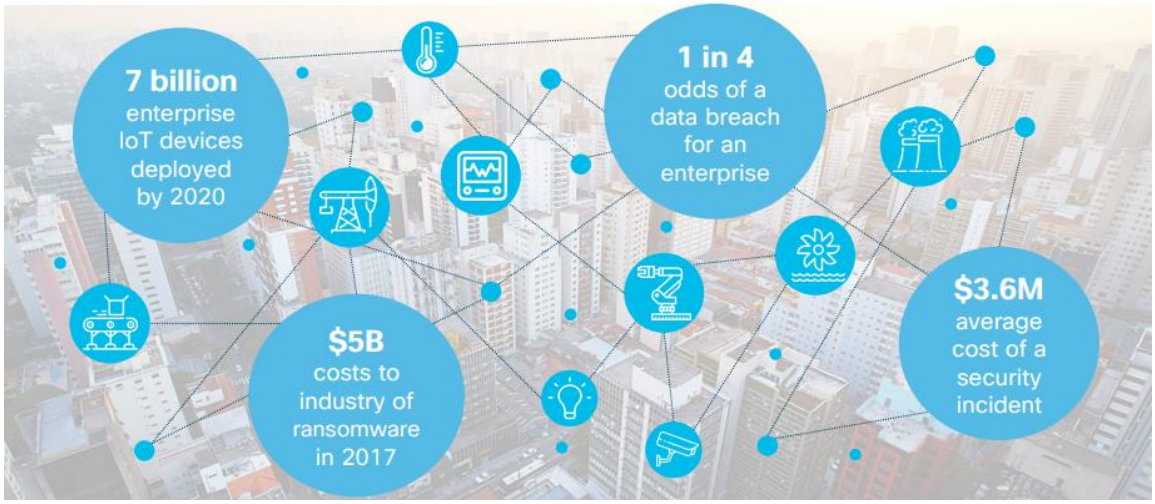
Assistimos ao crescimento exponencial de dispositivos ligados à Internet, como um paradigma emergente e um dos mais espetaculares da última década. Segundo o International Data Corporation (IDC) [5], em 2025 teremos 41.6 mil milhões de dispositivos IoT ou "coisas" que vão gerar 79.4 Zetabytes de dados. A Tabela 1, permite ter a noção e a correlação e a evolução dos dados, ao longo do tempo.

**Tabela 1: Evolução dos dados de Kilobyte ao Geopbyte [6]**

| *Unit* | *Approx* | $10^n$ | *Related to* |
|---|---|---|---|
| Kilobyte (KB) | 1,000 bytes | 3 | Circa 1952 computer memory. |
| Megabyte (MB) | 1,000 KB | 6 | Circa 1976 supercomputer memory |
| Gigabyte (GB) | 1,000 MB | 9 | Mid 1980's disk controller memory attached to a mainframe (that had 128 MB memory) |
| Terabyte (TB) | 1,000 GB | 12 | 2012 largest SSD in a laptop |
| Petabyte (PB) | 1,000 TB | 15 | 250,000 DVD's or the entire digital library of all known books written in all known languages. |
| Exabyte (EB) | 1,000 PB | 18 | 175 EB copied to disk in 2010 (est.) |
| Zettabyte (ZB) | 1,000 EB | 21 | 2ZB copied to disk in 2011 (est.) |
| Yottabyte (YB) | 1,000 ZB | 24 | Roughly equivalent to one septillion bytes |
| Brontobyte (BB) | 1,000 YB | 27 | Brontobyte is equivalent to one followed by 27 zeroes. |
| Geopbyte | 1,000 BB | 30 | Geopbyte is $1_5267\ 650_4\ 600\ 228\ _3229\ 401_2\ 496\ 703_1205$ 376 bytes. |

O desenvolvimento de diversos tipos de protocolos de comunicações, em simultâneo com a miniaturização dos dispositivos transmissores, permite a criação da oportunidade de transformar um dispositivo isolado, num dispositivo de comunicações, ou seja, a "coisa". Verifica-se ainda que, a potência de computação, capacidade energética e as capacidades de armazenamento, da computação miniaturizada dos dispositivos de sensorização tiveram uma melhoria significativa e, em simultâneo sofreram uma redução drástica ao nível das dimensões.

O fabricante Cisco[7], conforme a Figura 3 evidencia que sete mil milhões de dispositivos IoT empresariais estarão instalados no decorrer do ano de 2020, sendo que 25% desses dispositivos podem causar uma falha de segurança nas empresas, tendo um custo médio de 3.6 milhões de dólares em média por incidente. Estas vulnerabilidades, tiveram um custo de cinco mil milhões de dólares, causados por incidentes de *ransomware* no ano de




2017.

**Figura 3: Dispositivos IoT versus impacto nas organizações [7]**

## Levanta-se então uma questão, o porquê da adoção do IoT?

Segundo o estudo realizado pela Microsoft [4] e, conforme a Figura 4, existem dois fatores principais que levam as organizações a adotarem soluções de Internet das Coisas, sendo a primeira razão a otimização das operações, logo seguida pelo aumento da produtividade dos empregados. Este estudo permite ainda verificar que a segurança e proteção do local de trabalho, assim como os ativos da organização, acabam por se inserir numa preocupação relevante e com isto, levar também a que as organizações, considerem esta uma razão relevante.

É ainda possível concluir conforme Figura 4, que entre trinta a quarenta por cento de organizações implementam soluções IoT com o objetivo de gerir a cadeia de fornecimento, garantir a qualidade da sua produção e permitir a localização dos seus ativos.

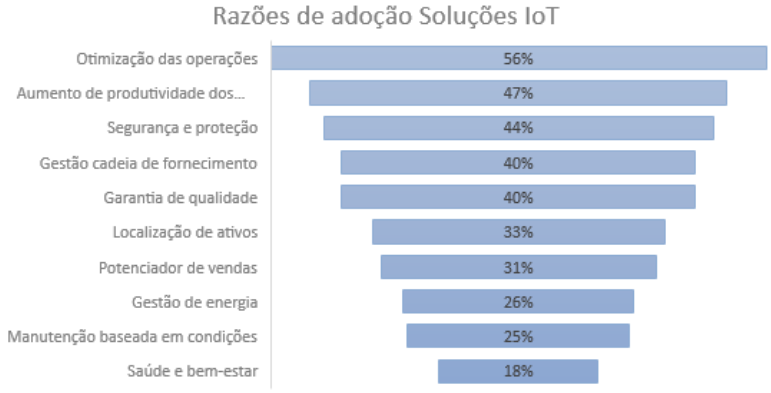



**Figura 4: Razões de adoção soluções IoT**

Fonte: Adaptado [4]

Esta automação permite as organizações otimizarem entregas e rotas, bem como usarem as soluções IoT no sentido de potenciarem as suas vendas.

## 1.2. Identificação do problema

Após a análise em termos de pertinência do tema em estudo e, sendo o IoT um tema tão lato em termos de abrangência, o presente trabalho pretende-se focar numa das derivadas do IoT, a Indústria 4.0, também por vezes mencionada como IIoT. A Indústria 4.0 veio dar competitividade às organizações nesta área, levando a que a indústria tenha a necessidade premente de se reinventar, por forma a acompanhar as evoluções necessárias de adaptação, no sentido de reduzir o *time-to-market,* bem como ajustar a produção à oferta de forma mais ágil. Esta necessidade de agilidade leva a que as organizações tenham que por vezes repensar a sua organização interna no todo, sendo que existem constrangimentos internos das organizações que levam a que muitas das vezes isso não aconteça. Estes constrangimentos, tem impacto direto no retorno de investimento das organizações, face aos concorrentes que por sua vez já adotaram estas medidas.

Entre os constrangimentos identificados, existem dois de maior relevo, que são nomeadamente a falta de uma visão e estratégia que enderece o tema da Indústria 4.0, como um tema a ser tratado de forma prioritário, por forma a colocar a organização no topo do seu setor, em termos de oferta, agilidade na resposta e assim conseguir-se demarcar das suas congéneres.

Outro constrangimento de que as organizações sofrem, advêm de uma consequência da evolução temporal inerente às diferenças existentes entre as unidades de negócio que endereçam a linha de produção e, por norma denominadas as tecnologias de operação versus, as unidades de negócio que endereçam as infraestruturas de tecnologias de informação, que por norma tem como objetivo, responderem às necessidades dentro desta área.

Estas duas unidades por razões históricas, sempre se demarcaram uma da outra, pelos perímetros que endereçavam, sendo que até ao aparecimento da Indústria 4.0 não tinham uma necessidade premente de se alinharem, na persecução dos objetivos da organização, sendo que cada uma poderia fazer o seu caminho em paralelo, para garantir que os objetivos seriam alcançados. A Indústria 4.0 vem reforçar a necessidade de alinhamento destas duas unidades, sendo que quando a organização inicia o processo de "digitalização" do chão de fábrica ou de transformação digital, começa também a expandir o espectro em termos de vulnerabilidades, que leva a que também se tenha que acautelar as necessidades de cibersegurança, nesta área.

A identificação do problema e as ineficiências geradas pelo mesmo, tem uma causa-efeito direto em termos de ineficiências organizacionais e estruturais, impactando com a competitividade da organização, não se coadunando com as estratégias adotadas pelas organizações com o foco de endereçarem a Indústria 4.0. O modelo a desenvolver, tem

como objetivo de reduzir este tipo de ineficiências bem como de reforçar a componente ao nível da segurança.

## 1.3. Objetivos e contribuições

O objetivo deste trabalho, é a criação de um modelo assente numa classificação, com base num índice aplicado ao estudo na indústria inteligente ou *Smart industry*, que é uma das áreas abrangidas pela implementação das soluções de Internet das Coisas, sendo também apresentada uma visão geral de outros segmentos, como por exemplo cidades inteligentes e *smart buildings.*

Este trabalho tem assim o propósito de disponibilizar o conhecimento e os meios, que possam suportar melhorias no processo organizacional e ao nível da produtividade. Este objetivo pretende reforçar a competitividade das organizações da indústria, contribuindo para o crescimento da economia.

Pretende-se demonstrar o nível de maturidade de implementação ao nível de Cibersegurança das Indústrias 4.0 através de um modelo concebido para esse fim. Para esta análise em termos processuais, é feita a primeira avaliação, no sentido de nivelar a organização, no estágio I4.0, com a inclusão da componente ao nível da cibersegurança, que com base nos modelos de índices e frameworks avaliados (RAMI, SIRI e SIMMI), estes modelos (de arquitetura e maturidade) não refletem de forma percetível esta camada, ao nível da integração na organização.

Este propósito e objetivo encontra-se em linha com desafio de manter e desenvolver a competitividade das organizações industriais, através da melhoria contínua. Esta dissertação pretende também partilhar o conhecimento, por forma a que possa ser usado, no meio académico bem como no meio empresarial.

## 1.4. Estrutura do trabalho

O trabalho encontra-se estruturado em sete capítulos, segmentados da seguinte forma. O presente capítulo (primeiro) apresenta o enquadramento do tema, com a introdução ao mesmo.

O segundo capítulo, incide sobre a Internet das Coisas, com uma análise abrangente de como, estes dispositivos, que consolidam a Internet das Coisas, estão a “conquistar” o mundo bem, como os protocolos existentes atualmente nesta área.

O terceiro capítulo, descreve as tendências em termos de mercado tendo por base o *Hype Cycle*, aplicado à Internet das Coisas, os protocolos usados bem como as ameaças e vulnerabilidades, ao nível das Internet das Coisas.

O quarto capítulo versa sobre a Indústria 4.0 e o estado da arte da mesma, este capítulo reveste-se de uma importância considerável, uma vez que endereça diferentes modelos de maturidade e arquiteturas aplicados à Indústria 4.0.

No quinto capítulo são apresentados os desafios associados à segurança, no que concerne a Internet das Coisas, associados aos dispositivos e de como estes dispositivos, podem ser categorizados, face ao setor, localização, conectividade, tecnologia, tipo de dispositivo. Este mesmo capítulo realça um dos modelos de segurança de referência, em termos de mercado, sendo também feita a correlação das iniciativas de segurança aplicadas ao IoT realizadas por diversas entidades.

No sexto capítulo, é apresentado o modelo desenvolvido $(MI)^2$4.0 com base em toda a informação recolhida com objetivo de articular a Indústria 4.0, no sentido de reforçar a segurança nesta área.

A conclusão é apresentada no sétimo capítulo, com a apresentação das conclusões resultantes do trabalho realizado e, onde são também referidos alguns tópicos para trabalho futuro.

# 2. Internet das Coisas

O presente capítulo faz o enquadramento do conceito “coisa” e a “explosão” que estas “coisas” tiveram a nível global. São também realçados alguns dos constrangimentos que estes dispositivos apresentam e que por sua vez levam a um aumento da superfície de ataque, levando a uma maior exposição das organizações. É realizada uma abordagem às comunicações wireless e as suas caraterísticas, que por norma asseguram as comunicações entre as “coisas” e as plataformas que garantem a recolha e tratamento dos dados e, os convertem em informação. Para uma melhor compreensão dos mercados que maior impacto na adoção destes dispositivos é também realizada uma análise neste âmbito que permite assim, corroborar o foco do trabalho incidir sobre a Indústria 4.0. Por fim são abordados os diversos protocolos mais comumente usados ao nível do IoT.

## 2.1. Caraterização da Internet das Coisas

O termo Internet das Coisas, como conceito foi mencionado pela primeira vez na década de 90. Esta “expressão” foi proposta por Kevin Asthon decorrente de uma apresentação realizada pelo mesmo em 1999 [8].

A Internet das Coisas está associada a uma rede de dispositivos com endereço IP, com capacidades de sensorização, recolha e envio de dados usando sensores embebidos, hardware de comunicação e processadores.

No IoT uma “coisa”, ou seja, a componente da “thing”, é um dispositivo concebido por um humano ou, um “objeto” feito por uma máquina implementado de forma natural, com comunicações para poder comunicar através da rede. Estas “coisas”, conforme é possível verificar na Figura 5, encontram-se disseminados na indústria, nas cidades, nos hospitais, nos edifícios e num número alargado de casos.

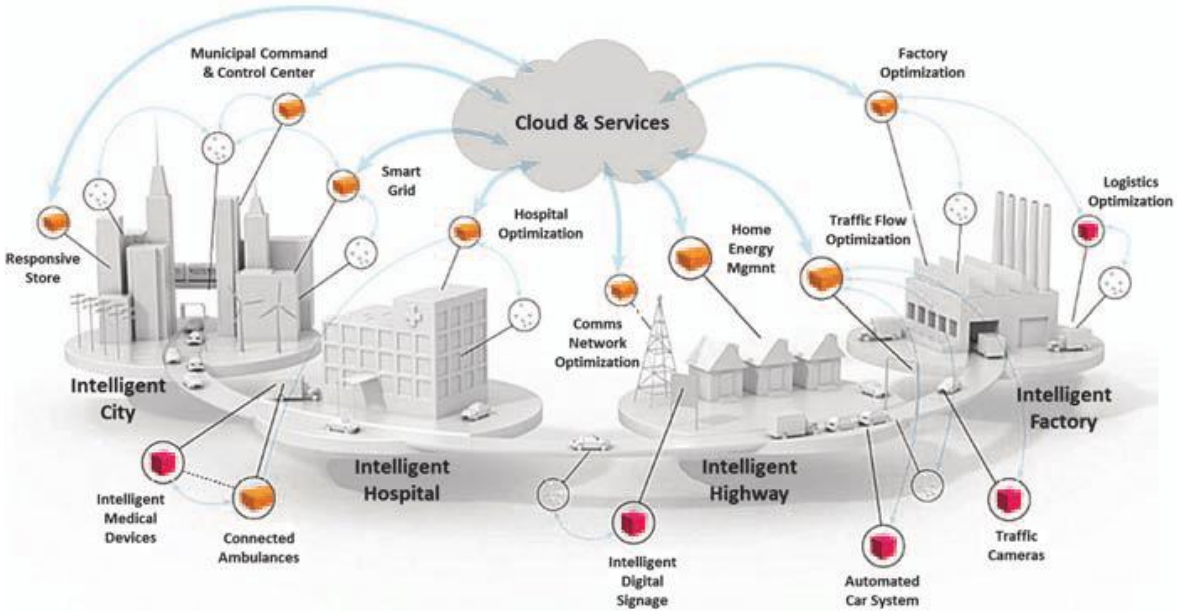



**Figura 5: Internet of Things – Framework de Sistema Inteligente**
Fonte: Intel

Os problemas de segurança na Internet das Coisas, diferem significativamente das ameaças tradicionais dos ambientes das tecnologias de informação e comunicações. A segurança "tradicional" nas tecnologias de informação e comunicações, foca principalmente na componente de proteção da confidencialidade, integridade e disponibilidade dos dados.

As tecnologias de informação têm na sua competência, garantir boas práticas ao nível da segurança como os últimos *updates* dos equipamentos, aplicações de *patch* de correção, cifragem dos dados por forma a garantir integridade dos dados, níveis de autenticação seguros, comunicações seguras com implementação de VPN's, segregação da rede com criação de VLAN's, etc.

As caraterísticas únicas dos dispositivos referentes à Internet das Coisas, tem na sua conceção, alguns constrangimentos de hardware, como limitações de processamento, memória, reduzida capacidade de arquivo, alimentação (bateria), taxas de transferência (reduzidas), tamanho, custos (baixos), associado a comunicações nem sempre com elevada fiabilidade (uso de protocolos inseguros).

Estas caraterísticas realçam o porquê destes dispositivos por definição, serem vulneráveis em termos de segurança (portas de comunicação abertas, sistemas insuficientes de privacidade, proteção e encriptação, falta de atualizações, componentes inseguros, etc.).

Conforme apresentado na Figura 6, é possível constatar que um dos maiores fabricantes nesta área, a Cisco, prevê a existência de mais de vinte mil milhões de dispositivos em 2020, onde se incluem os dispositivos empresariais, residenciais e industriais.

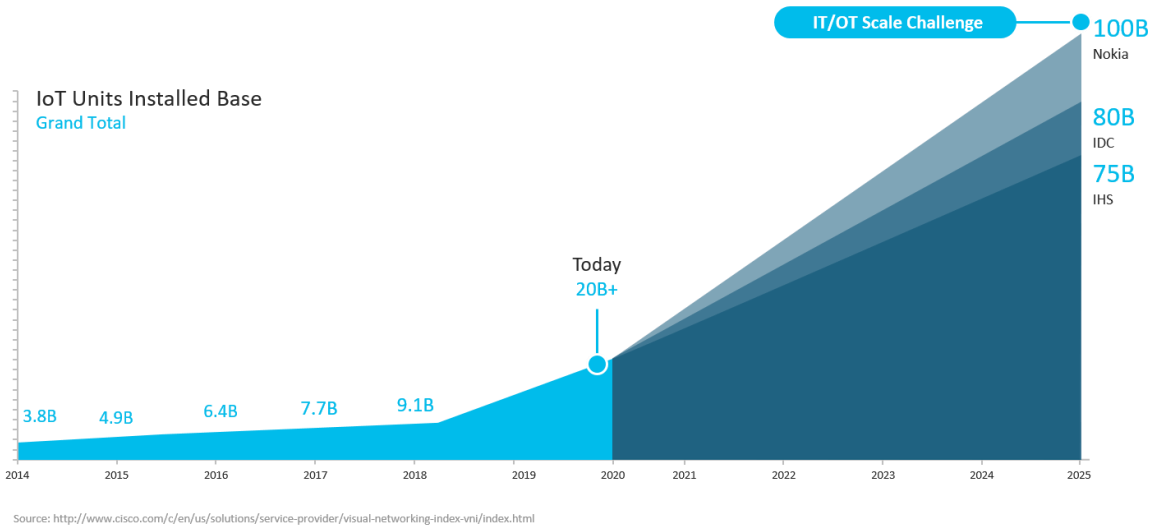



**Figura 6: Unidades de dispositivos instalados [9]**

Os dispositivos são implementados de forma rápida numa escala global, sendo desconhecido o tempo de vida dos mesmos. As soluções assentes em cima de dispositivos IoT, são um dos principais impulsionadores de inovação no mercado global, mas que por outro lado, também levam a um crescimento da insegurança.

Por forma a garantir uma implementação alargada, diferentes tipos de tecnologias *wireless* podem ser usadas, no sentido de assegurarem a cobertura das zonas a intervencionar. A Figura 7, permite correlacionar a largura de banda *versus* a distância de cobertura de cada uma dessas tecnologias.

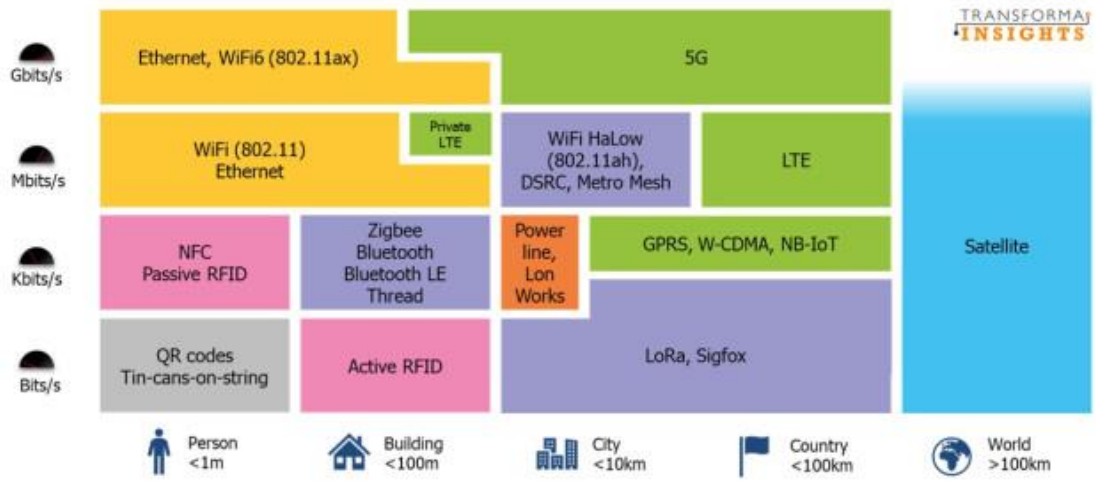



**Figura 7: Tecnologias Wireless IOT [10]**

O 5G (ou rede de quinta geração) é uma rede de telecomunicações de próxima geração, por norma disponibilizadas pelos operadores, que tem como grande diferença as velocidades de *download* e *upload* que estas vão permitir (cf. Figura 8):

- Até 10Gpbs de taxa de dados (Dez vezes superior ao 4G);
- Latência 1 milissegundo;
- 99,999% disponibilidade;
- 90% de redução da energia usada na rede;
- Até 10 anos de duração de duração das baterias para os dispositivos de IoT de baixo consumo;
- Até cem vezes mais dispositivos ligados por unidade de área (quando comparado com 4G LTE).

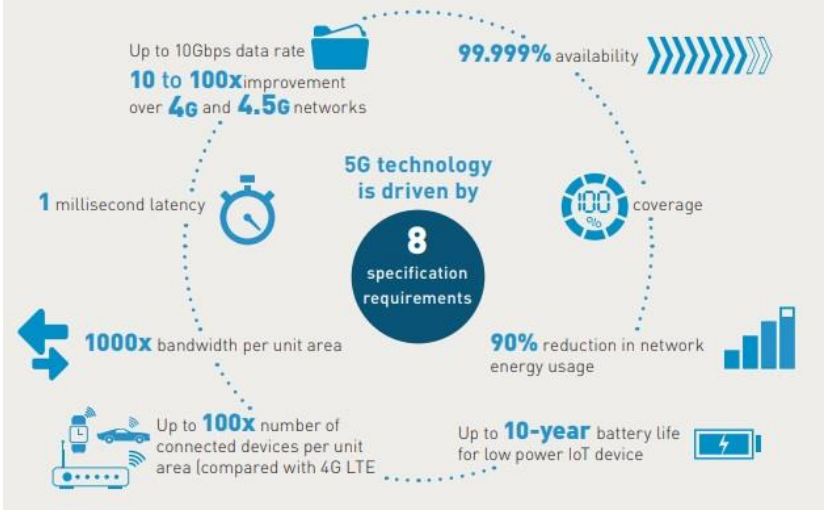



**Figura 8: Especificações 5G (Rede de 5ª geração)[11]**

Ao longo do tempo é possível verificar, que a evolução das redes de telecomunicações dos operadores, tem recebidos serviços conforme apresentado na Figura 9, que acrescentam valor às comunicações e assim também tem sido impulsionadas, tecnologicamente para garantirem essa qualidade de serviço e valor acrescentado para o cliente final.

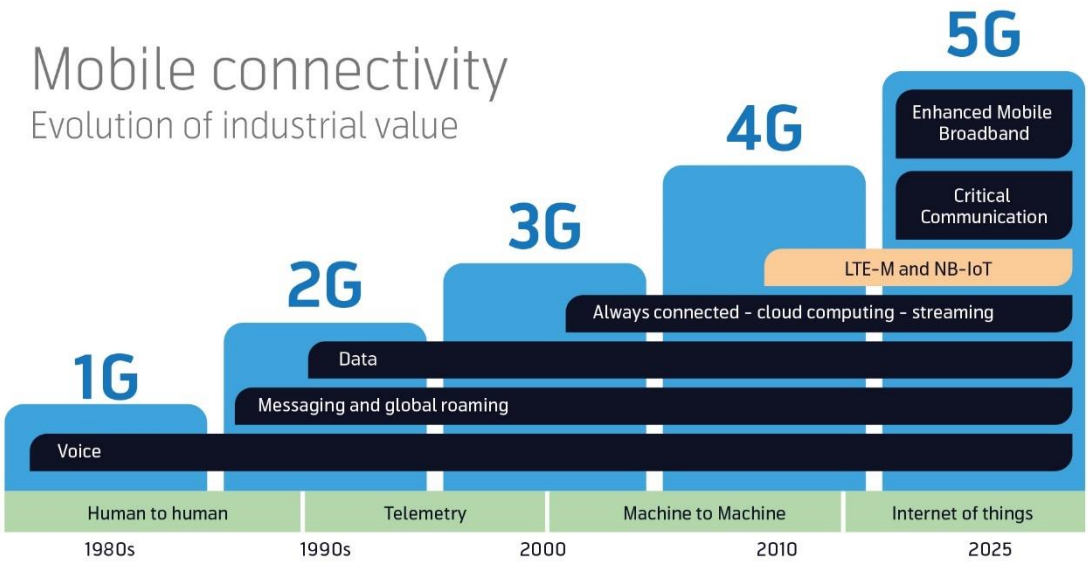



**Figura 9: Conetividade Móvel evolução do valor industrial [12]**

O Wi-Fi tem-se pautado por uma evolução tecnológica, com aumentos significativos em termos de taxas de transferência, conforme apresentado na Figura 10, desde os 11 Mbps do standard 802.11b, até ao atual 802.11ax com taxas de transferência que poderão ir até aos 9.6 Gbps.

| 802.11 | Frequency | Data rate | Channels | Channels 'usable' |
|---|---|---|---|---|
| a | 5 GHz | 54 Mbps | 24 | 24 |
| b | 2.4 GHz | 11 Mbps | 13 | 3 |
| g | 2.4 GHz | 54 Mbps | 13 | 3 |
| 4 | 2.4 GHz & 5 GHz | (min) 65, 150, 300, 450, (max) 600 Mbps | 2.4 GHz & 5 GHz Rules apply. | 2.4 GHz & 5 GHz Rules apply. |
| 5 | 5 GHz | 867 Mbps 1.3 Gbps | 24* 37** | 24* 37** |
| 6 | 2.4 GHz & 5 GHz | 1.2 Gbps 9.6 Gbps | 2.4 GHz & 5 GHz 13 & 24/37(US) | 2.4 GHz & 5 GHz 3 & 24/37(US) & subcarriers |

* = 802.11ac Wave 2** = 802.11ac Wave 2 (US)

**Figura 10: Frequência e taxas de transferência Wi-Fi [13]**

Conforme apresentado na Figura 11, o standard 802.11ax, recebeu a denominação de Wi-Fi 6 pela *Wi-Fi Alliance*[14], sendo que os standards precedentes receberam a denominação de Wi-Fi 5 para o 802.11ac e, Wi-Fi 4 para o 802.11n e assim sucessivamente.

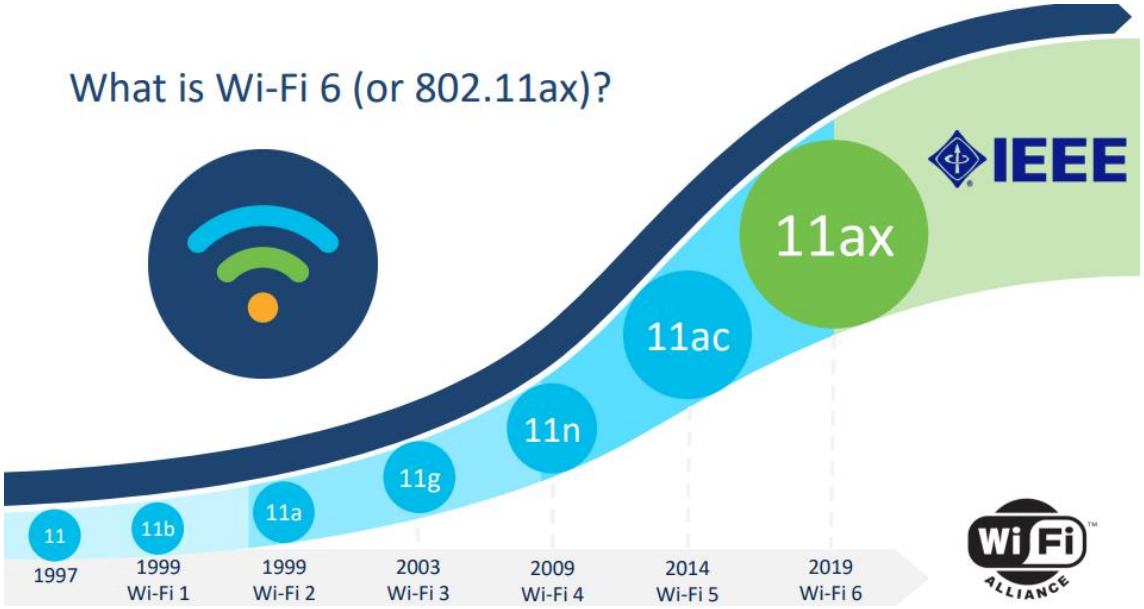



**Figura 11: Evolução dos standards Wi-Fi [13]**

Os standards apresentados à direita do logo "Wi-Fi", na Figura 12, como o 802.11ad, ah (Wi-Fi HaLow), ay e az são standards futuros.


**Figura 12: Standards Wi-Fi [13]**

Caraterísticas resumo destes standards futuros:

**802.11ad**

- Baixa potência;
- Distâncias curtas (+/- 10 metros);
- Uso interior;
- Taxas de transferência na ordem dos 4.6 Gbps;
- Frequência 60Ghz.

**802.11ay**

- Apresenta-se como o sucessor do 802.11ad;
- Taxas de transferência >20Gbps;
- Próxima geração de frequências de 60Hz.

**802.11af**

- Baixa potência;
- Grandes distâncias:
- Baixas taxas de transferência;
- Taxas de transferência na ordem dos 30Mbps;
- Frequências < 1Ghz;
- Tipicamente usado para IoT.

**802.11ah**

- Frequência < 1Ghz;
- Inicialmente previsto 700 Mhz e 900Mhz;
- Grande alcance;
- Taxas de transferência até 350 Mbps;
- Tipicamente usado para o IoT.

O NFC é uma tecnologia que funciona por aproximação entre dois dispositivos e é, comumente usada nos terminais de pagamento *POS – Point of Sale*, em conjunto com os cartões multibanco. O NFC funciona num subconjunto das frequências das redes sem fio que se encontra a funcionar no 13.56Mhz.

O RFID é uma tecnologia que corre em cima de rádio frequência usado para a identificação de pessoas ou objetos, onde o método mais usado é o armazenamento de por exemplo um número de série para identificar uma pessoa, um objeto ou outra informação ficando a mesma armazenada num, microchip.

QR Codes, são códigos de “barras” dimensionais, que pode ser digitalizado, contendo na sua codificação informação sobre produtos, contactos, localizações, etc.

A Tabela 2, evidencia as principais diferenças das tecnologias mais usadas, atualmente ao nível do wireless, como LoRaWan, Sigfox, NB-IoT, etc.

**Tabela 2: Comparação de tecnologias Wireless [15]**

| Attribute | Bluetooth® Low Energy Technology | Wi-Fi | Z-Wave | IEEE 802.15.4 (Zigbee, Thread) | LTE-M | NB-IoT | Sigfox | LoRaWAN |
|---|---|---|---|---|---|---|---|---|
| Range | 10 m – 1.5 km | 15 m – 100 m | 30 m - 50 m | 30 m – 100 m | 1 km – 10 km | 1 km – 10 km | 3 km – 50 km | 2 km – 20 km |
| Throughput | 125 kbps – 2 Mbps | 54 Mbps – 1.3 Gbps | 10 kbps – 100 kbps | 20 kbps – 250 kbps | Up to 1 Mbps | Up to 200 kbps | Up to 100 bps | 10 kbps – 50 kbps |
| Power Consumption | Low | Medium | Low | Low | Medium | Low | Low | Low |
| Ongoing Cost | One-time | One-time | One-time | One-time | Recurring | Recurring | Recurring | One-time |
| Module Cost | Under $5 | Under $10 | Under $10 | $8-$15 | $8-$20 | $8-$20 | Under $5 | $8-$15 |
| Topology | P2P, Star, Mesh, Broadcast | Star, Mesh | Mesh | Mesh | Star | Star | Star | Star |
| Shipments in 2019 (millions) | ~3,500 | ~3,200 | ~120 | ~420 | ~7 | ~16 | ~10 | ~45 |

A massificação do IoT, tem levado a várias abordagens ao nível das comunicações que podem passar por usar um operador de telecomunicações, com implementação de comunicações assentes em 3G, 4G/LTE e mais recentemente a instalação do 5G. As opções em termos de implementação neste nível podem também, passar por comunicações de frequências não licenciadas como por exemplo LoRa, Sigfox, etc.

Os projetos em si, pelos requisitos inerentes ao mesmo, levam à implementação/escolha de uma tecnologia em detrimento de outra, levando em consideração o tipo de uso pretendido da mesma, onde são analisados requisitos como:

- Quantidade de dados que se pretende transmitir;
- Distancia entre os locais a transmitir;
- Orçamento.

A expansão exponencial do IoT, endereça vários segmentos, como:

- Indústria;
- Transportes;
- Energia;
- Retalho;
- Cidades Inteligentes (*Smart Cities*);
- Saúde;
- Cadeia de Fornecimento;
- Agricultura;
- Edifícios Inteligentes.

O presente trabalho, teve em consideração o alargado leque de mercados em termos de aplicabilidade das soluções IoT, conforme os acima discriminados.

Com uma panóplia tão alargada de mercados/setores a dissertação, incide sobre o setor que maior crescimento apresenta e, que tem um forte impacto nas economias dos países, que é a Indústria 4.0.

Uma análise realizada, a 1414 projetos IoT, realizado pelo *IoT Analytics* [16] e conforme apresentado na Figura 13, o setor com maior crescimento é o da Indústria 4.0, com 22% do total dos projetos, seguido pelos transportes (15%) e a energia (14%).

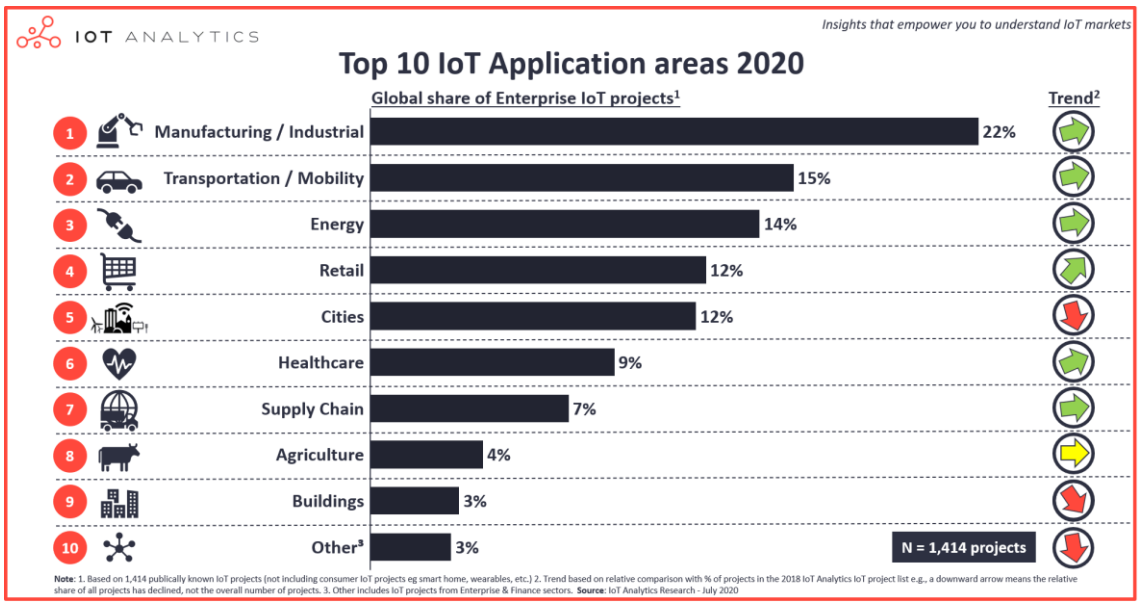



**Figura 13: Dez principais áreas de aplicação do IoT [16]**

Este indicador, serviu de base na realização da dissertação, permitindo focar o trabalho na área de maior crescimento (Indústria 4.0) e, que impacta de forma direta, no crescimento económico dos países. O capítulo 4, desenvolve esta área, bem como as potenciais ameaças ao nível de segurança, nos dispositivos IoT.

## 2.2. Protocolos IoT

Os protocolos mais comumente usados nas comunicações no IoT, realçam-se os seguintes o *Message Queue Telemetry Transport* (MQTT), o *Constrained Application Protocol* CoAP), O *Extensible Messaging and Presence Protocol* (XMPP) e, o *Advanced Message Queuing Protocol* (AMQP).

### MQTT

O protocolo MQTT[53] é um protocolo "leve" de mensagens, que funciona sobre TCP/IP. Este protocolo é especialmente focado para dispositivos IoT com restrição de recursos (exemplo: memória, CPU, etc.), bem como o uso de redes com uma largura de banda mais limitada, alta latência ou redes não confiáveis. O MQTT funciona bem para dispositivos que operam em locais remotos, onde a largura de banda da rede é restrita.

**CoAP**

O CoAP é um protocolo da camada aplicacional que foi definido pela IETF (Internet Engineering Task Force)[54] concebido para pequenos dispositivos eletrónicos, particularmente usada em termos de tecnologia do IoT e das suas redes associadas. O CoAP pode trabalhar com uma variedade de dispositivos da Internet, que consomem apenas recursos limitados, como sensores de rede sem fios (denominado Wi-Fi), sensores de baixa potência e outros tipos de componentes.

**XMPP**

O XMPP[55] teve o seu início como Jabber, uma tecnologia aberta de mensagens instantâneas. O XMPP é baseado em XML e, foi expandido para ser usado em sistemas de *publish-subscriber* (publicante-subscritor, conforme apresentado na Figura 14), vídeo e aplicações IoT como redes inteligentes.

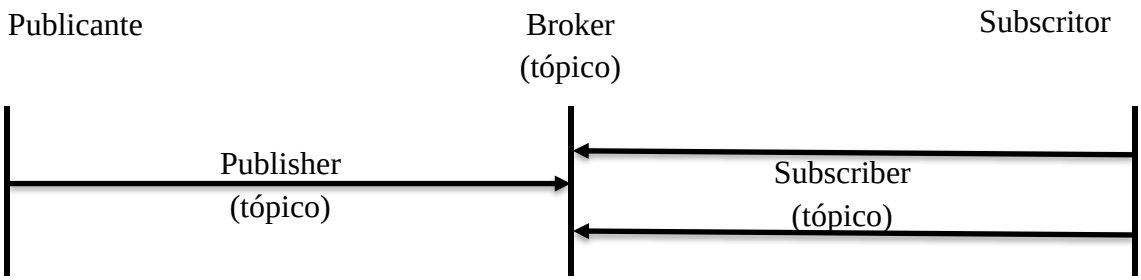



**Figura 14: Publish-Subscriber**

**AMQP**

O AMQP[56] é um protocolo de ligação binária concebido para *middleware* orientado a mensagens, conhecido pela sua interoperabilidade e confiabilidade. Seus principais recursos são orientação das mensagens, filas e, reencaminhamento de mensagens através do roteamento das mesmas (incluindo ponto a ponto, publicação e assinatura), fiabilidade e segurança. Este protocolo disponibiliza uma grande quantidade de controlo.

## 2.3. Síntese

Este capítulo tem como objetivo fazer o enquadramento do tema Internet das Coisas, apresentado uma perspetiva global com a apresentação dos diversos setores, que podem ser endereçados por esta vaga.

Os indicadores apresentados, permitem concluir que se assiste a uma massificação de instalação de dispositivos, sendo que muitos destes dispositivos, pelas qualidades associadas aos mesmos, como por exemplo o baixo custos destes, leva a que sejam descurados muitos pontos importantes, como a segurança.

Para que estes dispositivos sensores/coisas possam comunicar, necessitam de ter um meio de comunicação, tecnologia que é por norma eleita, em função do projeto a implementar, que leva em consideração, indicadores como, distâncias, quantidade de informação a

transmitir e inevitavelmente o orçamento que o cliente tem para implementação do projeto.

Ao nível das comunicações do IoT, são também analisados os protocolos mais frequentemente usados, nesta componente.

Esta análise, realizada neste capítulo permitiu também concluir, que o setor que maior crescimento apresenta é o da Indústria. Sendo a indústria o principal setor de crescimento, potenciado pela revolução da indústria 4.0, sustentado pelas novas tecnologias assentes em cima das Internet das coisas.

Com um setor tão relevante para a economia dos países a análise dos problemas de segurança da internet das coisas, incidirá no setor da indústria 4.0.

# 3. Evoluções futuras do IoT, no curto, médio e longo prazo.

Este capítulo avalia as tendências futuras do IoT, em diferentes horizontes temporais. Esta análise permite obter uma "imagem" da evolução do IoT, perspetivando a possibilidade das organizações se posicionarem melhor, ao nível da estratégia organizacional obtendo desta forma vantagens competitivas face às suas congéneres. Esta análise permite percecionar as evoluções ao nível dos serviços, bem como evoluções ao nível dos produtos.

## 3.1. Tendências

Numa análise em termos de segurança, é relevante a análise da evolução no médio e no longo prazo, sendo para tal efetuado uma abordagem do Hype Cycle da Gartner apresentado na Figura 15, que nos perspetiva na presente data, as evoluções a ocorrer no curto e médio prazo.

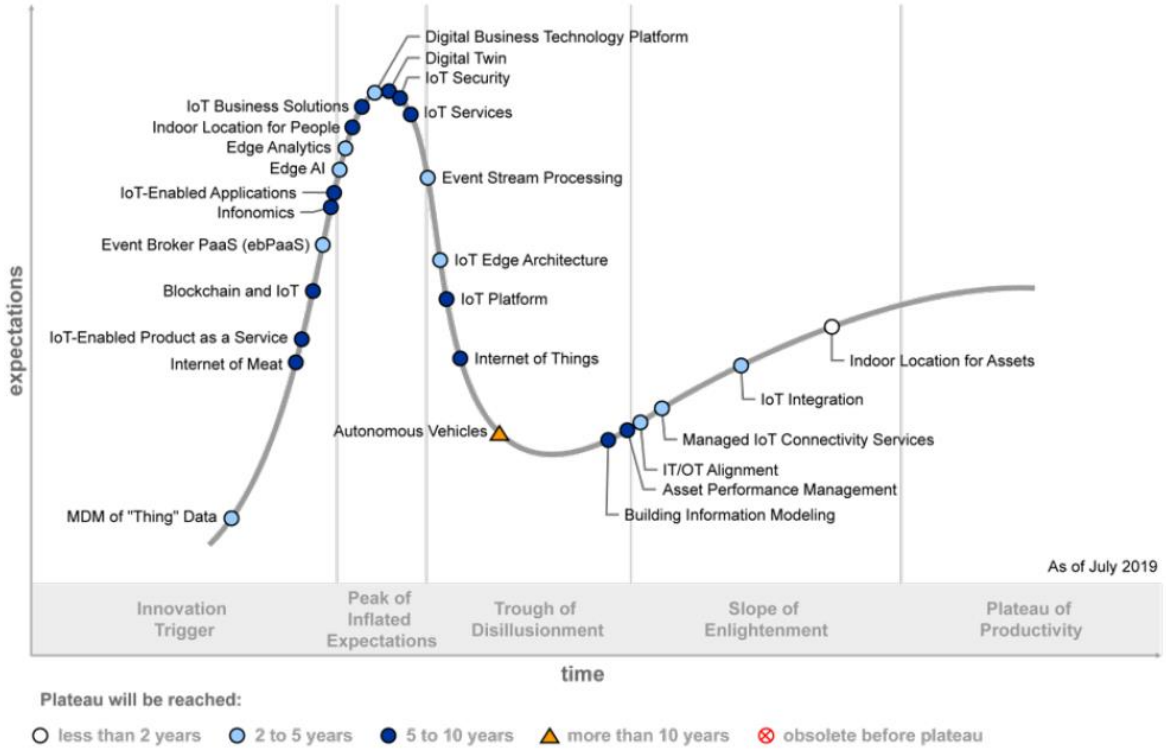



**Figura 15: Hype Cycle for Internet of Things 2019 [57]**

Em termos de definição temporal, assume-se menos de dois anos como o curto prazo, o médio prazo entre dois a cinco anos e o longo prazo em mais de cinco anos.

Neste *Hype Cycle* podemos na Tabela 3, analisar as quatro fases desde a *Innovation Trigger* até à *Slope of Enlightenment*, com análise temporal no curto, médio e longo prazo.

**Tabela 3: Matriz de Prioridades da Internet das Coisas, 2019 [57]**

| Benefícios | Menos de 2 anos | 2 a 5 anos | 5 a 10 anos | Mais de 10 anos |
|---|---|---|---|---|
| Transformação | | • Plataforma Tecnológica Digital de Negócio<br>• Inteligência Artificial no EDGE<br>• Processamento de eventos de streaming | • IoT e Blockchain<br>• Digital Twin<br>• Infonomics<br>• Internet das Coisas<br>• Soluções de Negócio IoT<br>• Aplicações IoT ativos<br>• Produto IoT as a Service | Veículos autónomos |
| Elevado | Localização de ativos no interior | • Analítica no Edge<br>• Event Broker PaaS (ebPaaS)<br>• Arquitetura IoT no Edge<br>• Integração IoT<br>• Alinhamento IT/OT<br>• MDM dos Dados das "Coisas" | • Gestão de desempenho de ativos<br>• Construção de Modelação de Informações;<br>• Localização de pessoas no interior de edifícios<br>• Internet of Meat<br>• Plataforma IoT<br>• Segurança IoT<br>• Serviços IoT | |
| Moderado | | • Gestão IoT<br>• Serviços de Conectividade | | |
| Baixo | | | | |

Apresenta-se abaixo a decomposição do *Hype Cycle for the Internet of Things 2019:*

a) MDM dos dados das "Coisas", é a aplicação da gestão dos dados principais. a prática, a disciplina e a capacidade tecnológica, no apoio do domínio dos dados de identificação da entidade habilitada de objetos para o IoT e os seus *digital-*

*twins*[1]. Permite a representação semântica dos dados principais da "coisa" através das arquiteturas distribuídas, IoT, OT e IT. O resultado permite a resolução da entidade do objeto, independentemente do aplicativo, sistema ou plataforma;

b) Internet of Me(at) (IoM), é um conceito em que a tecnologia é instalada no interior do corpo, ligada e acessível através de comunicações wireless, fazendo os humanos parte do mundo ligado, mesmo que de forma intermitente ou temporariamente;

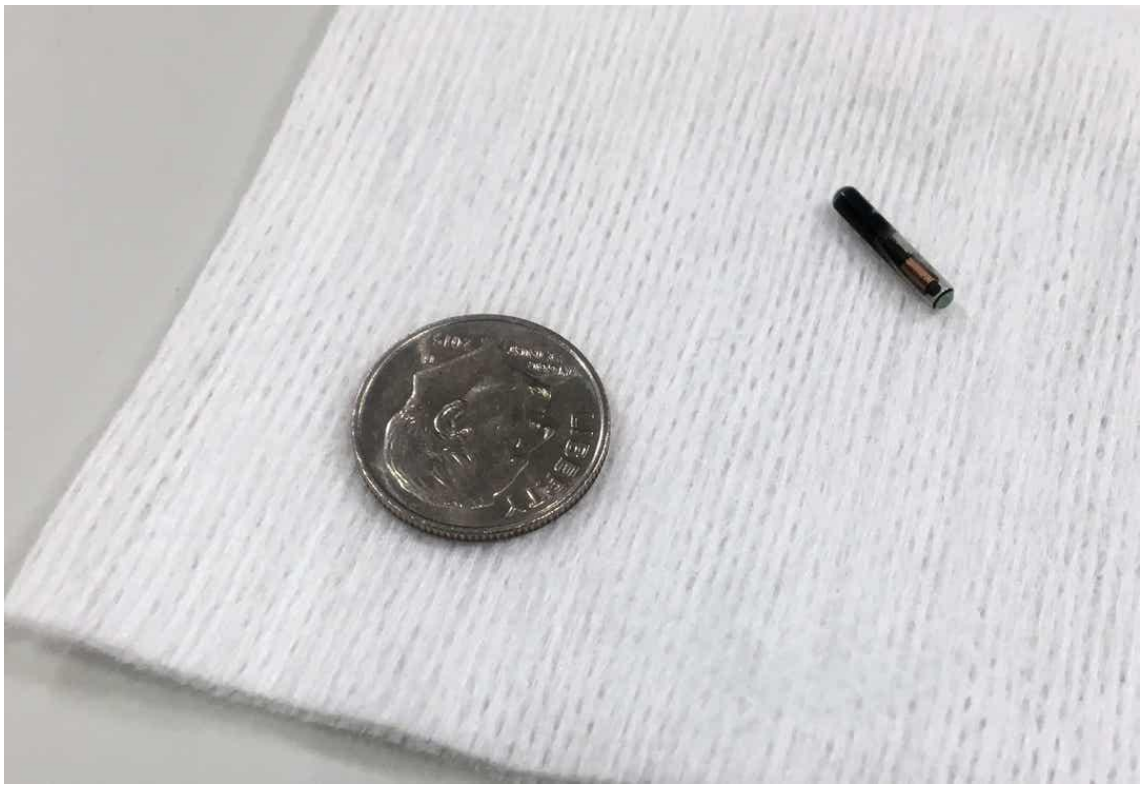


**Figura 16: Comparação do chip com o cêntimo de dólar [58]**

Esta tendência está a ser maioritariamente a ser seguida na Suécia, onde na presente data da elaboração da dissertação, mais de quatro mil pessoas[59] já tinham sido submetidas a esta intervenção de inserção do chip debaixo da pele, conforme exemplo apresentado na Figura 16 e Figura 17.

[1] Digital Twins – Representações virtuais de uma entidade

**Figura 17: Internet of Me(at)[59]**

c) IoT como Produto as a Service é um modelo que se enquadra no âmbito de produto como serviço, sendo que a organização adquire os equipamentos como ativos operacionais recorrentes;
d) Blockchain e IoT, endereça o uso do blockchain em conjunto com os dispositivos e tecnologias IoT. Integração do IoT e Blockchain no suporte de processos confiáveis multipartidários, que "ligam" o mundo físico das "coisas" ao processo do ambiente computacional do negócio;
e) O Event Broker PaaS (ebPassS) na cloud, desempenha o papel de intermediário numa arquitetura orientada a eventos (EDA – event-driven architecture), na gestão das relações do publisher e do subscriber (publicador e do assinante) no sentido de facilitar as suas interações;
f) O conceito *infonomics,* é a teoria e prática de tratamento da informação como um ativo organizacional;
g) As aplicações disponíveis para o IoT, são concebidas nativamente ou modernizadas para suporte direto do IoT como:
    - É integrada com os dispositivos e plataformas na fronteira do IoT;
    - Assimilação e análise dos dados e eventos do IoT no sentido de produzir uma descoberta e orquestrar uma resposta do negócio;
    - Para garantir os itens acima utiliza *digital twins*;
h) Inteligência artificial no *edge* (na fronteira), incide no uso de técnicas de inteligência artificial embebido nos dispositivos terminais, *gateways* e dispositivos de *edge* em aplicações que variam desde veículos autónomos até analítica de *streaming*.

Embora predominantemente focado na inferência da inteligência artificial, o sistema mais sofisticado pode incluir capacidade de formação local de fornecer otimização dos modelos de inteligência artificial;

i) Analítica no *edge*, é a disciplina que aplica a lógica (exemplo: regras) e matemática (algoritmos) aos dados de forma a disponibilizar informação para tomar melhores decisões;
j) A localização interna de pessoas é uma necessidade de várias organizações, numa base de necessidade de segurança das mesmas ou numa perspetiva de produtividade. Os mercados verticais de localização de pessoas incluem clientes, empregados, crianças e idosos e dependem do resultado, sendo que cada um dos casos podem exigir o uso de tecnologia diferente no sentido de atingir o objetivo;
k) Soluções de negócio IoT é a combinação de tecnologias IoT e aplicações de negócio que produzem resultados desejados, como otimização de ativos ou produto como serviço;
l) Plataformas de negócio de tecnologia digital, é a combinação de um conjunto de tecnologias que permitem uma organização participar num ecossistema digital. Integra plataformas existentes de IT, envolvimento do cliente, dados e analítica, sistema de parceiros e *Internet of Things* para "sentir" os eventos do negócio, decidir o que fazer e implementar uma resposta do negócio, que cria valor aos envolvidos. Plataforma que partilha os ativos como os dados, algoritmos e transações com ecossistema de negócio de forma a mapear, criar e trocar serviços;
m) "Gémeos Digitais" ou *Digital Twins*, são representações virtuais de uma entidade como um ativo, pessoa ou processo que é desenvolvida para suportar novos objetivos ou objetivos melhorados. Os três tipos de *digital Twins* são o discreto, o composto e o organizacional. Elementos necessários no sentido de responderem aos objetivos do negócio são, modelo, dados, associação um-para-um e monitorização, sendo elementos opcionais a analítica, controlo e simulação;
n) Segurança na *Internet of Things* é parte da segurança digital. Funciona em conjugação com a segurança ciber física e, endereça iniciativa digitais envolvendo o IoT para o software, hardware, rede e proteção de dados. A segurança no IoT partilha muitas das tecnologias e processos das tecnologias de informação, tecnologias de operação e segurança física. Os controlos de segurança do IoT criam confiança, bem como disponibilizam segurança, fiabilidade, sistemas digitais privados e resilientes para o negócio digital;
o) Serviços IoT abrangem suporte, manutenção e serviços profissionais para fornecer um leque alargado do negócio e especialidade técnica no suporte dos planos IoT de criação e execução de serviços. Várias *frameworks*, metodologias e ativos estão dentro do âmbito dos serviços IoT. Os serviços IoT devem de ser vistos num âmbito mais amplo de "serviços digitais";
p) Processamento de fluxos de eventos, define um fluxo de eventos como uma sequência de objetos de eventos organizados por uma determinada ordem, normalmente por tempo. O processamento de fluxo de eventos (ESP) é a computação que é realizada nos objetos do evento, com a finalidade de integração

dos dados de fluxo ou, análise de fluxo (também chamado de processamento de eventos complexos [CEP]). O ESP é normalmente aplicado aos dados conforme estes chegam (dados "em movimento"). O ESP fornece informações sobre ameaças emergentes, oportunidades de alertas "quase" em tempo-real, painéis de monitorização (denominados *dashboards*), processos de deteção e resposta e armazena os dados numa base de dados, para uso em análises subsequentes;

q) Arquitetura IoT no Edge é uma arquitetura de "ponta" do IoT que representa a conjugação de diversos elementos de hardware, software e comunicações que permitem a otimização de recursos como computação, armazenamento, rede e análise, a serem implementados mais próximo de onde os dados IoT são produzidos ou consumidos. A arquitetura no *edge* define como as informações são geradas, pelos sensores e terminais e são agregadas no *edge* da rede ou num *datacenter*;

r) Plataforma IoT, uma plataforma de Internet das Coisas (IoT) é um software que permite o desenvolvimento, implementação e gestão de soluções que se ligam e recolhem dados de endpoints de IoT para permitir melhores decisões ao nível do negócio. As capacidades funcionais incluem:

   - Gestão de dispositivos;
   - Integração;
   - Gestão de dados;
   - Analítica;
   - Ativação de aplicativos;
   - Segurança.

Pode ser entregue como uma combinação híbrida de uma plataforma de software de ponta e/ou, uma plataforma de IoT cloud como um serviço;

s) Internet das Coisas (IoT) é um bloco de construção central para negócios e plataformas digitais. O IoT é a rede de objetos físicos e dedicados que contem tecnologia incorporada para comunicar, medir ou interagir com seus estados internos e/ou o ambiente externo. O IoT compreende um ecossistema que inclui equipamentos ativos e produtos, protocolos de comunicação, aplicativos e dados e analítica;

t) Os veículos Autónomos, usam várias tecnologias de deteção e localização, como o lidar, radar, câmaras, GPS e dados de mapas, em combinação com a tomada de decisões baseada em IA, para conduzir sem intervenção humana;

u) Modelagem de informação de edifícios, do inglês *Building Information Modeling (BIM)* é o processo de gestão de dados e de informações, sobre instalações e infraestruturas físicas usando um conhecimento partilhado. Estes dados partilhados e recursos de conhecimento, apoiam a tomada de decisão desde o início da conceção à conclusão bem como captura de forma rastreável, as decisões e os resultados dessas decisões;

v) Gestão de Desempenho de Ativos, do inglês *Asset Performance Management (APM)*, compreende ferramentas de software e aplicativos para otimizar a disponibilidade dos ativos operacionais (como instalações, equipamentos e

infraestrutura) essenciais para a operação de uma empresa. O APM usa captura de dados, integração, visualização e análise para melhorar as operações, os tempos de manutenção e as atividades de inspeção para executar em ativos críticos. O APM inclui os conceitos de estratégia de ativos e gestão de risco, monitorização de condições, previsão preditiva e manutenção centrada na fiabilidade;

w) Alinhamento TI/TO, os sistemas de TI e TO (sistemas de controlo e processo industrial) existem na maioria das organizações com ativos de uso intensivo, como domínios separados. Alinhamento é o processo de validação de padrões, processos de suporte, segurança e arquitetura de planeamento para construir compatibilidade entre sistemas de TI e TO;
x) Serviços Geridos de Conectividade IoT, são também conhecidos como serviços geridos máquina a máquina (M2M), abrangem hardware, software, serviços de redes e serviços TI que geralmente são agrupados e geridos por um fornecedor externo. Estes serviços permitem que as empresas se liguem, monitorizem e controlem os ativos e os processos de negócio por meio de uma ligação fixa cabelada ou uma ligação sem fio. Estes serviços são essenciais para integrar sistemas autônomos e construídos de propósito, plataformas de IoT ou sistemas IT (por exemplo, ERP, CRM) e sistemas OT;
y) Integração IoT – A integração IoT refere-se aos requisitos de integração e tecnologias necessárias a instalar soluções de negócios, prontas para IoT que incluem desafios de integração específicos de IoT, como integração dispositivos IoT, dados IoT, *digital twins* e múltiplas plataformas IoT. Outro desafio de integração mais tradicional inclui, aplicativos corporativos e integração de dados, integração de processos de negócios, integração SaaS e integração do ecossistema B2B, bem como aplicativo móvel e integração de sistemas, mas antigos;
z) Localização Interna de Ativos, fornece informações sobre a localização física interna de dispositivos fixos ou móveis, wearables ou outros objetos. Esta informação é derivada de diferentes algoritmos que usam Wi-Fi, 5G, bem como infraestruturas de sobreposição, que incluem uma ou mais tecnologias, como Bluetooth, frequência muito alta (VHF), frequência ultra-alta (UHF), banda ultra larga (UWB), ultrassom, sonar, luz visível (VLC) / infravermelho (IR) ou *LiDAR.*

A janela temporal de elaboração deste trabalho, permitiu assim consagrar a análise da Gartner realizada em 2019, bem como a do presente ano 2020, conforme apresentado na Figura 18.

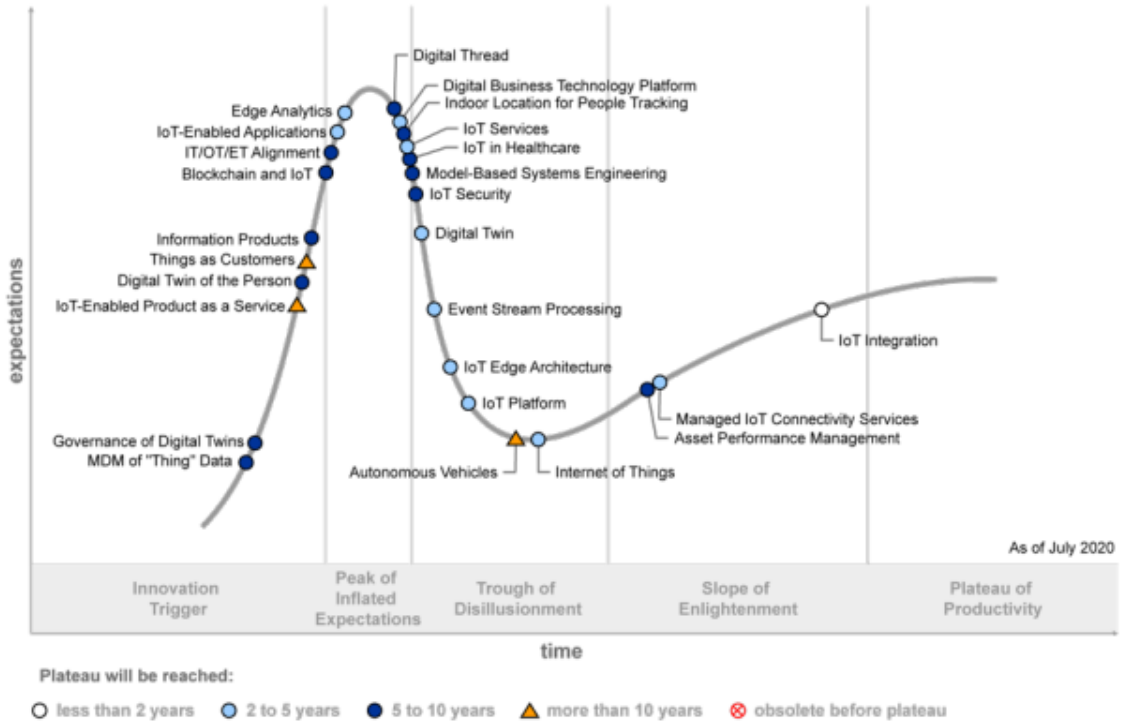



**Figura 18: Hype Cycle for Internet of Things 2020 [60]**

Neste *Hype de Cycle* de 2020 podemos assistir à emergência de alguns conceitos/tecnologias novas a começarem a singrar e que são apresentados de forma resumida na Tabela 4.

**Tabela 4: Matriz de Prioridades da Internet das Coisas, 2020 [60]**

| Benefícios | Menos de 2 anos | 2 a 5 anos | 5 a 10 anos | Mais de 10 anos |
|---|---|---|---|---|
| Transformação | | • Plataforma Tecnológica Digital de Negócio<br>• Digital Twins<br>• Processamento de fluxos de eventos<br>• Internet of Things<br>• Aplicações IoT-Enabled | • IoT e Blockchain<br>• Digital Twin da pessoa<br>• IoT na saúde<br>• Sistemas de engenharia baseados em modelos | • Veículos autónomos<br>• Produto IoT-Enabled as Service |
| Elevado | Integração Iot | • Analítica no Edge<br>• Arquitetura IoT no Edge<br>• Plataforma IoT<br>• Serviços IoT<br>• Serviços geridos de conectividade IoT | • Gestão de desempenho de ativos<br>• Tendências digitais<br>• Localização de pessoas no interior de edifícios<br>• Produtos Informativos<br>• Segurança IoT<br>• Alinhamento IT/OT/ET<br>• MDM dos dados das "Coisas" | • "Coisas" como clientes |
| Moderado | | | Governança dos Digital Twins | |
| Baixo | | | | |

Apresenta-se a decomposição do *Hype Cycle for the Internet of things, 2020*[60]*:*

a) MDM dos dados das "Coisas", é a aplicação da gestão dos dados principais. a prática, a disciplina e a capacidade tecnológica, no apoio do domínio dos dados de identificação da entidade habilitada de objetos para o IoT e os seus *digital-*

*twins*[2]. Permite a representação semântica dos dados principais da "coisa" através das arquiteturas distribuídas, IoT, OT e IT. O resultado permite a resolução da entidade do objeto, independentemente do aplicativo, sistema ou plataforma;

b) Governança de *Digital Twins* refere-se à supervisão e aos mecanismos necessários para garantir que os *Digital Twins*, entregam os benefícios de negócios pretendidos a um nível aceitável dos custos organizacionais e riscos corporativos ao longo do ciclo de vida física do "*Twin*";

c) IoT como Produto as a Service é um modelo que se enquadra no âmbito de produto como serviço, sendo que a organização adquire os equipamentos como ativos operacionais recorrentes;

d) *Digital Twin of the Person (DToP*), ou o "gémeo" digital da pessoa não apenas espelha um indivíduo único, mas também é uma multipresença sincronizada próximo do tempo-real do indivíduo, nos espaços digital e físico. Esta instanciação digital (ou múltiplas instanciações) de um indivíduo físico continuamente "entrelaça-se", atualiza, medeia, influencia e representa a pessoa em vários cenários, experiências, circunstâncias e personas;

e) "Coisas" como cliente, o cliente de uma coisa (ou máquina) é um ator econômico não humano que obtém mercadorias ou serviços em troca de pagamento. Os exemplos incluem assistentes pessoais virtuais, aparelhos inteligentes, carros conectados e equipamentos de fábrica habilitados para IoT. Esses clientes agem em nome de um cliente humano ou organização;

*f)* *Information Product*, ou produtos informativos, estes produtos são também conhecidos como produtos de dados, é uma oferta que diretamente monetiza dados ao gerar valor, receita ou outros benefícios financeiros. Inclui várias análises como licenciamento, troca ou partilha de dados e/ou informações que podem ser proprietárias ou, subprodutos das operações de negócio; ou disponibilizados pelo IoT ou outra instrumentação física de produtos e serviços; ou uma combinação de dados proprietários, públicos e exógenos;

g) *Blockchain* e IoT, endereça o uso do blockchain em conjunto com os dispositivos e tecnologias IoT. Integração do IoT e *Blockchain* no suporte de processos confiáveis multipartidários, que "ligam" o mundo físico das "coisas" ao processo do ambiente computacional do negócio;

h) Alinhamento TI/TO/TE, refere-se à orquestração das tecnologias da informação (TI), tecnologias operacionais (TO) e a tecnologia de engenharia (ET) para se apoiarem mutuamente por meio de padrões e regulamentação. Cada um desempenha um papel complementar, mas mutuamente reforçador, das outras duas tecnologias. Enquanto as TI registam transações e processos de negócios, a TO opera e monitora ativos industriais (por exemplo, soluções SCADA), e as TE é usado para definir, projetar, simular, analisar, visualizar e validar esses ativos (por exemplo, CAD / CAM);

i) As aplicações disponíveis para o IoT, são concebidas nativamente ou modernizadas para suporte direto do IoT como:

[2] Digital Twins – Representações virtuais de uma entidade

- É integrada com os dispositivos e plataformas na fronteira do IoT;
- Assimilação e análise dos dados e eventos do IoT no sentido de produzir uma descoberta e orquestrar uma resposta do negócio;
- Para garantir os itens acima utiliza *digital twins*;

j) Analítica no *edge*, é a disciplina que aplica a lógica (exemplo: regras) e matemática (algoritmos) aos dados de forma a disponibilizar informação para tomar melhores decisões;

*k)* Tendências Digitais, são uma estrutura para recolher, organizar, associar, rastrear e apresentar dados para múltiplos fatores. Múltiplos fatores esses, como design, produção, serviços e manutenção que influenciam um produto e/ou processo e as suas evoluções ao longo dos seus respetivos ciclos de vida. A integração e organização dos dados semanticamente ricos com tendências digitais, permitem que vários utilizadores possam aceder, integrar, organizar, rastrear e transformar dados técnicos, baseados em conhecimento diverso, oriundos de vários sistemas operacionais de nível empresarial;

l) Plataformas digitais de tecnologia digital, é a combinação de um conjunto de tecnologias que permitem uma organização participar num ecossistema digital. Integra plataformas existentes de IT, envolvimento do cliente, dados e analítica, sistema de parceiros e *Internet of Things* para "sentir" os eventos do negócio, decidir o que fazer e implementar uma resposta do negócio que cria valor aos envolvidos. Plataforma que partilha os ativos como os dados, algoritmos e transações com ecossistema de negócio de forma a mapear, criar e trocar serviços;

m) A localização interna para rastreamento de pessoas é uma necessidade de várias organizações, numa base de necessidade de segurança das mesmas ou numa perspetiva de produtividade. Os mercados verticais de localização de pessoas incluem clientes, empregados, crianças e idosos e dependem do resultado, sendo que cada um dos casos podem exigir o uso de tecnologia diferente no sentido de atingir o objetivo;

n) IoT na área da saúde, é um conjunto de dispositivos, aplicativos, equipamentos, aparelhos e edifícios que possuem inteligência e tecnologia para se ligarem, comunicarem e interoperarem uns com os outros, usando padrões dentro do ecossistema das TI's do provedor de saúde de "coisas inteligentes". O uso do IoT na saúde é fundamental para um sistema de saúde em tempo real;

o) Serviços IoT abrangem suporte, manutenção e serviços profissionais para fornecer um leque alargado do negócio e especialidade técnica no suporte dos planos IoT de criação e execução de serviços. Várias *frameworks*, metodologias e ativos estão dentro do âmbito dos serviços IoT. Os serviços IoT devem de ser vistos num âmbito mais amplo de "serviços digitais";

p) Sistemas de engenharia baseados em modelos, é uma abordagem digital para endereçar desafios, descrevendo esses desafios como modelos digitais. Estes modelos incluem relacionamentos entre as variáveis e sistemas, que influenciam comportamentos relevantes a serem compreendidos e melhorados. Os modelos podem variar desde o muito simples ligando algumas variáveis, até ao muito complexo ligando muitas variáveis;

q) Segurança na *Internet of Things* é parte da segurança digital. Funciona em conjugação com a segurança ciber física e, endereça iniciativa digitais envolvendo o IoT para o software, hardware, rede e proteção de dados. A segurança no IoT partilha muitas das tecnologias e processos das tecnologias de informação, tecnologias de operação e segurança física. Os controlos de segurança do IoT criam confiança, bem como disponibilizam segurança, fiabilidade, sistemas digitais privados e resilientes para o negócio digital;

r) "Gémeos Digitais" ou *Digital Twins,* são representações virtuais de uma entidade como um ativo, pessoa ou processo que é desenvolvida para suportar novos objetivos ou objetivos melhorados. Os três tipos de *digital Twins* são o discreto, o composto e o organizacional. Elementos necessários no sentido de responderem aos objetivos do negócio são, modelo, dados, associação um-para-um e monitorização, sendo elementos opcionais a analítica, controlo e simulação;

s) Processamento de fluxos de eventos. Um fluxo de eventos é uma sequência de objetos de eventos organizados por uma determinada ordem, normalmente por tempo. O processamento de fluxo de eventos (ESP) é a computação que é realizada nos objetos do evento, com a finalidade de integração dos dados de fluxo ou, análise de fluxo (também chamado de processamento de eventos complexos [CEP]). O ESP é normalmente aplicado aos dados conforme estes chegam (dados "em movimento"). O ESP fornece informações sobre ameaças emergentes, oportunidades de alertas "quase" em tempo-real, painéis de monitorização (denominados *dashboards*), processos de deteção e resposta e armazena os dados numa base de dados, para uso em análises subsequentes;

t) Arquitetura IoT no Edge. A arquitetura de ponta do IoT representa a conjugação de diversos elementos de hardware, software e comunicações que permitem a otimização de recursos como computação, armazenamento, rede e análise, a serem implementados mais próximo de onde os dados IoT são produzidos ou consumidos. A arquitetura no *edge* define como as informações são geradas, pelos sensores e terminais e são agregadas no *edge* da rede ou num *datacenter*;

u) Plataforma IoT, uma plataforma de Internet das Coisas (IoT) é um software que permite o desenvolvimento, implementação e gestão de soluções que se ligam e recolhem dados de *endpoints* de IoT para permitir melhores decisões ao nível do negócio. As capacidades funcionais incluem:

   - Gestão de dispositivos;
   - Integração;
   - Gestão de dados;
   - Analítica;
   - Ativação de aplicativos;
   - Segurança;

Pode ser entregue como uma combinação híbrida de uma plataforma de software de ponta e/ou, uma plataforma de IoT cloud como um serviço;

v) Os veículos Autónomos, usam várias tecnologias de deteção e localização, como o lidar, radar, câmaras, GPS e dados de mapas, em combinação com a tomada de decisões baseada em IA, para conduzir sem intervenção humana;
w) Internet das Coisas (IoT) é um bloco de construção central para negócios e plataformas digitais. O IoT é a rede de objetos físicos e dedicados que contem tecnologia incorporada para comunicar, medir ou interagir com seus estados internos e/ou o ambiente externo. O IoT compreende um ecossistema que inclui equipamentos ativos e produtos, protocolos de comunicação, aplicativos e dados e analítica;
x) Gestão de Desempenho de Ativos, do inglês *Asset Performance Management (APM)*, compreende ferramentas de software e aplicativos para otimizar a disponibilidade dos ativos operacionais (como instalações, equipamentos e infraestrutura) essenciais para a operação de uma empresa. O APM usa captura de dados, integração, visualização e análise para melhorar as operações, os tempos de manutenção e as atividades de inspeção para executar em ativos críticos. O APM inclui os conceitos de estratégia de ativos e gestão de risco, monitorização de condições, previsão preditiva e manutenção centrada na fiabilidade;
y) Serviços Geridos de Conectividade IoT, são também conhecidos como serviços geridos máquina a máquina (M2M), abrangem hardware, software, serviços de redes e serviços TI que geralmente são agrupados e geridos por um fornecedor externo. Estes serviços permitem que as empresas se liguem, monitorizem e controlem os ativos e os processos de negócio por meio de uma ligação fixa cabelada ou uma ligação sem fio. Estes serviços são essenciais para integrar sistemas autônomos e construídos de propósito, plataformas de IoT ou sistemas IT (por exemplo, ERP, CRM) e sistemas OT;
z) Integração IoT – A integração IoT refere-se aos requisitos de integração e tecnologias necessárias a instalar soluções de negócios prontas para IoT que incluem desafios de integração específicos de IoT, como integração dispositivos IoT, dados IoT, *digital twins* e múltiplas plataformas IoT. Outro desafio de integração mais tradicional inclui, aplicativos corporativos e integração de dados, integração de processos de negócios, integração SaaS e integração do ecossistema B2B, bem como aplicativo móvel e integração de sistemas, mas antigos.

## 3.2. Síntese

Este capítulo, pretende apresentar as tendências associadas à Internet das Coisas. As tendências endereçam janelas temporais distintas, como curto prazo (2 a 5 anos), médio prazo (5 a 10 anos) e longo prazo (mais de 10 anos).

Nestas tendências, assiste-se a uma consolidação de tecnologias, como *blockchain*, inteligência artificial, o movimento de realização de analítica no *edge* e, o uso mais consistente das representações virtuais *Digital Twins.*

A análise de 2020 apresenta assim um espetro mais focada numa pesquisa que suporta a análise e planeamento dos autores, reduzindo desta forma o número de perfis de inovação verificados no *Hype Cycle*. Esta revisão levou à remoção dos seguintes perfis da análise de 2020:

- Construção de informação modelada;
- AI no Edge;
- Event broker PaaS (ebPaaS);
- Localização no interior de ativos;
- Infonomics;
- Internet of meat;
- Soluções de negócio IoT;
- Alinhamento IT/OT.

As tecnologias chave, na janela temporal de dois a cinco anos para o IoT incluem:

- Digital Twin;
- Analítica no Edge;
- Processamento de eventos de stream;
- Arquitetura IoT no edge;
- Plataforma IoT;
- Serviços geridos de conectividade IoT.

# 4. Indústria 4.0

O presente capítulo faz uma análise da evolução da indústria 1.0, até à Indústria 4.0 com as tecnologias emergentes e as plataformas *Cyber Physical System* ou seja os sistemas ciber-fisicos, decorrentes desta evolução. São também abordados os diferentes protocolos usados ao nível dos sistemas indústriais e analisados diferentes modelos, i.e. modelos de maturidade e modelo de arquitetura aplicado à Indústria 4.0

## 4.1. Evolução Industrial

O desenvolvimento da tecnologia ao longo dos tempos, representou um grande papel para o desenvolvimento global e na prosperidade das economias e consequentemente, nos países. A Revolução Industrial iniciou-se por volta do ano 1750 (Primeira Revolução Industrial), onde a produção mecânica fabril foi melhorada em termos de produtividade com a implementação do motor a vapor, associado à expansão da indústria têxtil do algodão. Um século mais tarde por volta de 1850 assistiu-se à Segunda Revolução Industrial, com a introdução da eletricidade, linhas de montagem, associado à produção em massa, assente na divisão do trabalho, etc.

A Terceira Revolução Industrial ocorre no século dezanove, com a automatização da produção, com a eletrónica, dando origem a uma fase inicial tecnologias de informação com a introdução da robótica. Estas inovações permitem a integração do CN (Controlo Numérico), CNC(Controlo de Computação Numérica) e DNC (Controlo Numérico Direto).

O controlo numérico (CN) assegura que as funções das máquinas possam ser controladas por letras, número e símbolos. Este tipo de controlo permite a obtenção de vantagens significativas como:

- Redução do ciclo de produção;
- Operações complexas de maquinaria;
- Elevado nível de precisão;
- Menor necessidade de inspeção;
- Redução dos erros humanos;
- Aumento da produtividade;
- Redução de desperdício;
- Aumento da eficiência das operações;
- Redução do conhecimento técnico do operador;

Por outro lado, tinha algumas limitações ao nível de:

- Elevados investimentos;
- Esforços de manutenção mais elevados;
- Necessidade de programadores com mais conhecimentos;
- Necessidade de maior intensidade de utilização;

A Quarta Revolução Industrial ou, Indústria 4.0 (I4.0) comparativamente às revoluções industriais anteriores, tem uma evolução exponencial em vez de uma evolução linear. Esta "explosão" ocorre face ao resultado de vivermos num mundo altamente globalizado e ligado a nível tecnológico, tecnologia essa que tem um efeito catalisador no sentido de criar mais tecnologia, potenciando esta "explosão" tecnológica.

Existe uma considerável sobreposição entre o conceito Indústria 4.0 desenvolvido na Alemanha e, o *Industrial Internet of Things*, desenvolvido nos Estados Unidos.

"… a internet industrial é uma internet de coisas, máquinas, computadores e pessoas permitindo operações industriais inteligentes, usando análise de dados avançada para resultados de negócios transformadores …" [17]

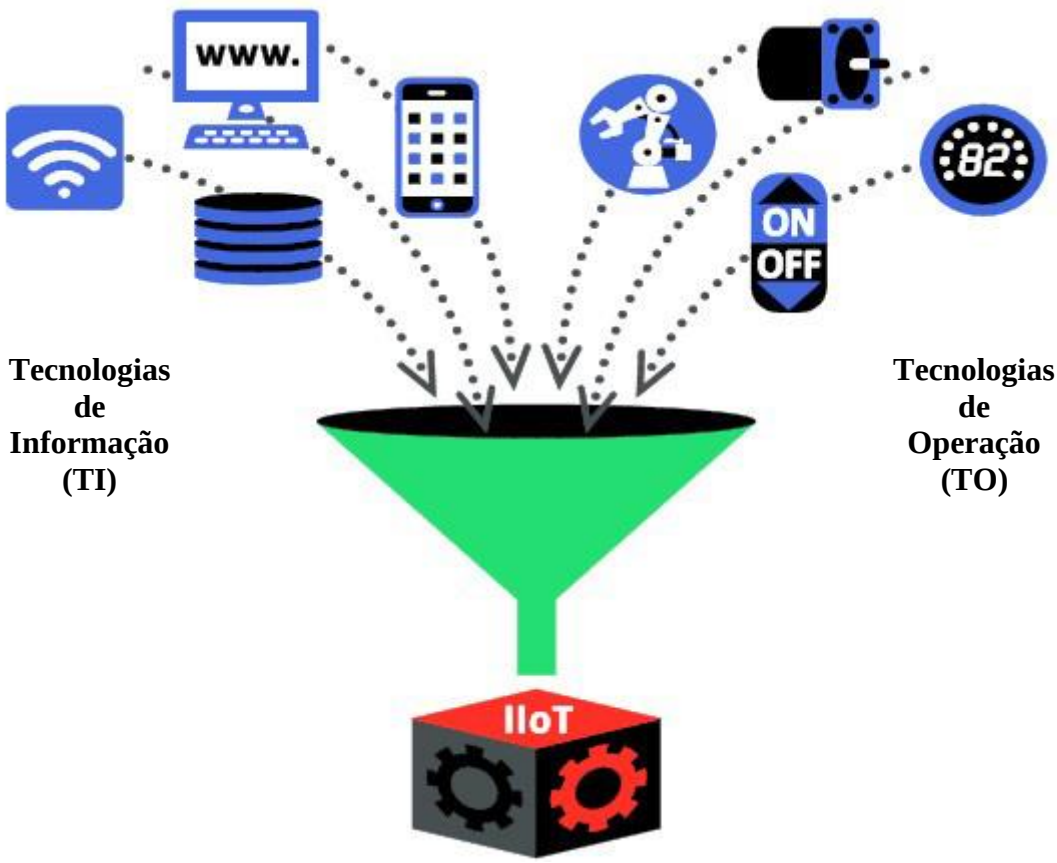



**Figura 19: Convergência IT/OT**

A convergência das TO e das TI's, (cf. Figura 19) requer aqui, que sejam ultrapassadas algumas barreiras, pelo facto de terem prioridades e objetivos antagónicos. As TO priorizam a disponibilidade das linhas de produção, enquanto as TI's priorizam a confidencialidade da informação ao nível da propriedade intelectual. A necessidade desta

convergência vai requerer que estas unidades, numa determinada altura no tempo, tenham de se alinhar em torno de um bem maior i.e., os objetivos da organização.

O termo Indústria 4.0 foi usado pela primeira na Alemanha na feira de Hannover em 2011[18] e tem tido fortes desenvolvimentos desde essa altura. O principal conceito saído da Indústria 4.0 passa pela integração das linhas de produção, também conhecido como "chão de fábrica" com as tecnologias emergentes e, os sistemas ciber-físicos (CPS - Cyber Physical System)[3] melhorando e promovendo as comunicações entre humanos, as máquinas de produção física e os sistemas de planeamento de recursos, também conhecidos como ERP (Enterprise Resource Planning).

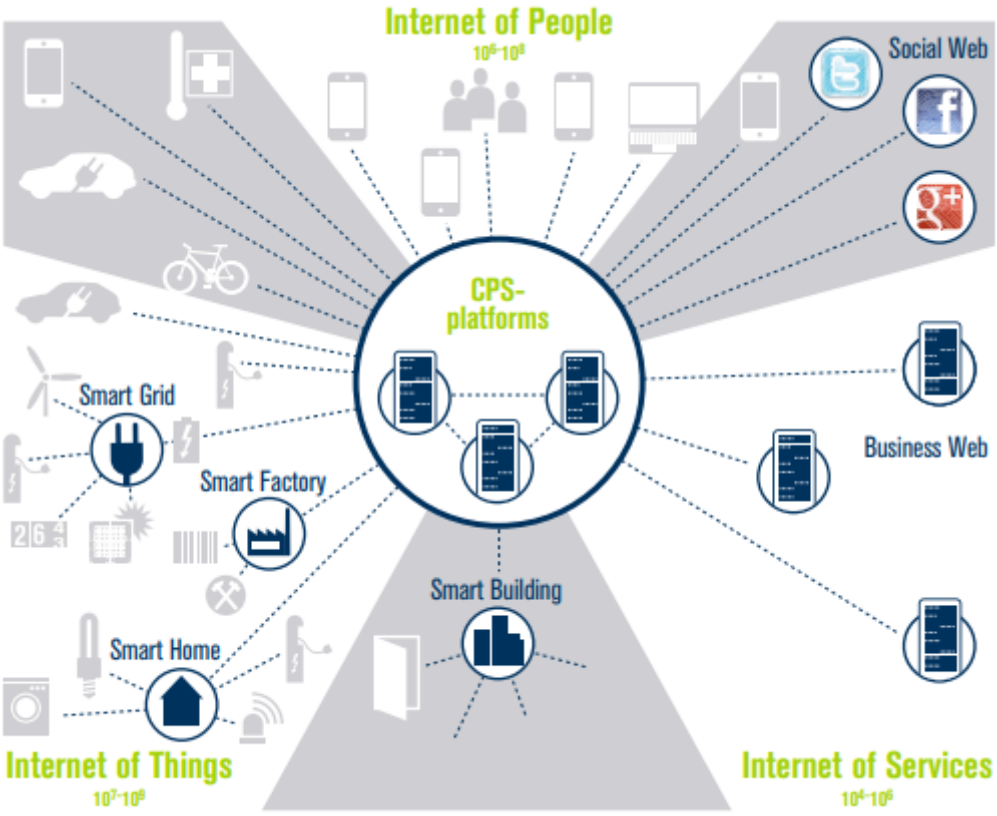



**Figura 20: Internet das Coisas e Serviços – Rede de pessoas, objetos e sistemas [19]**

O ecossistema das plataformas CPS conforme apresentado na Figura 20, agregam vários ambientes no seu perímetro, como a Internet das Coisas, (que incluem debaixo do acrónimo de IoT, os edifícios inteligentes, as fábricas inteligentes, as casas inteligentes e as redes inteligentes). A Internet das pessoas, por sua vez agregam as ligações das pessoas à componente das redes sociais como, Facebook, Instagram, Linkedin, entre outras. A Internet dos serviços, foca a componente dos serviços, por exemplo as plataformas como serviços (PaaS – *Platform as a Service*), software como serviços (SaaS – *Software as a Service*).

[3] Nos sistemas de produção, os sistemas ciber-físicos, incluem máquinas inteligentes, sistemas de arquivo e, estas instalações de produção são capazes de forma autónoma de trocarem informação, despoletarem ações e conseguirem exercer esse controlo independente.

Estes desenvolvimentos levaram a que fosse possível de monitorizar a produção em massa, em tempo real, com a digitalização de todo o estado de produção nas diferentes fábricas existentes em diferentes países. Esta evolução, permite a obtenção de informação analítica com a possibilidade de preditividade de potenciais problemas, que possam ocorrer ao nível dos equipamentos (máquinas) e/ou na capacidade de produção.

A Indústria 4.0, tem um potencial grande no sentido de endereçar e resolver alguns dos desafios que o mundo enfrenta nos dias atuais, como eficiência de recursos e energética, produção urbana e alterações demográficas. A indústria 4.0 garante a continuidade de produtividade ao nível dos recursos, com a eficiência a ser entregue através da totalidade da cadeia de valor. Esta I4.0 permite que o trabalho seja organizado de forma a ter em consideração as alterações demográficas e também os fatores sociais.

## 4.2. Protocolos Industriais integrados nos *smart buildings*

O ciclo de vida destes dispositivos (industriais) é único, uma vez que por norma tem um período de substituição mais alargado (por vezes superiores a 30 anos) e que por norma são geridos, pelas tecnologias de operação, sendo que por outro lado as tecnologias de informação, tem ciclos de vida mais curtos nos seus equipamentos, como por exemplo, os computadores e/ou dos *smartphones*, que rondam entre três a cinco anos.

Ao analisarmos um ambiente organizacional heterogéneo, como por exemplo a sede de uma organização, podemos identificar uma multiplicidade de equipamentos, industriais bem como equipamentos do âmbito das tecnologias de informação. Ao nível dos sistemas industriais temos todos os equipamentos, como sistemas de HVAC, sistemas de tratamento de iluminação, sistemas de energia (renováveis), sistemas de tratamento de águas. As tecnologias de informação endereçam as soluções de redes de comunicações, servidores, computadores, telefonia, entre outros a Figura 21, apresenta um conjunto de diferentes tecnologias, que são usadas ao nível dos *smart buildings.*

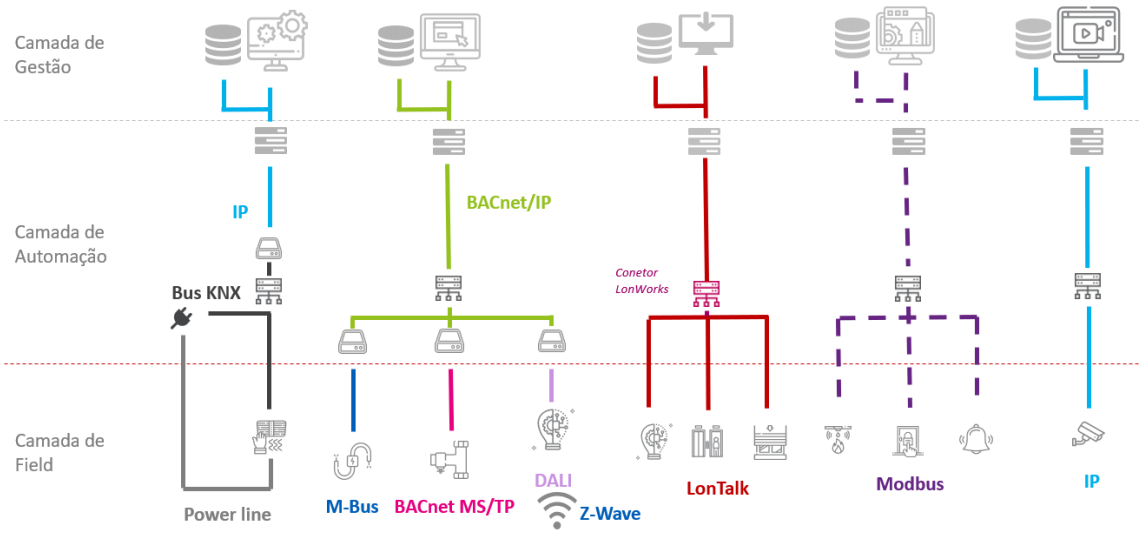



**Figura 21: Exemplos de diferentes tecnologias usadas em Smart Buildings**

**IP (Internet Protocol)** – O *Internet Protocol (IP)* ou protocolo de Internet foi concebido para uso em sistemas interligados de redes de comunicações de computadores. Este protocolo implementa duas funções básicas, o endereçamento e a fragmentação. O módulo de internet usa o endereçamento para a transmissão de datagramas em direção ao destino. A seleção do caminho de transmissão é definido como *routing*. O módulo de internet usa os campos de cabeçalho, para fragmentar e reagrupar os datagramas internet quando necessário para transmissão de "pequenos pacotes" na rede[20].

Um datagrama conforme Figura 22, está dividido em duas áreas, uma área de cabeçalho e outra de dados. O cabeçalho contém toda a informação necessária que identifica o conteúdo do datagrama. A área de dados encapsula o pacote do nível superior, ou seja, um pacote TCP ou UDP.

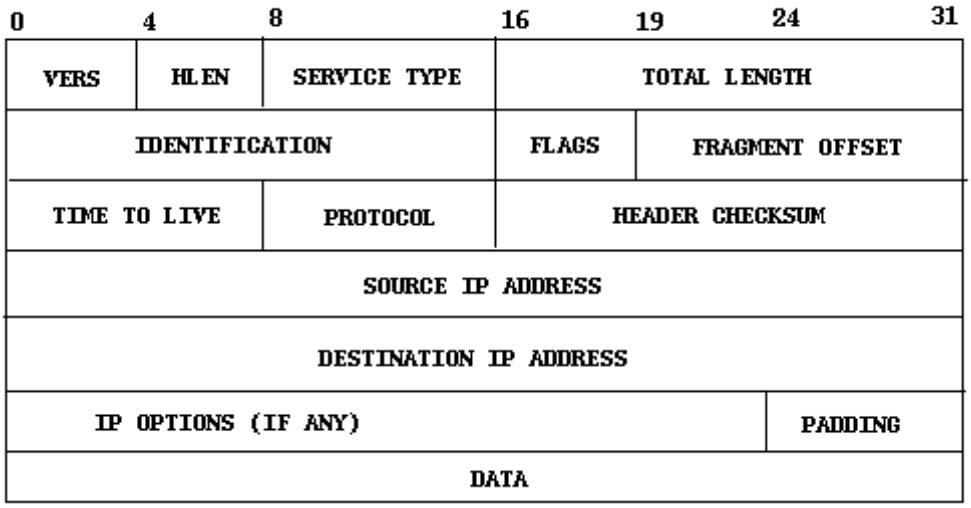



**Figura 22: Formato do datagrama IP [21]**

**BACnet/IP** – Este protocolo (*BAC – Building Automation and Control Networks*) foi criado pela associação de fabricantes e utilizadores *ASHRAE ( American Society of Heating, Refrigerating and Air-Conditioning Engineers)*, com foco no ar nos sistemas de ar condicionado (*HVAC – Heating Ventilation and Air Conditioning*).[22]

**LonWorks** – É uma plataforma usada nas infraestruturas dos edifícios para disponibilizar uma infraestrutura comum, para todos os sistemas desses edifícios (HVAC, iluminação, controlo de acessos, sistemas de alarme, elevadores, estores automáticos) usando um protocolo comum *(CNP – Control Network Protocol)* nos dispositivos a interligar nesse edifício. Protocolo proprietário desenvolvido pela *Echelon Corp.*[23]

**Bus KNX** – Teve origem em 1999 com a criação da *KNX Association cvba*, que incluía na sua origem a EIBA ( *European -Instalation Bus Association) a EHSA (European Homes System Association)* e a *BCI (BatiBUS Club International).* O KNX é um protocolo assente em linhas de energia (*power line*), que surge da necessidade de interoperabilidade entre diferentes fabricantes (sistemas de aquecimento, iluminação e

sistemas de controlo) no mercado residencial. Este protocolo deixou de ser proprietário a partir de 2016[24].

**Power Line** – É um standard que permite a transmissão de comunicações sobre as linhas de energia.(IEEE 1901-2010)[25].

**M-Bus** – M-Bus ou Meter Bus é um standard europeu (EN 13757-2 Camada física ou de comunicações, EN 13757-3 camada aplicacional) para a leitura dos contadores de água, luz ou gás. Este Meter Bus é também usada em outros tipos de leitura de consumos. O interface M-Bus é desenvolvido para comunicações de dois fios, garantindo o custo beneficio[26].

**BACnet MS/TP** – É um protocolo de comunicações por norma usado ao nível da automação de edifícios e na indústria HVAC (aquecimento, ventilação e ar condicionado). Este protocolo permite a comunicação de equipamentos de ar condicionado, sistemas de ventilação com sistemas PLC (Programmable Logic Controller)[4]. MS/TP (Master-Slave / Token Passing) usa a passagem de tokens para comunicar entre os dispositivos. Dispositivos "mestres" colocam solicitações de serviço, apenas se tiverem um token. Dispositivos "escravos" enviam respostas a essas solicitações e não precisam de um token para enviar suas respostas. MS / TP está geralmente suportado em rede de cobre a 2 fios, frequentemente usado ao nível dos equipamentos [27].

**Z-Wave** – É uma tecnologia sem fio segura que opera com pouca energia e não interfere com as redes sem fio tradicionais, por funcionar em frequências mais baixas. Esta tecnologia permite a comunicação de dispositivos como iluminações, fecho de portas, termostatos[28].

**LonTalk** – É um protocolo concebido para comunicações em redes de controlo. Estas redes são caraterizadas por mensagens curtas (poucos bites), custo muito baixo por nó, múltiplos meios de comunicação, baixa largura de banda, baixa manutenção, equipamentos de múltiplos vendedores e custos de suporte reduzidos[29].

**Modbus** - O protocolo Modbus é uma estrutura de mensagens desenvolvida pela Modicon em 1979. É usado para estabelecer a comunicação cliente-servidor entre dispositivos inteligentes. É um padrão, verdadeiramente aberto e o protocolo de rede mais usado no ambiente de produção industrial[30].

Estes sistemas mais antigos, com ciclos de substituição prolongados no tempo, refletem a possibilidade de existência de vetores de ataque nos sistemas embebidos com vulnerabilidades de segurança.

[4] PLC – É um computador com um microprocessador, usada na automação industrial, que pode automatizar processos específicos, função de uma determinada máquina ou, uma linha de produção na sua totalidade.

## 4.3. Sistemas de controlo Industrial (ICS)

Os Sistemas de Controlo Industrial (ICS) inserem-se num conjunto alargado de sistemas usados para disponibilizar funcionalidades de controlo e monitorização nas instalações de equipamentos de produção e equipamentos industriais. Um sistema ICS agrega uma variedade de sistemas incluindo Processos de Controlo de Sistemas (PCS), Sistemas de controlo Distribuído (DCS), sistemas de Controlo Supervisionado e Aquisição de Dados (SCADA), Sistemas Instrumentalizados de Segurança (SIS) e muitos outros.

A Figura 23 é uma representação simplificada de um sistema ICS, composto por controladores e um conjunto de entradas e saída de dados ligados, válvulas, manómetros, motores, entre outros, funcionando todos em conjunto de forma a automatizarem tarefas.

As tarefas são controladas por uma aplicação ou, a serem executas de forma lógica no interior de um controlador, com painéis de visualização local, ou são usados interfaces homem-máquina (HMI), de forma a disponibilizar uma "vista" do controlador, permitindo ao operador, verificar os valores realizando alterações na forma como o controlador está a funcionar.

Os ICS, tipicamente incluem kits de ferramentas, para criação de processos lógicos, que definem tarefas, bem como permite a criação customizada de interfaces de operador ou interfaces gráficas de utilizador, implementados em interfaces homem-máquina.

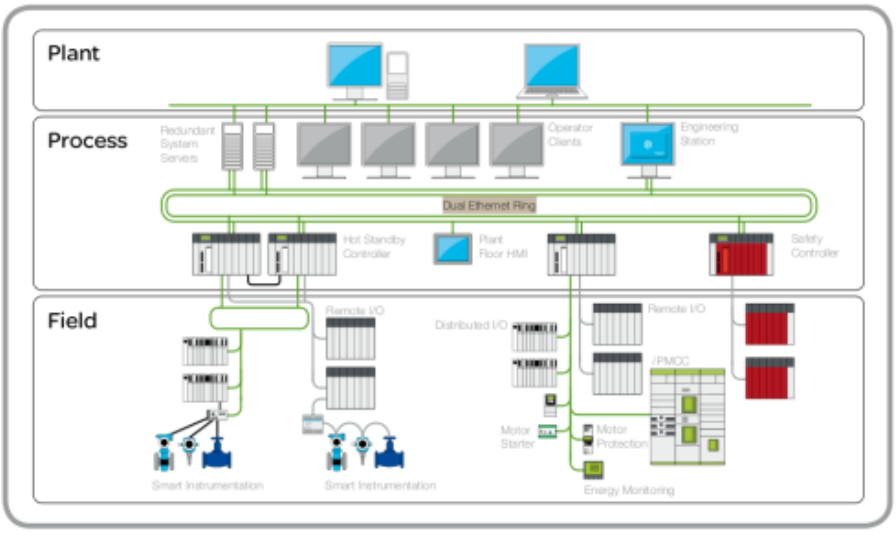



**Figura 23: Sistema ICS [31]**

No início existiam diferenças significativas entre as arquiteturas de DCS e os sistemas SCADA. Com a evolução da tecnologia estas diferenças esbateram-se, levando a que exista frequentemente uma "névoa" onde determinado sistema ICS é de facto classificado como DCS ou SCADA.

Ambos os sistemas são concebidos para monitorizar (leitura de dados) e apresentá-los ao operador humano e simultaneamente a outras aplicações, como *Historians*

(Historiadores) aplicações de controlo avançado e para controlo (definição de parâmetros e instruções de execução) de equipamento de produção ou industrial.

Basicamente são arquiteturas que podem variar de fabricante para fabricante, mas de um modo geral incluem aplicações e ferramentas necessárias para gerar, testar, implementar, monitorizar e controlar um processo automatizado.

Estes sistemas inserem-se numa perspetiva em termos de enquadramento de ferramentas multifacetadas o que significa que, uma estação de trabalho pode ser usada com o objetivo de ficar apenas num modo de supervisão (modo de leitura), permitindo uma análise qualitativa do trabalho produzido, enquanto outra estação de trabalho pode ser usada para otimização de um processo lógico, onde escreve programas novos para um controlador, enquanto uma terceira estação de trabalho pode ser usada como um interface de controlo centralizado para controlar um processo que possa requer mais intervenção humana, conferindo-lhe um papel ao nível de interface homem-máquina (HMI).

## 4.4. Modelos e Arquiteturas aplicadas à Indústria 4.0

### 4.4.1 Modelo de Arquitetura de Referência para a Indústria 4.0

O RAMI 4.0 ( *Reference Architecture Model Industrie* 4.0) [32], foi desenvolvido por uma associação alemã de fabricantes de material eletrónico e elétrico, para suportar os desenvolvimentos na Indústria 4.0, sendo que este modelo RAMI 4.0, foi ganhando preponderância a nível mundial.

O modelo RAMI 4.0 é um mapa tridimensional conforme apresentado na Figura 24, que apresenta de forma estruturada a abordagem à Indústria 4.0. Este modelo pretende criar uma *framework* por forma a garantir que todos os envolvidos nas atividades e discussões sobre o tema Indústria 4.0 tem uma plataforma comum.

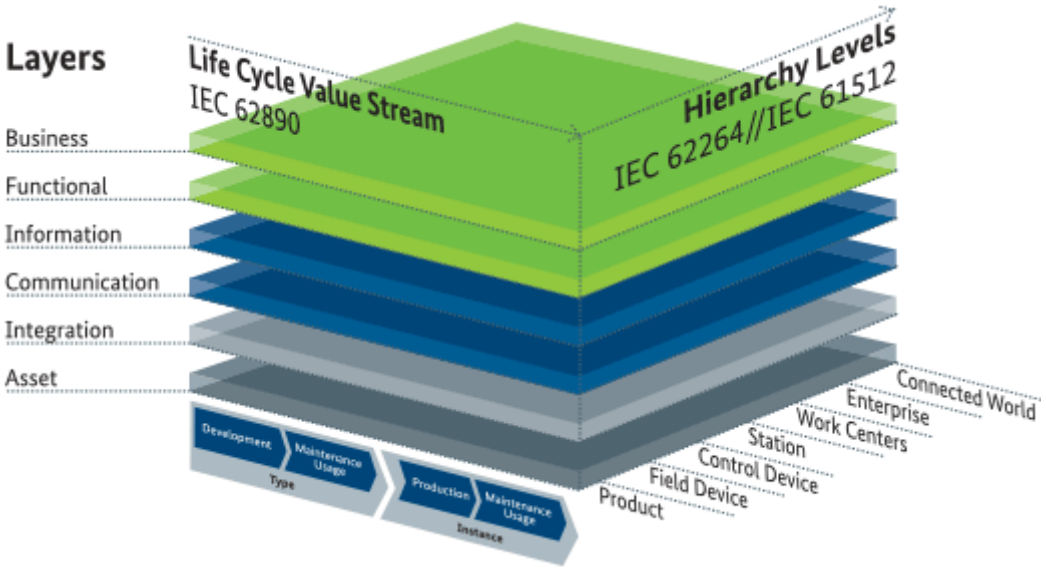



**Figura 24: Modelo de Arquitetura de Referência para a Indústria [32]**

Este modelo apresentado na Figura 24, é composto por três níveis, o nível Hierárquico da fábrica (*Hierarchy Level*), o nível do Ciclo de Vida do Produto (Primeira Dimensão "*Life Cycle Value Stream*") e o nível de Arquitetura ("*Layers*" que agrega conteúdos compatíveis)

O modelo RAMI 4.0, apresenta os seguintes benefícios;

- Arquitetura orientada aos serviços;
- Conjuga todos os elementos e componentes das TI's, numa camada e o modelo de ciclo de vida;
- Decompõe os processos complexos em pacotes simplificados em termos de entendimento, incluindo a privacidade de dados e a segurança das TI's.

O nível Hierárquico da fábrica é composto pelas camadas, produto, dispositivos de campo, estação de trabalho, centro de trabalho e a organização, conforme apresentado na Figura 25.

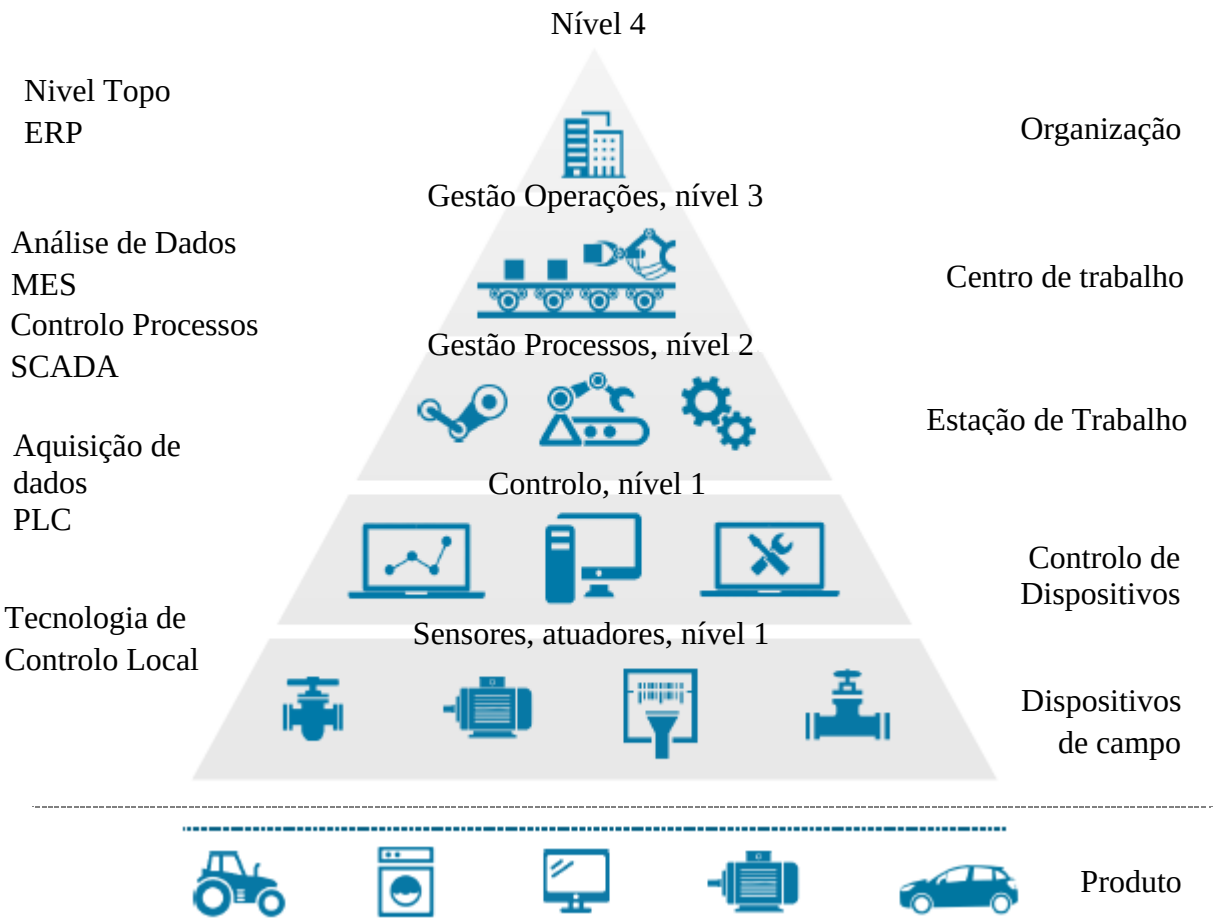



**Figura 25: Nível hierárquico da fábrica**

Fonte: Adaptado[32] gráfico Ana Salari desenhado por Freepik

Comparativamente a indústria 3.0 estava assente em:

- Estrutura baseada em hardware;
- As funções estão diretamente vinculadas ao hardware;
- Hierarquia baseada em comunicação;
- Produto é isolado.

Por outro lado, a indústria 4.0 assenta em cima:

- Sistemas e máquinas mais flexíveis;
- Funções estão distribuídas ao longo da rede;
- A rede pode passar as fronteiras da organização;
- Participantes interagem ao longo dos níveis hierárquicos;
- Todos os participantes são capazes de comunicar uns com os outros;
- Produto faz parte da rede.

A Figura 26, representa o papel da fábrica "flexível" no contexto da Indústria 4.0, onde faz a "ponte" entre a produção e a ligação ao mundo exterior. O ecossistema da fábrica num princípio de transformação digital, interage com os diferentes sistemas (Controlo de dispositivos, estações de trabalho, dispositivos de campo, CRM, ERP, etc.), existentes na fábrica "flexível". Esta interação coloca a fábrica no centro do processo em termos de conexão entre o produto e as plataformas e sistemas na WAN.

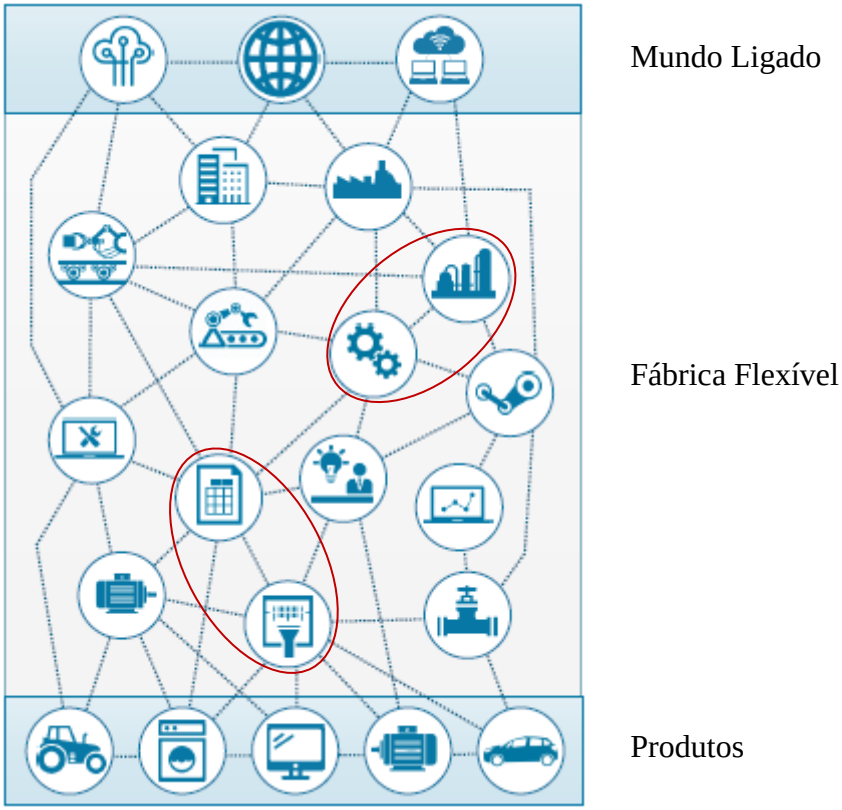



**Figura 26: Hierarquia da fábrica**
Fonte: Adaptado[32] gráfico Ana Salari desenhado por Freepik

A primeira dimensão “Life Cycle Value Stream” endereça o ciclo de vida do produto, conforme apresentado na Figura 27.


**Figura 27: Ciclo de vida do produto**
Fonte: Adaptado[32]

### Camada Tipo

A camada “Tipo” é sempre criada com a ideia inicial, ou seja, assim que o produto integra a fase de desenvolvimento. A fase inicial “Desenvolvimento” na camada “Tipo”, carateriza-se pela elaboração de um plano que inclui:

- Desenvolvimento;
- Construção;
- Simulação;
- Protótipo.

Ainda dentro da camada “Tipo”, é definido o modelo da manutenção no campo “Uso manutenção”, caraterizado por:

- Atualizações de software;
- Manuais de instruções;
- Alterações ao produto.

### Camada Instância

Esta camada ocorre na sequência da produção industrializada dos produtos, que tem por base a tipificação geral. Cada produto produzido, representa em si uma instância desse, tipo sendo identificados, de forma inequívoca por um número de série, único. As instâncias são vendidas e entregues aos clientes.

Para o cliente os produtos são numa primeira fase apenas “tipos”. Os produtos tornam-se “instâncias” quando são instalados num sistema em particular. A mudança de “tipo” para “instância” pode ser repetida diversas vezes.

A fase “Produção” dentro da camada “Instância” é caraterizado por:

- Produção do produto;
- Qualidade dos dados;
- Números de série.

O modelo de manutenção “Uso manutenção”, na camada “Instância” é caraterizado por serviços como:

- Otimização da manutenção;
- Atualizações;
- Despistagem de problemas;
- Reciclagem.

A segunda dimensão é a camada de Arquitetura de “Layer” de negócio. As camadas individuais e as suas inter-relações são descritas abaixo:

**Camada de negócio**

- Assegura a integridade das funções nos fluxos de valor;
- Mapeia os modelos de negócio resultantes do processo global;
- Condições de regulação com base legal;
- Modelação de regras que o sistema tem de cumprir;
- Orquestração de serviços na camada funcional;
- Ligação entre diferentes processos de negócio;
- Recebe eventos para processos avançados de negócio.

**Camada Funcional**

- Descrição formal das funções;
- Plataforma para integração horizontal de diversas funções;
- Ambiente de modelagem e tempos de execução, que suportam processos de negócios;
- Ambiente para aplicações de funcionalidades técnicas.

**Camada de Informação**

- Ambiente de execução de pré-processamento de eventos;
- Execução de regras relacionadas com eventos;
- Descrição de formal de regras;
- Contexto pré-processamento de eventos. Nesse contexto as regras são aplicadas a um ou mais eventos, para gerar um ou mais eventos adicionais, que em seguida inicia o processamento da camada funcional;
- Persistência de dados que representam os modelos;
- Confirmação da integridade dos dados;

- Integração consistente dos diferentes dados;
- Obtenção de novos dados de elevada qualidade (dados, informação, conhecimento);
- Fornecimento de dados estruturados por meio de interfaces de serviço;
- Recebimento de eventos e a sua transformação por forma a combinar os dados disponíveis para a camada Funcional.

**Camada de Comunicação**

- Padronização da comunicação, usando um formato de dados uniforme na direção da camada de Informação;
- Provisão de serviços para controlo da camada de Integridade.

**Camada de Integração**

- Fornecimento de informações sobre os ativos (componentes físicos, hardware, documentos, software, etc.), num formulário que pode ser processado por computador;
- Controlo assistido por computador do processo técnico;
- Geração de eventos dos ativos;
- Contém elementos ligados às tecnologias da informação com leitores RFID, sensores HMI;

Interação com humanos ocorre a este nível por exemplo através do HMI, ou interface homem-máquina.

### Camada de Ativos

- Representa a realidade, i.e. componentes físicas, como eixos lineares, peças de metal, documentos, diagramas de circuitos, ideias e arquivos;
- Os humanos começam a ser também parte da camada de ativos e são ligados ao mundo virtual através da camada de integração;
- Conexão passiva dos ativos com a camada de integração, por exemplo através dos códigos QR.

A Figura 28 apresenta em resumo, a conclusão do anteriormente apresentado.


**Figura 28: Arquitetura**
Fonte: Adaptado[32]

## 4.5. Modelos de Maturidade

Os modelos de maturidade são ferramentas que permitem avaliar a situação corrente e os requisitos da Indústria 4.0 em diferentes áreas, sendo avaliados o modelo SIMMI 4.0 (System Integration Maturity Model Industry 4.0) [33] e o modelo SIRI (Smart Industry Readiness Index) [34].

### 4.5.1. Modelo de Maturidade de Integração de Sistemas para a Indústria 4.0

Este modelo SIMMI 4.0 [33], desenvolvido pela Universidade Técnica de Dresden, permite que as empresas possam obter uma classificação, por forma a percecionarem o estágio em que se encontram, em relação à Indústria 4.0. Este modelo é composto por cinco etapas, onde cada uma destas etapas descrevem diferentes caraterísticas da digitalização e, que permite às empresas realizar uma autoavaliação.

Adicionalmente cada etapa de maturidade é dividido em quatro dimensões, que representam os diferentes níveis de foco.

**A dimensão 'vertical'**, é uma dimensão que foca nos componentes do nível mais baixo da organização, onde as diferentes coisas físicas (produtos, máquinas, etc.) necessitam de trocar informação neste nível e, com os níveis acima deste.

**A dimensão 'horizontal'**, é uma dimensão que garante a integração horizontal através das diferentes redes, reforça a capacidade do fluxo de informações ao longo de diferentes sistemas de planeamento organizacional (ERPs) em diferentes partes interessadas, como clientes globais, material e fornecedores.

**A Dimensão 'desenvolvimento digital de produto'**, foca na capacidade de representação digital de cada um dos passos a executar. Para a realização deste propósito, pelo menos um dos sistemas empresariais deve de ser integrado em cada etapa respetiva do processo, como resultado os dados e a informação obtida em cada uma das etapas deve de ser reencaminhada a próxima etapa do sistema empresarial.

**A Dimensão de 'critérios de tecnologia de seção transversal'**, esta dimensão, foca-se na avaliação do uso das tecnologias usadas, em todos os diferentes campos da indústria 4.0.

Com base nos requisitos, os respetivos avaliados em termos de campos são: Arquitetura orientada a serviços (SOA – *Service Oriented Architecture*), computação na *cloud*, *big data*, e segurança de TI's. Além disso, o nível de apoio que os sistemas empresariais podem fornecer nestes campos, devem de ser avaliados nesta dimensão.

### Etapas do Modelo de Maturidade de Integração de Sistemas para a Indústria 4.0

O SIMMI 4.0 está segmentado em cinco etapas[35], onde cada uma dos etapas é composta por atividades chave, que devem de ser concluídas com o objetivo de atingir uma etapa mais elevado, sendo um dos pilares para as bases, na Indústria 4.0.

### Etapa 1 – Digitalização básica

Nesta etapa a empresa não endereçou o conceito Indústria 4.0. Os requisitos não são totalmente, ou parcialmente cumpridos. Os sistemas empresariais ao longo da cadeia de valor, apenas suportam, os seus campos de atividade. Quando esta integração é alcançada é assente numa implementação de interfaces complexa.

A criação de protótipos é desenvolvida de uma forma onerosa, porque não existem atividades de desenvolvimento de produto, digitalizados. A empresa não tem como objetivo o foco nos serviços nem tem orientações a estratégias na *cloud*.

Os dados dos sistemas empresariais são agregados, apenas para decisões estratégicas, adicionalmente a confidencialidade dos dados, não é fornecida. Os dados da empresa não se encontram protegidos contraespionagem industrial, levando a elevados custos anuais. A disponibilidade continua dos dados não é assegurada, sendo que os utilizadores por vezes não têm acesso aos dados, quando necessitam. As atividades nesta etapa, são:

1. Início do compromisso com o foco na Indústria 4.0;
2. Primeiras interações nas abordagens aos serviços.

### Etapa 2 – Digitalização Interdepartamental

A empresa está ativamente comprometida com os tópicos da Indústria 4.0. Digitalização foi realizada e concluída em termos de implementação, através dos departamentos e os primeiros requisitos para a Indústria 4.0 foram implementados ao longo da empresa. A informação pode ser trocada (parcialmente) entre os diferentes departamentos e unidades de negócio. Este nível de integração não tem dados isolados, dentro da empresa.

Adicionalmente os diferentes blocos fabris de produção encontram-se, ligados através da troca de informação através de diferentes formas (e-mail, servidores FTP, papel, etc.), não se encontrando, ainda no estágio de se encontrar "ligado" à *cloud*. Nesta etapa a produção e o nível de desenvolvimento é suportado por diversos sistemas empresariais, sendo que os dados e a informação não são processados de forma automatizada.

As organizações começam a implementar, uma arquitetura orientada aos serviços (SOA), sendo que os novos sistemas a instalar, tem por base esta nova arquitetura, os processos iniciais podem ser desenvolvidos como serviços, adicionalmente um sistema de serviços empresariais é implementado para substituir os princípios de integração aplicacionais empresariais e para permitir ligações entre os novos sistemas.

Atividades:

1. Implementação de uma arquitetura orientada aos serviços;
2. Integração entre departamentos;
3. Primeira aproximação para um modelo de segurança IT;
4. Primeiros desenvolvimentos em aplicações móveis.

**Etapa 3 – Digitalização vertical e horizontal**

A empresa encontra-se digitalizada na horizontal e na vertical. Os requisitos da indústria 4.0, foram implementados dentro da empresa e os fluxos de informação foram automatizados. Os desenvolvimentos dos produtos são suportados de forma consistente, pelos sistemas da empresa. A informação do processo corrente, pode ser reencaminhado para o processo seguinte ou para o processo antecedente.

A empresa estabeleceu um processo de arquitetura orientada aos serviços, sendo que todas as funcionalidades dos sistemas integrados são disponibilizadas com serviços. São aplicados princípios de disponibilizar a informação na *cloud*, para troca de informação dentro da empresa, ficando estes serviços disponibilizados de forma a serem acedidos de qualquer local. Os empregados podem aceder à informação através dos seus dispositivos móveis de qualquer local. Com esta funcionalidade, os dispositivos podem exibir informação adicional acerca das máquinas (etapa de processamento atual, estado da manutenção, etc.). A informação gerada pela produção será agregada e processada em conjunto, sendo otimizado em tempo real, podendo a mesma ser adaptada em tempo real, podendo ser adaptado mantendo essas condições ou alterando, sempre que necessário.

A segurança é incrementada através do uso de um modelo avançado de segurança, sendo o acesso aos dados protegido de forma contínua e os dados transmitidos num formato encriptado dentro da organização. A confidencialidade, integridade e disponibilidade estão garantidas.

Atividades

1. Ligação a outras empresas no sentido de construir redes de valor;
2. Desenvolvimento de uma plataforma baseada na *cloud* de forma a oferecer serviços através da empresa.

**Etapa 4 – Digitalização Total**

A empresa encontra-se completamente digitalizada mesmo para lá das suas fronteiras e, integrada na rede de valor, sendo que a Indústria 4.0 encontra-se incorporada na estratégia da empresa. Nesta etapa o nível de integração verifica-se em toda a empresa. Por forma a otimizar os processos, o desenvolvimento das fases do produto, comunica de forma automática às etapas de produção posteriores e anteriores.

A empresa define um serviço orientado a uma plataforma *cloud* que oferece serviços na rede, por forma a trocar informações ao longo da cadeia de valor em tempo real. As máquinas podem ser mantidas globalmente, independentemente da sua localização (em

relação ao software). Os dados são agregados e processados em toda a empresa bem com a cadeia de valor. A linha de produção está de uma forma geral no seu mais alto nível em termos de otimização. A cifragem de dados nesta etapa, é usado em toda a empresa e, também é usada nas redes de valor. Os utilizadores podem aceder aos dados em qualquer lugar, usando medidas de autenticação implementadas.

**Atividades**

Iniciação de colaborações entre empresa na cadeia de valor para soluções completas e otimização dos fluxos de informação.

**Etapa 5 – Digitalização Total Otimizado**

A empresa é um exemplo nas atividades da Indústria 4.0, uma vez que tem uma forte colaboração com os seus parceiros de negócio e assim otimiza a cadeia de valor. Através destas colaborações, novos modelos de negócio bem como soluções completas são desenvolvidas e implementadas. Durante este processo de desenvolvimento, cada fase interna e externa da empresa é digitalizada.

Dentro da rede de valor, o valor físico e os fluxos de informação podem ser representados digitalmente, logo o processo integral de valor pode ser simulado em tempo real, assim é possível realizar automaticamente os ajustes necessários para todas as empresas da rede de valor. Todo este processo garante que a segurança das tecnologias de informação, se ajustam de uma forma rápida a novos riscos, os problemas inerentes à segurança, são resolvidos imediatamente onde a cifragem é otimizada em cooperação com os parceiros ao longo da rede de valor.

### 4.5.2 SIRI Smart Industry Readiness Index

O índice *Singapore Smart Industry Readiness Index*, ou SIRI[34] , foi criado em parceria com empresa TUV SUD certificada em inspeção, certificação e formação sendo validado por especialistas da indústria, bem como académicos especialistas, tendo a mesma sido concebida como uma ferramenta para ser usada pelas organizações independentemente do seu tamanho, ou indústria onde estas operam.

Este índice representado na Figura 29, abrange três, blocos fundamentais na indústria 4.0, Processos, Tecnologia e Organização, sendo que debaixo destes três pilares principais encontram-se oito pilares de foco. Estes oito pilares por sua vez subdividem-se em dezasseis dimensões de avaliação, por forma a que as organizações possam usar no sentido de avaliar as suas próprias empresas.

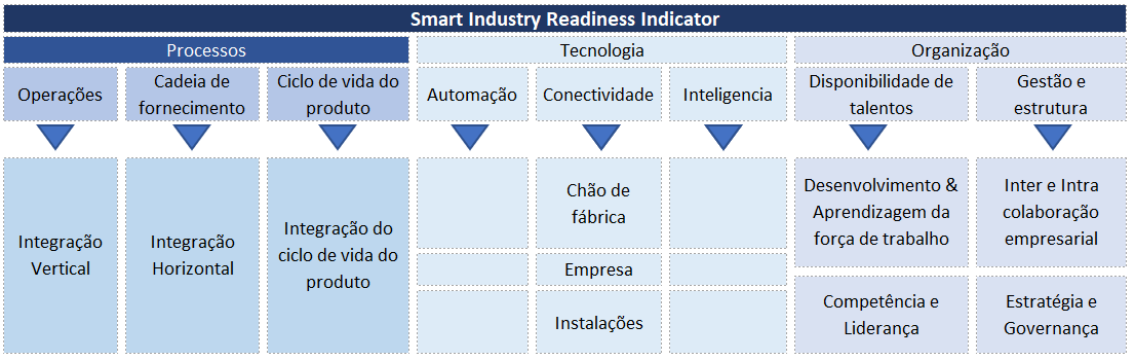



**Figura 29: Smart Industry Readiness Indicator**
Fonte: Adaptado [34]

## Bloco base ou central - Tecnologia

A tecnologia tem estado na base das três revoluções industriais. A primeira revolução teve na sua base o uso do vapor na produção, a segunda revolução assentou no uso energia elétrica e, as tecnologias de informação estiveram por sua vez na base da terceira revolução industrial, o que permitiu às organizações alcançarem elevados níveis de eficiências. Este bloco encontra-se segmentado em três pilares, nomeadamente: automação, conectividade e a inteligência.

### Tecnologia - Pilar base Automação

A automação, tem por base a aplicabilidade da tecnologia para monitorizar, controlar e executar a produção no sentido de permitir a entrega de produtos e serviços. A automação liberta os trabalhadores das tarefas repetitivas, bem como aumenta a velocidade, qualidade e consistência de execução.

### Tecnologia – Pilar base Conectividade

A conectividade permite garantir/medir interligação entre equipamentos, máquinas e sistemas baseados em computadores, por forma a garantir as comunicações e a troca de dados entre os ativos. O aumento de pontos de conetividade, aumentam por sua vez o

número de pontos de vulnerabilidade em termos de exposição no sistema, provocando um impacto significativamente superior em termos de segurança, ao anteriormente registado.

**Tecnologia – Pilar base Inteligência**

A inteligência tem como princípio, o tratamento e processamento da análise dos dados. Os avanços tecnológicos verificados em áreas como a *cloud,* análise de dados (*data analytics),* potenciam capacidades adicionais e mais possibilidades na análise dos dados, de traduzirem o conhecimento em ações de diagnóstico de problemas e identificar oportunidades de melhoria.

## Bloco base - Processos

O bloco fundamental de Processos inclui, operações, cadeia de fornecimento e ciclo de vida do produto, que convergem num sistema unificado e simples onde os dados são partilhados, processados e integrados através da gestão de produto, produção e das camadas empresariais da organização.

**Processos - Pilar base Operações**

O primeiro pilar 'Operações' engloba no planeamento a execução de processos que levam à produção de bens e serviços. O objetivo final é converter matérias-primas e mão de obra em bens e serviços com o menor custo. Neste pilar evidencia-se o uso de dados analíticos, para reduzir o desperdício e melhorar processos ineficientes. Este pilar mede simultaneamente, o grau de integração dos processos e sistemas em todos os níveis hierárquicos dentro das instalações. Esta integração vertical permite a automatização e a flexibilização das redes garante a eficiência de troca de dados e à rápida análise de informação.

**Processos - Pilar Cadeia de Fornecimento**

A Cadeia de Fornecimento inclui o planeamento e gestão de matérias-primas e um inventário de bens e serviços da empresa, desde o ponto de origem até o ponto de consumo. Debaixo de uma perspetiva da Indústria 4.0 os modelos de cadeia de fornecimento, tornar-se-ão mais digitalizados, onde os processos ao longo desta cadeia de fornecimento serão ligados através de uma rede de sensores e geridos centralmente num *hub* de dados e com um "motor" de analítica na sua base. A digitalização das cadeias de fornecimento, permitem decisões sobre custo, stocks e operações a serem feitas a partir de uma perspetiva transversal em vez de esta ser feita de forma isolada.

**Processos - Pilar do Ciclo de Vida de Produto**

O Ciclo de Vida do Produto refere-se à sequência de estágios, pelo qual o produto passa desde o processo inicial de concetualização até à remoção do mesmo do mercado. Os

estágios variam desde o design, engenharia, produção/fabrico para uso do cliente, serviço e disposição.

Uma *framework* de gestão robusta do ciclo de vida do produto, faz parte integrante das operações de fabrico; no entanto, ciclos de produto mais curtos e, uma crescente procura por produtos personalizados tem acentuado a necessidade de maior integração e, digitalização nos diferentes estágios do ciclo de vida do produto.

Os avanços nas ferramentas digitais vieram facilitar a recolha de dados, processos, sistemas de negócios no sentido de criar um único e unificado *backbone* de informações que pode ser gerido de forma digitalmente.

A Indústria 4.0 introduz o conceito de *Digital Twin*, que é uma representação virtual dos ativos físicos, dos processos e dos sistemas envolvidos num ciclo de vida do produto. Esta modelagem *Digital Twin*, oferece dois benefícios principais, o primeiro, a informação gerada em cada etapa pode ser partilhada, facilitando uma melhor tomada de decisão e permitindo que processos sejam otimizados dinamicamente noutras etapas.

Isto permite que as empresas encurtem seus ciclos de projeto e engenharia no sentido de responder à procura por parte dos clientes mais rapidamente. O segundo benefício, um *Digital Twin* remove as limitações de trabalhar com protótipos físicos. A facilidade de trabalhar com *Digital Twins* permite que vários protótipos possam ser criados e testados virtualmente a uma maior velocidade e escala com um custo muito mais baixo.

## Bloco base da Organização

Por forma a aumentar a produtividade das organizações, este bloco foca em duas componentes, a primeira componente são os colaboradores que compõem a organização, nomeadamente, toda a força de trabalho desde as equipas de topo (de gestão), até as equipas operacionais. O segundo componente, são os sistemas institucionais que governam como a empresa funciona.

### Organização – Pilar Disponibilidade de Talentos

Para qualquer transformação agregar valor, a força de trabalho tem que ter a capacidade de conduzir e promover Iniciativas referentes à Indústria 4.0 - serão um fator chave para o sucesso. À medida que as organizações adotam estruturas ágeis e mais planas permitindo tomadas de decisão descentralizadas, torna-se fundamental criar uma força de trabalho competente e flexível, caracterizada pela aprendizagem e desenvolvimento contínuos em todos os níveis da força de trabalho.

### Organização – Pilar Estrutura e Gestão

A estrutura de uma organização tem por base o seu sistema de regras e políticas implícitas, que descrevem como as funções e as responsabilidades são atribuídas, controladas e coordenadas.

A gestão é fundamental para garantir que os colaboradores a trabalham juntos, em torno de um objetivo comum bem definido.

Uma gestão e uma estrutura robusta, tornam a organização mais flexível e colaborativa, com poderes para desenhar e implementar estratégias efetivas da Indústria 4.0.

## 4.6. Síntese

O capítulo presente, faz a análise do estado da arte ao nível da Indústria 4.0, descrevendo a sua origem e, o termo pelo qual é muitas vezes associado, *Industrial Internet of Things*.

A descrição do porquê da Indústria 4.0, permite percecionar a importância que as revoluções industriais tiveram e, que esta última irá ter a nível mundial. São avaliados os diferentes sistemas industriais e, sistemas de controlo industrial, dentro deste setor permitindo compreender, onde a Internet das Coisas, terá um papel preponderante, no desenvolvimento desta indústria.

Na avaliação do estado da arte, são analisadas arquiteturas de referência como a RAMI 4.0 - *Reference Architecture Model Industrie* 4.0, sendo também avaliados dois modelos de maturidade de referência nesta área, o modelo SIMMI – *System Integration Maturity Model Industry* 4.0 e, o modelo SIRI – *Singapore Smart Industry Readiness Index.* Esta arquitetura e estes modelos permitem sustentar o modelo a desenvolver na sequência deste trabalho.

# 5. Segurança

Este capítulo incide sobre a segurança em torno do IoT sendo realçado o facto das limitações que os dispositivos IoT apresentam, aumentando a insegurança das soluções. É feita a avaliação em termos de caraterização da aplicabilidade destas soluções ao nível dos setores da indústria, da sua localização em termos de instalação, caraterização por tipo de conectividade, caraterização por tipo de tecnologia e caraterização por tipo de utilizador. São abordadas arquiteturas de referência e *frameworks* ao nível da segurança e, neste âmbito são também analisados diferentes tipos de ameaças e vulnerabilidades que podem ser encontradas no IoT.

## 5.1. Framework de Cibersegurança

O desafio associado à segurança, é tema de elevada importância, uma vez que a tecnologia usada na Internet das Coisas, concebe os sensores para recolher informação de forma discreta, do ambiente que os rodeia. Acontece, porém, que muita da informação recolhida é informação sensível, para as pessoas e para as organizações.

O conceito de segurança nas tecnologias de informação, remete-nos para o modelo *CIA*, ( cf. Figura 30) sendo que este acrónimo reflete os principais conceitos sobre os quais as organizações devem de se reger, que são a Confidencialidade, Integridade e a Disponibilidade, que vem do inglês *Confidentiality*, *Integrity* e *Availability*, sendo estes conceitos assim definidos:

**Confidencialidade** – evita que a informação sensível chegue às mãos das pessoas erradas, assegurando que a informação chega às pessoas certas. Para garantir a confidencialidade é usado a cifragem por forma a proteger os dados em transito ou armazenados, de forma a prevenir acessos não autorizados aos dados protegidos.

**Integridade** – envolve manter a consistência, precisão e a confiabilidade dos dados durante todo o seu ciclo de vida. Os dados não devem de ser alterados em trânsito ou quando estes se encontram parados/arquivados e, devem de ser tomadas medidas para garantir que os dados não possam ser alterados por pessoas não autorizadas.

**Disponibilidade** – Assegurar que o acesso à informação está sempre disponível aos utilizadores autorizados.


**Figura 30: Triângulo CIA**
Fonte: Criação do autor

Um dos maiores problemas e desafios associados ao IoT, prende-se com as limitações associadas a estes dispositivos. Muitos destes dispositivos têm limitações de memória, energia, largura de banda e capacidades de processamento, (cf. Figura 31) e com isto impossibilita-os de adotarem mecanismos de segurança usados noutros equipamentos.


Figura 31: Constrangimentos dos dispositivos IoT
Fonte: Criação do autor

Outro constrangimento que é frequentemente identificado, no desenvolvimento desta área, incide no facto de que estes dispositivos nem sempre são usados em ambientes controlados, como escritórios ou em ambientes residenciais.

Muitas das vezes estes dispositivos, são instalados em ambientes industriais com condições de ambiente muitas das vezes não são totalmente controladas, aumentando o risco destes dispositivos seja em termos de mau funcionamento, seja por outro lado a possibilidade de sabotagem física e/ou manipulação indevida dos mesmos.

**Categorização transversal**

Numa perspetiva aplicacional, dos dispositivos IoT apresenta-se uma caracterização[36], dos setores, localizações, conetividade, categorias, tecnologias, em termos de aplicabilidade desta panóplia de sensores, bem como o tipo de utilizador que interage com esta diversidade tecnológica.

### Caracterização por categoria de setor da indústria

A Figura 32, reflete os vários setores da indústria com aplicabilidade de implementações no âmbito do IIoT.

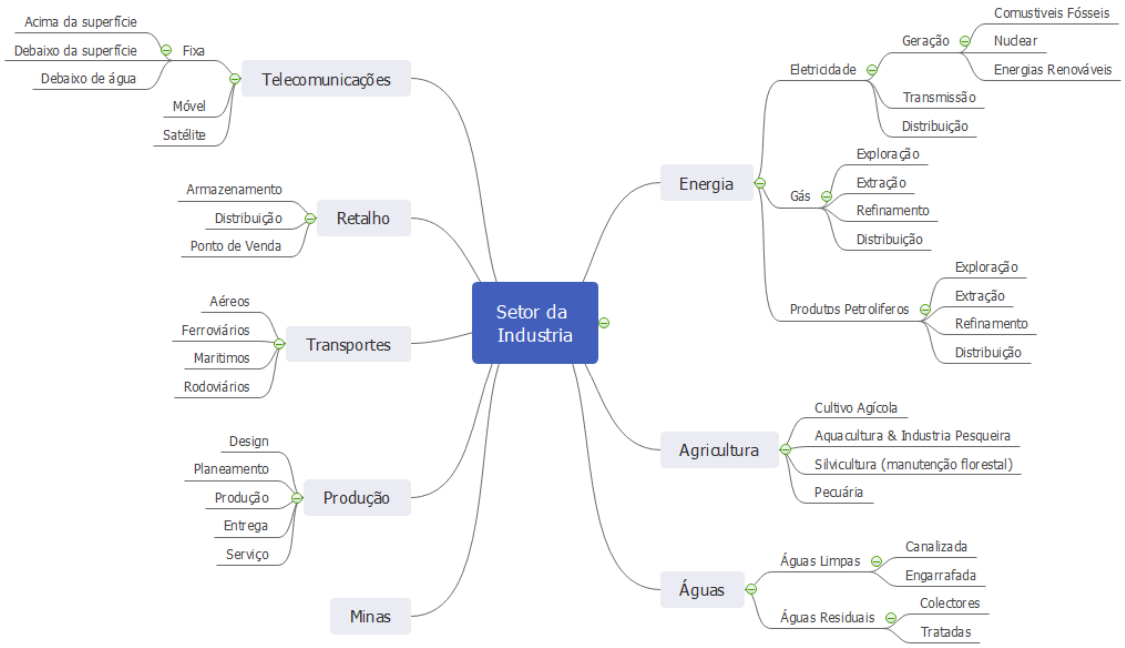



**Figura 32: Caraterização setor (adaptado de [36])**

### Caracterização por categoria de localização

As instalações destes dispositivos podem ter uma alargada diversidade de localizações, mapeada pela Figura 33.

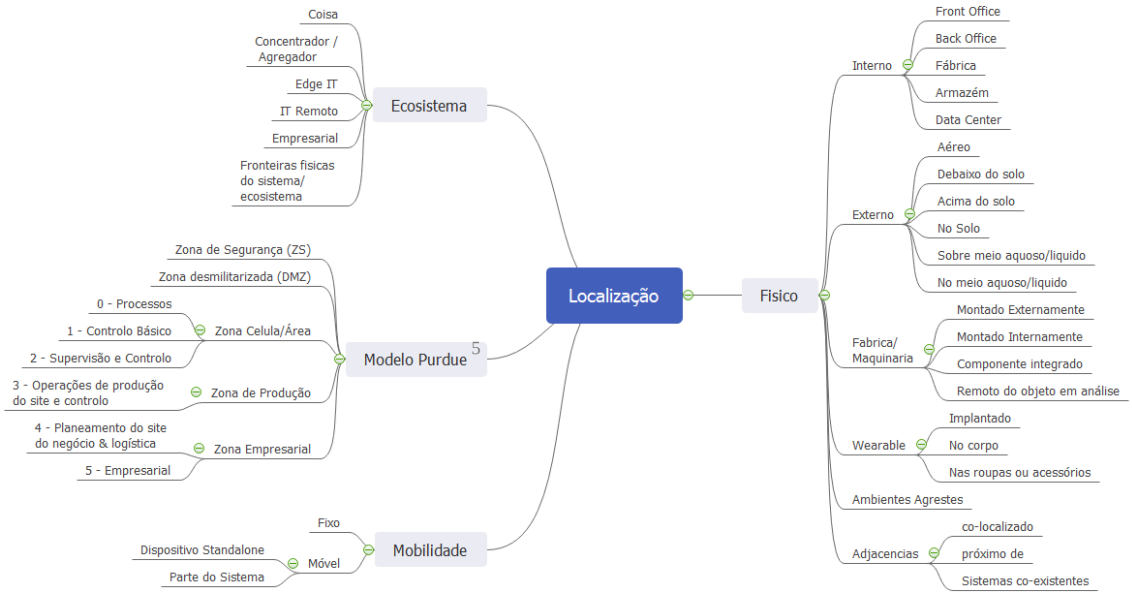



**Figura 33: Categoria localização (adaptado de [36])**

[5] **O modelo Purdue é apresentado em detalhe no capítulo 5.2**

### Caracterização por categoria de conectividade

Com um leque tão alargado de dispositivos, leva a que se possam considerar diferentes tipos de conectividade em função da aplicabilidade da solução. A Figura 34, reflete as variáveis desta conectividade.

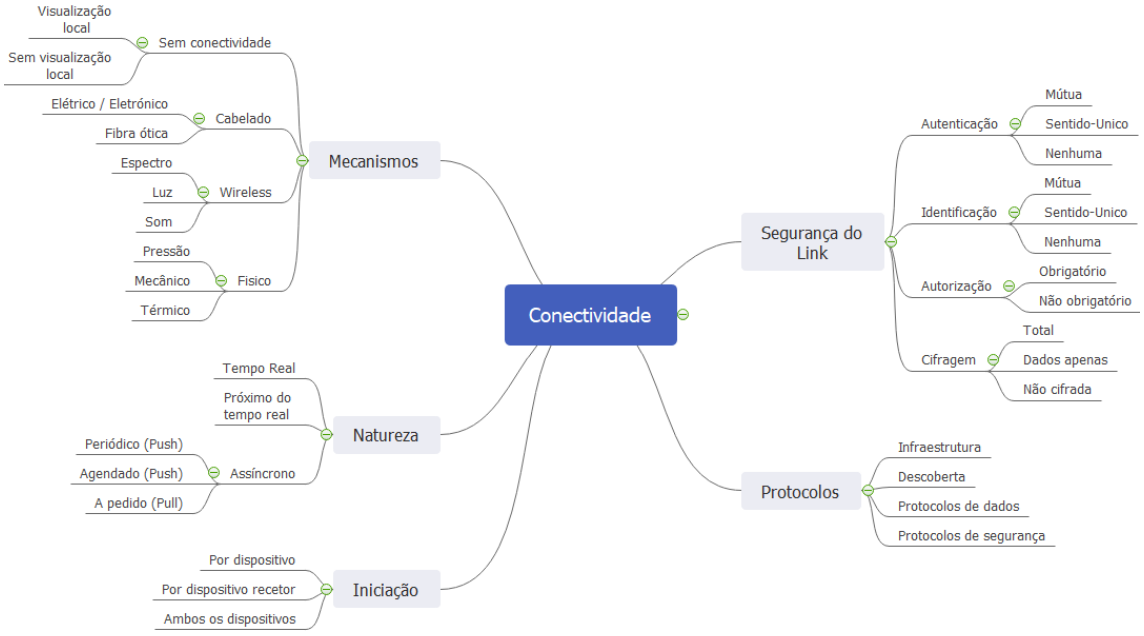



**Figura 34: Categoria Conectividade (adaptado de [36])**

### Caracterização por categoria de dispositivo

As soluções de implementação ao nível do IIoT permitem uma panóplia distinta de dispositivos que são suportados em diferentes indicadores, seja pela funcionalidade dos mesmos, seja pela criticidade. A Figura 35, correlaciona estes indicadores, na sua plenitude.

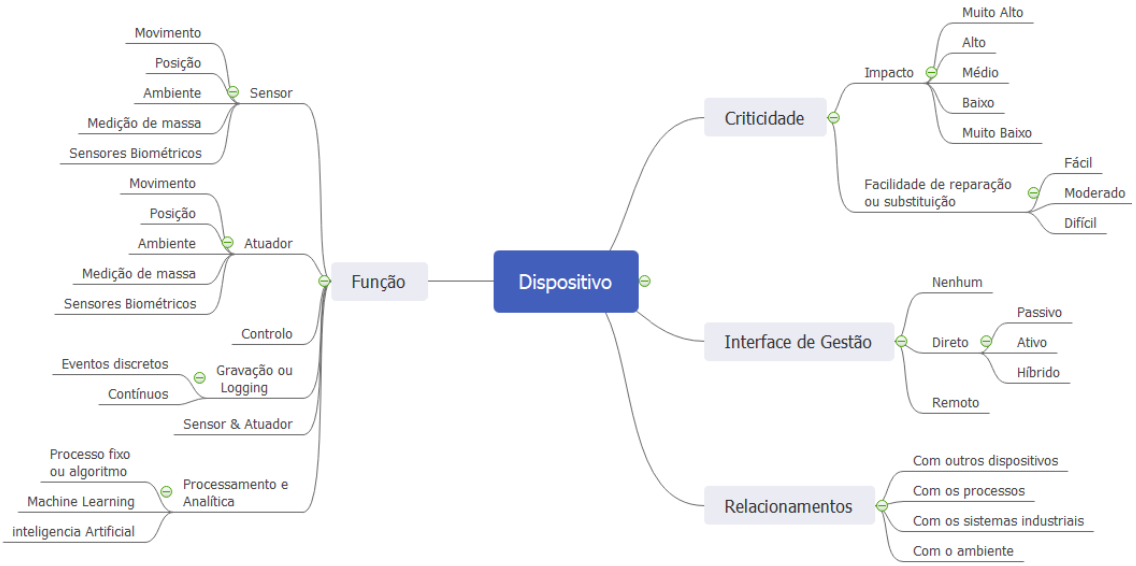



**Figura 35: Categoria Dispositivo (adaptado de [36])**

## Caracterização por categoria por tecnologia

A tecnologia é a base do IIoT e nesse sentido, a Figura 36, permite de uma forma lógica e simples, percecionar as variáveis que podem impactar, no desenho de uma solução industrial,

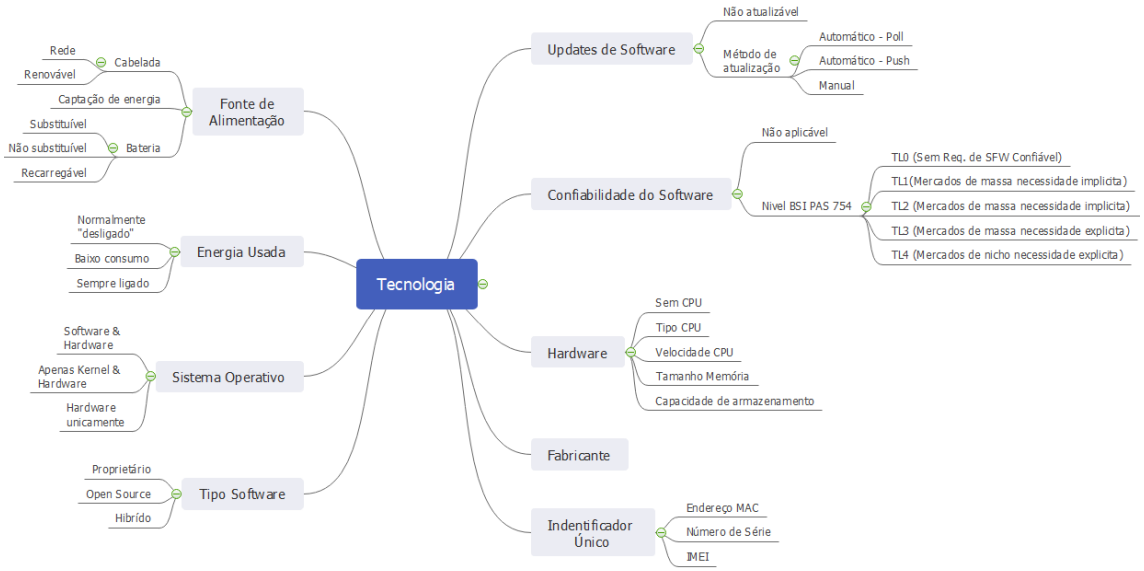



**Figura 36: Categoria Tecnologia (adaptado de [36][37])**

## Caracterização por categoria por utilizador

Ao nível do utilizador este pode ser categorizado pelo tipo de utilizador, ou pelo interface usado para acesso, sendo essa análise refletida na Figura 37.


**Figura 37: Categoria Utilizador (adaptado de [36])**

## 5.2. Modelo de Purdue

O Modelo Purdue para Controlo Lógico de uma Framework Hierárquica, foi desenvolvido pela International Society of Automation ISA-99 Committee for Manufacturing and Control Systems Security[38], que tendem a formar uma base para os Sistemas de Controlo Industrial e é formado por seis níveis conforme representado na Figura 38.


**Figura 38: Modelo Purdue de Framework lógica do controlo hierárquico (adaptado de [39])**

O modelo de Purdue [38] [39] usa o conceito de zonas, subdividido uma rede empresarial e uma rede industrial em segmentos lógicos compostos por sistemas que desempenham funções similares ou tem requisitos similares.

**Zona Empresarial – Nível 5: Empresa**

O Nível 5 é onde tipicamente as infraestruturas de sistemas e as aplicações IT existem. Os acessos a esta camada são por norma realizados, por acessos VPN assim como os acessos empresariais à internet estão concentrados nesta camada. As comunicações diretas entre os sistemas empresariais e os ICS, tem tendência a que não sejam realizadas pelo elevado risco, que representam para a organização. Nestes casos são criadas camadas de zonas desmilitarizadas (DMZ), para garantir acesso a estas zonas.

**Zona Empresarial – Nível 4: Planeamento do Site de negócio & Logística**

O nível 4 é muitas das vezes percecionado como uma extensão do Nível 5, porque acolhem os sistemas IT que permitem a elaboração de relatórios, agendamentos (atualizações), gestão de inventário, capacidade de planeamento, gestão operacional e gestão de manutenção, serviços de e-mail, impressão, etc. Os serviços, sistemas e aplicações dos Níveis 4 e 5 normalmente são geridos e operados pelos departamentos de IT.

**Zona Empresarial – Nível 3: Operações de Produção do site e Controlo**
Os sistemas no Nível 3 são por norma responsáveis pela gestão de controlo das operações fabris por forma a produzir o produto final. As aplicações, serviços e sistemas que se encontram neste nível, incluem:

- Histórico, dados da planta fabril;
- Sistema de relatórios de produção;
- Sistema de agendamento de produção;
- Garantia de confiabilidade;
- Postos de trabalho da engenharia;
- Servidores de rede de ficheiros;
- Serviços IT, como DNS, DHCP, Active Directory e NTP;
- Serviços de acesso remoto;
- Área de *staging.*

Os sistemas e aplicações do Nível 3 comunicam com os sistemas na zona empresarial através de uma DMZ.

**Zona Célula/Área – Nível 2: Área de Controlo e Supervisão**
O Nível 2 incluem equipamento e sistemas de operações e produção, para a produção individual, que tipicamente incluem:

- Interfaces Homem Máquina (HMI);
- Sistemas de Alerta/Alarmes;
- Estações de trabalho em Salas de controlo.

Estes sistemas podem comunicar com os sistemas no Nível 1. Adicionalmente podem fazer de interface com os sistemas nas zonas Empresariais de produção através de uma DMZ.

**Zona Célula/Área – Nível 1: Controlo Básico**
O Nível 1 incluiu equipamento de controlo de processos que recebe informação dos sensores, que processa os dados inseridos usando os algoritmos de controlo e, envia os dados processados para um elemento final. Os dispositivos neste nível são responsáveis pelos controlos sequenciais e não sequencias e controlo por lotes. Alguns dos dispositivos que existem nesta camada são, Sistema Distribuído de Controlo (DCS – Distributed Control System), PLC Controladores Lógicos Programáveis (PLC – Programmable Logic Controllers) e, as Unidades de terminal Remoto (RTU – Remote Terminal Units).

**Zona Célula/Área – Nível 0: Processo**
O Nível zero (0), incluiu os sensores e os elementos instrumentais que diretamente ligam ao processo de produção e controlo. Estes dispositivos são controlados pelos equipamentos que se encontram no Nível 1.

**Zona de Segurança**
Os sistemas na zona de segurança, fazem a monitorização de eventuais anomalias nos processos, automaticamente retornam aos processos de segurança, se determinado limite foi ultrapassado, alertando de imediato o operador para as potenciais questões de segurança. Estes sistemas são por norma sistemas *air-gapped (desligado)* dos restantes sistemas de controlo.

## Arquitetura de referência dos Sistemas de Controlo industrial

A necessidade de interligar as redes de negócio ao nível dos Sistemas de Controlo Industrial com as redes IT, deve ter por base em termos de recomendação, que o número de pontos de entrada no ambiente de Sistemas de Controlo Industrial seja limitado ao mínimo possível. Isto permite reduzir o número de potenciais zonas de entrada nestes ambientes, sendo também recomendado a proibição de comunicações diretas entre o IT e as redes ICS.

A Figura 39 ilustra a arquitetura de referência dos Sistemas de Controlo Industrial. Esta arquitetura usa o conceito de zonas para dividir a rede em ambientes mais pequenos e mais focados onde os controlos de sistemas podem ser consistentemente aplicados. Uma zona é um segmento de rede dentro do ambiente de rede com um perímetro bem definido.

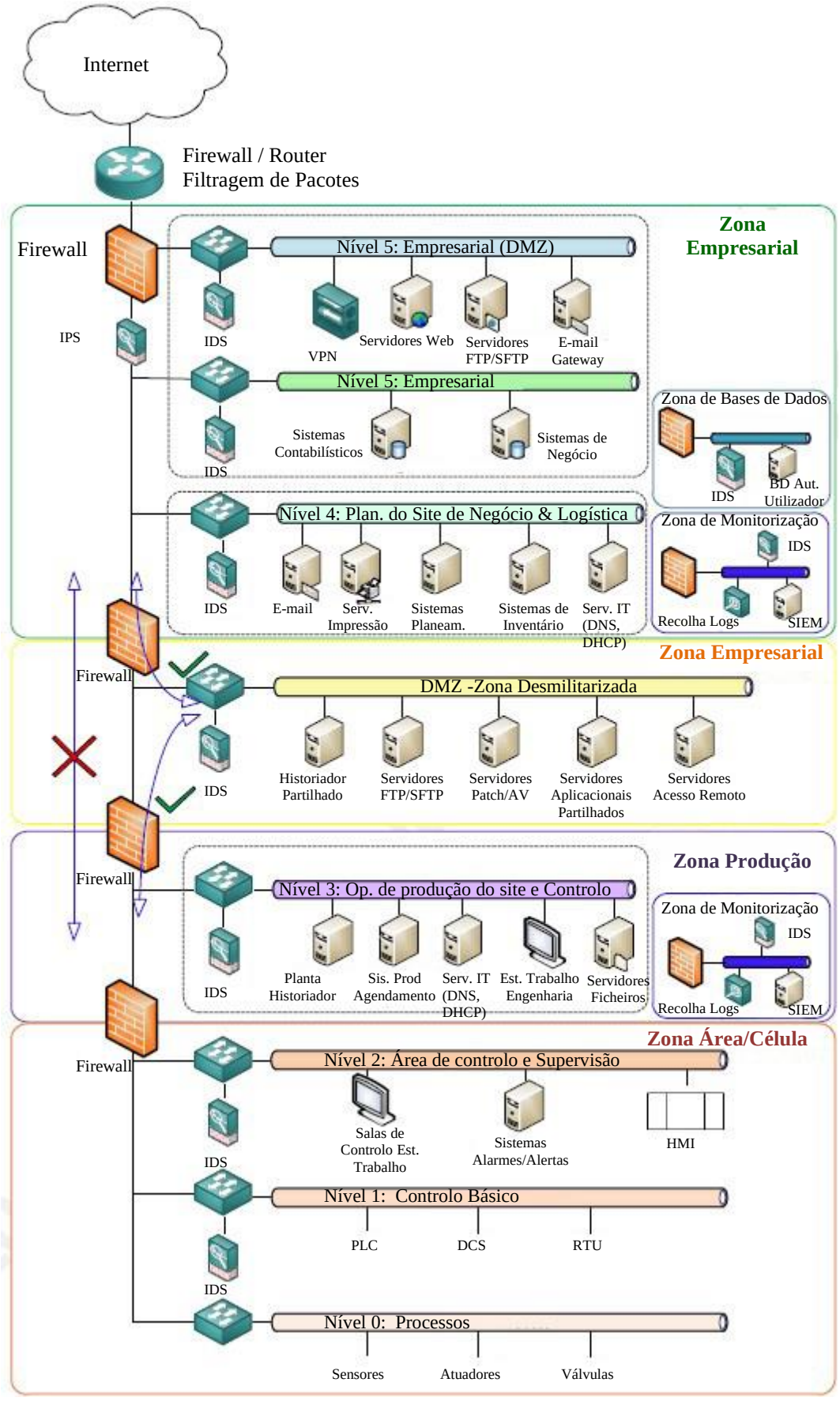



**Figura 39: Modelo de Purdue modificado para um controlo de arquitetura de hierarquia (adaptado publicação especial NIST [40])**

## 5.3. Standards

Organizações de desenvolvimento de standards, como ITU[1], NIST[41], ETSI[42], IETF[43] e ISO[44], tem como missão o desenvolvimento de standards com intuito de serem adotados de forma global. Muitas destas organizações, iniciaram os processos no espaço focado nos desafios do IoT, incluindo os casos de estudo e interoperabilidade, mas também a endereçarem a segurança ao nível do IoT.

A Tabela 5, permite apresentar diversas iniciativas, no âmbito da segurança IoT endereçadas por diversas entidades.

**Tabela 5: Iniciativas de segurança IoT – Desafios Endereçados**
Adaptado de [45]

| | Iniciativas de segurança IoT | Cibersegurança e privacidade por defeito | Standards de Segurança IoT | Avaliação e Certificação | Legislação à prova de "futuro" | Econsistema industrial responsável | Segurança no fornecimento da cadeia (suply chain) | Suporte de ciclo de vida do produto | Identidade do dispositivo e root of trust | So seguros, Cloud e aplicações | Comunicações e infraestruturas seguras | Analitica e monitorização segura |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Alliance for IoT Innovation | ● | ● | | ● | | | | | | | |
| 2 | Cloud Security Alliance | | ● | | | | | | | ● | | |
| 3 | ENISA IoT | ● | ● | | ● | | | | | | | |
| 4 | ETSI | ● | ● | | | | | | | | | |
| 5 | GlobalPlatform | | | ● | | | | | ● | | | |
| 6 | Global Cyber Alliance | | | | | | | | | | | ● |
| 7 | GSMA | | ● | | | | | | | | ● | |
| 8 | Internet Engineering Task Force | | ● | | | | | | | | ● | |
| 9 | Industrial Internet Consortium | | ● | | | ● | ● | ● | ● | ● | ● | ● |
| 10 | IoT Acceleration Consortium | | ● | | | | | | | | | |
| 11 | IoT Consortium | | | | | ● | | | | | | |
| 12 | IoT Cybersecurity Alliance | | ● | | | | | | | ● | ● | ● |
| 13 | IoT European Platforms Initiative | | | | | ● | | | | | | |
| 14 | IoT Security Foundation | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● |
| 15 | ITU Study Group 20 | | ● | | | | | | | | ● | |
| 16 | LoRa Alliance | | ● | ● | | | | | | | ● | |
| 17 | NIST Cybersecurity for IoT Program | | ● | | | | | | | | | |
| 18 | Open Connectivity Foundation | | ● | | | | | | | | ● | |
| 19 | OWASP IoT Project | ● | ● | | | | | | | ● | ● | |
| 20 | Prpl Foundation | | | | | | | | ● | | ● | |
| 21 | Thing-to-Thing Research Group | | ● | | | | | | | ● | ● | |
| 22 | Trusted Computing Group | | | | | | | | ● | ● | | |
| 23 | UEFI Forum | | ● | | | | | | ● | | | |
| 24 | Wi-SUN Alliance | | ● | ● | | | | | | | ● | |
| 25 | Zigbee Alliance | | ● | ● | | | | | | | ● | |

**Tabela 6: Iniciativas de segurança IoT – Associados**

Adaptado de [45]

| | IoT Iniciativa de segurança | | Governo | Indústria | Academias | | America | Europa | Asia | Global |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Alliance for IoT Innovation | | | ● | | | ● | ● | | |
| 2 | Cloud Security Alliance | | | ● | ● | | | | | ● |
| 3 | ENISA IoT | | ● | | | | | ● | | |
| 4 | ETSI | | ● | ● | ● | | | ● | | |
| 5 | GlobalPlatform | | | ● | | | | | | ● |
| 6 | Global Cyber Alliance | | | ● | | | | | | ● |
| 7 | GSMA | | | ● | | | | | | ● |
| 8 | Internet Engineering Task Force | | | ● | ● | | | | | ● |
| 9 | Industrial Internet Consortium | | | ● | | | | | | ● |
| 10 | IoT Acceleration Consortium | | ● | ● | ● | | | | ● | |
| 11 | IoT Consortium | | | ● | | | ● | ● | | |
| 12 | IoT Cybersecurity Alliance | | | ● | | | ● | ● | | |
| 13 | IoT European Platforms Initiative | | ● | | | | | ● | | |
| 14 | IoT Security Foundation | | | ● | | | ● | ● | | |
| 15 | ITU-T Study Group 20 | | ● | ● | ● | | | | | ● |
| 16 | LoRa Alliance | | | ● | | | | | | ● |
| 17 | NIST Cybersecurity for IoT Program | | ● | | | | ● | | | |
| 18 | Open Connectivity Foundation | | | ● | | | | | | ● |
| 19 | OWASP IoT Project | | | ● | ● | | ● | ● | | |

(continuação)

| | IoT Iniciativa de segurança | | Governo | Indústria | Academias | | America | Europa | Asia | Global |
|---|---|---|---|---|---|---|---|---|---|---|
| 20 | Prpl Foundation | | | ● | | | | | | ● |
| 21 | Thing-to-Thing Research Group | | | ● | ● | | ● | ● | | |
| 22 | Trusted Computing Group | | | ● | | | | | | ● |
| 23 | UEFI Forum | | | ● | | | | | | ● |
| 24 | Wi-SUN Alliance | | | ● | | | | | ● | |
| 25 | Zigbee Alliance | | | ● | ● | | ● | ● | | |
| | Total | | 6 | 22 | 8 | | 8 | 10 | 2 | 12 |

### 5.3.1. ENISA (European Union Agency for Cybersecurity) Framework

Na avaliação da informação disponibilizada pela ENISA[46], é possível agregar seis destes documentos desta organização, que permitem a criação de uma *framework*, interligada ao IoT/IIoT, os documentos são:

- Security and Resilience of Smart Home Environments Good practices and recommendations[47];

  Este estudo tem como objetivo proteger ambientes residenciais inteligentes de ameaças cibernéticas, destacando boas práticas que se aplicam a todas as etapas do ciclo de vida do produto: desde o seu desenvolvimento, a sua integração em ambientes residenciais inteligentes e o seu uso e manutenção até o final da vida útil. O estudo também destaca a aplicabilidade das medidas de segurança a diferentes tipos de dispositivos.

- Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures[48];

  Este relatório tem como objetivo a elaboração de recomendações base de cibersegurança para a IoT, com foco em infraestruturas críticas de informação, que abrangem instalações, redes, serviços e equipamentos físicos de tecnologias da informação. Estas infraestruturas são consideradas críticas, porque sua destruição ou interrupção pode trazer consequências catastróficas para a saúde, para a segurança e o bem-estar económico dos cidadãos.

- Good Practices for Security of Internet of Things in the context of Smart Manufacturing[49];

  Este estudo visa abordar os desafios de segurança e privacidade relacionados à evolução dos sistemas e serviços da indústria, que foram acelerados pela introdução de inovações de IoT. Os principais objetivos passam por recolher as boas práticas para garantir a segurança da IoT no contexto da Indústria 4.0 / Produção (fabril) Inteligente, enquanto mapeia os desafios relevantes de segurança e privacidade, ameaças, riscos e cenários de ataque.

- Towards Secure Convergence of Cloud and IoT[50];

  Este relatório combina o conhecimento da ENISA em IoT e em segurança na *cloud* e, apresenta uma análise dos desafios de segurança e possíveis sugestões de segurança, que os fornecedores de dispositivos de IoT e, provedores de serviços na *cloud* (denominados operadores de telecomunicações) podem vir a considerar. Entre as questões de segurança, a segurança de ponta-a-ponta e a adoção de medidas base de segurança, são as que confirmam a necessidade de uma abordagem holística da segurança, para o ecossistema de IoT.

- IoT Security Standard Gap Analysis – Mapping of existing standards against requirements on security and privacy in the area of IoT[51];

  Este relatório fornece informações sobre os requisitos de segurança de IoT, mapeando ativos críticos e ameaças relevantes, avalia possíveis ataques e identifica potenciais boas práticas e medidas de segurança, a serem aplicadas para proteger os sistemas de IoT.

- Industry 4.0 Cybersecurity: Challenges & Recommendations[52];

  Os principais objetivos deste documento são a recolha de boas práticas por forma a garantir a segurança da IoT no contexto da Indústria 4.0 / Produção (fabril) Inteligente, mapeando os desafios relevantes de segurança, privacidade, ameaças, riscos e cenários de ataque. Com base neste relatório, este documento fornece os resultados de uma análise de lacunas, realizadas a fim de identificar os principais desafios à adoção das medidas de segurança e segurança da Indústria 4.0 e o IoT industrial.

A Figura 40 resume as principais caraterísticas dos documentos ENISA, que permitem a criação de uma framework, focada no IoT/IIoT.

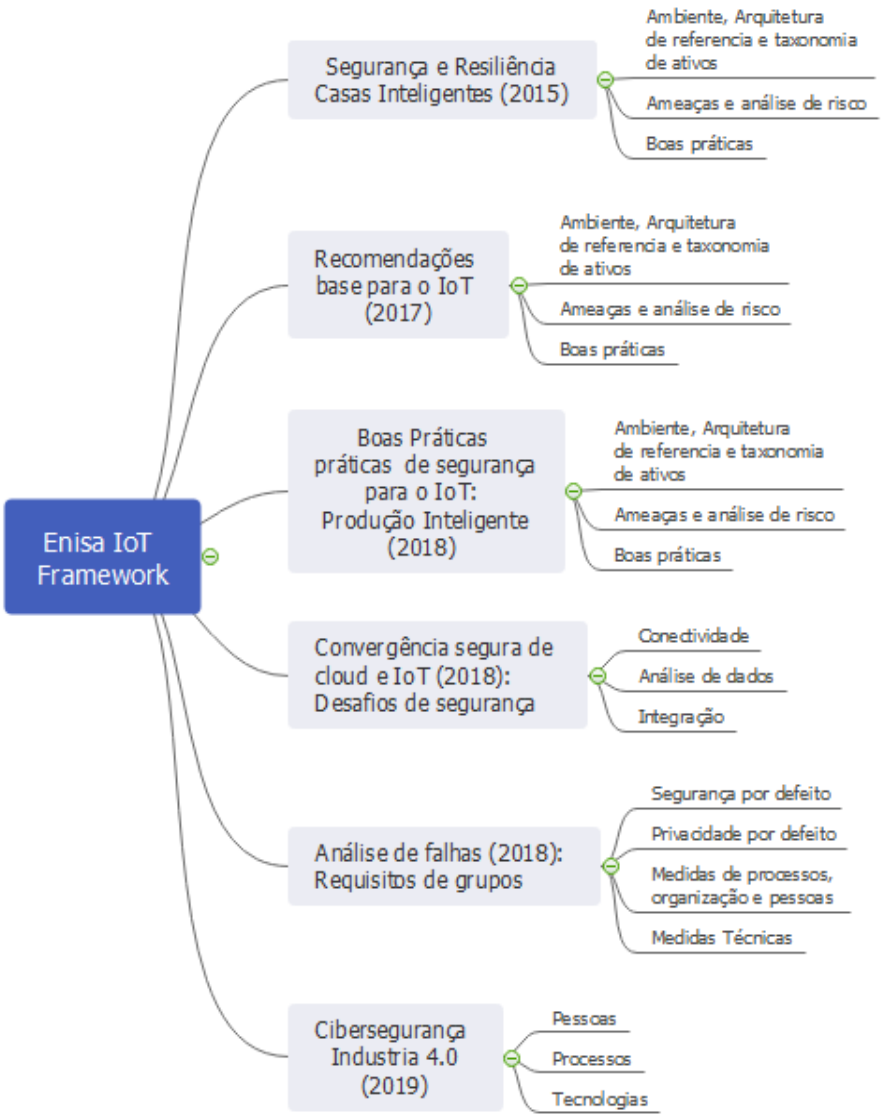



**Figura 40: ENISA IoT/IIoT Framework de Segurança**
Fonte: Criação do autor

## 5.4. IoT Ameaças e Vulnerabilidades

Muitas são as ameaças e vulnerabilidades a que estes dispositivos se encontram expostos, entre eles evidenciam-se os seguintes.

**Dispositivo vulnerável ao software**

Os dispositivos de IoT "correm" software que pode conter más opções de design e/ou erros de segurança, como *buffer overflow* e tratamento inadequado de exceções. Este erro de "conceção" torna-os vulneráveis a uma panóplia diversificada de ataques, que podem comprometer a confidencialidade e/ou integridade dos dados.

**Ameaça de privacidade**

As possibilidades de rastreamento da localização dos dispositivos representam um elevado risco de privacidade dos utilizadores. Um atacante, pode obter dados confidenciais desses dispositivos de forma a poder usá-los para fins ilícitos e/ou vender a informação obtida, na *dark web*, para monitorização não autorizada.

***Eavesdropping***

A comunicação através de uma rede IoT pode ser intercetada e decifrada se o canal de comunicação não estiver suficientemente protegido, por exemplo, se a chave de cifragem, parâmetros de segurança ou definições de configuração, forem trocados de forma clara ou se forem utilizados algoritmos criptográficos fracos ou inadequados. Os ataques relacionados, incluem *man-in-the-middle, session hijacking* ou, reprodução de mensagens

**Negação de Serviço (*Denial-of-Service*, DoS)**

Os dispositivos, por serem limitados nos seus recursos, são suscetíveis a ataques de negação de serviço, lançados por atacantes que enviam solicitações contínuas por forma a esgotar os recursos do dispositivo. Por outro lado, os dispositivos comprometidos podem ser usados, para interromper a operação de outras redes ou sistemas por meio de um ataque de *Denial-of-Service* distribuído (DDoS).

**Ataque ao nível do *Firmware***

Um atacante pode proceder à substituição do *firmware* do dispositivo, com o pretexto de uma atualização de rotina, ou numa instalação base desse dispositivo.

**Cópia ou substituição do dispositivo**

Uma fábrica não-confiável pode copiar caraterísticas físicas, *firmware/software* e configuração de segurança dos dispositivos. Os dispositivos implementados, podem ser comprometidos, usando para o efeito *reverse-engineer* para cópia desse firmware/software. Desta forma os dispositivos copiados, podem ser clonados e vendidos mais baratos no mercado, podendo conter modificações funcionais, incluindo *backdoors*. Em alternativa um dispositivo original, pode ser substituído por um clone ou uma variante, durante o transporte ou na preparação.

***Data-Leakage***

Divulgação de dados confidenciais, intencional ou não, para organizações não autorizadas. Os dados confidenciais podem ser capturados por um atacante a partir de dispositivos individuais, durante o trânsito desde dados ou no *back-end*.

***Malware***

Os dispositivos podem ser infetados com programas concebidos para executar ações não autorizadas nos sistemas, usando vulnerabilidades existentes nos softwares ou nos *firmwares*.

**Credenciais fracas de autenticação dos utilizadores/administradores**

Uma gestão deficiente de credenciais, como escolhas fracas de senha e falta de autenticação multifator para interfaces de utilizadores e administrativas de dispositivos, *gateways* ou *back-ends*, é uma vulnerabilidade comum em muitos sistemas de informação, incluindo a IoT.

A Figura 41 apresenta uma relação entre ameaças e, o impacto potencial das mesmas, na organização.

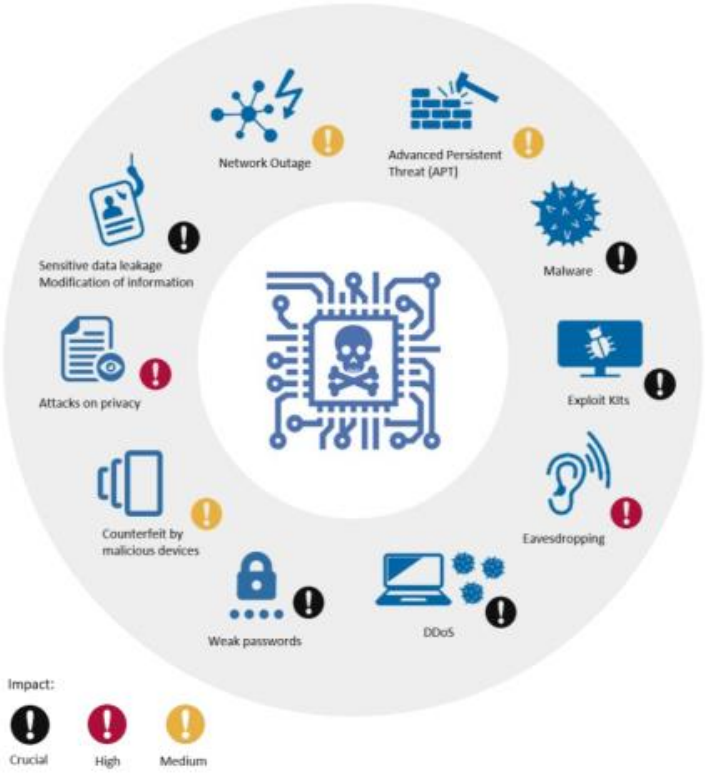



**Figura 41: Impacto das ameaças IoT [48]**

## 5.5. Síntese

Este capítulo, permite efetuar a análise de segurança ou falta desta, na Internet das Coisas. Para a realização da avaliação são identificados os constrangimentos associados aos dispositivos, que fazem parte do ciclo da Internet das Coisas e em simultâneo, é efetuado a caracterização transversal da aplicação destes dispositivos, em termos de aplicabilidade do setor da indústria, localização, tipo de conectividade, categoria de dispositivo, tecnologia, e tipo de utilizador.

É feita a análise do modelo de referência ao nível da Indústria 4.0 e a decomposição das zonas que o constituem. Este modelo, permite às organizações que implementam esta arquitetura, criarem camadas de segurança ao longo da sua rede empresarial e rede do chão de fábrica.

Com uma panóplia tão alargada de entidades, a endereçarem questões de segurança, foi criada uma matriz que correlaciona as entidades com as iniciativas que estas organizações, apresentam. Esta matriz permite uma maior legibilidade organização/iniciativa. Das vinte cinco entidades, mapeadas na matriz é feita uma análise mais incisiva, sobre alguns dos artigos publicados pela ENISA (European Union Agency for Cibersecurity).

No âmbito da segurança é feita a análise dos protocolos, envolvidos nas comunicações na Internet das coisas, bem como vulnerabilidades identificadas nesta área.

# 6. Modelo de Maturidade de Implementação na Indústria I4.0 – $(MI)^2$4.0

O presente capítulo desenvolve o processo que deu origem à formulação do modelo. O modelo a desenvolver, encontra-se segmentado em três blocos principais que endereçam a componente da administração da organização, com o objetivo de ter o comprometimento desta, perante a estratégia a definir e os respetivos objetivos a alcançar. Sendo um modelo orientado à Indústria 4.0, inclui as tecnologias de operação com o objetivo de garantir que esta se encontra alinhada com os objetivos de negócio e que simultaneamente, está alinhada com as tecnologias de informação, para garantir que as soluções a implementar lhe vão garantir a evolução dentro da Indústria 4.0, sem comprometer a segurança da organização.

As tecnologias de informação no modelo, tem também como objetivo de garantir que se encontram alinhados com os objetivos de negócio e que se encontram "sincronizados", com as tecnologias de operação para que em conjunto, respondam ao desafio da "digitalização" do chão de fábrica. Após a definição dos respetivos "atores" no modelo, foram definidos um conjunto de questões, para cada um dos blocos que permitem ao auditor, ter uma ferramenta (desenvolvida em excel) que com base num questionário ter uma avaliação, do estado da organização no que concerne à sua maturidade. As questões tem associado uma ponderação, com base em cada uma das respostas à mesma, sendo que as respostas ao modelo, devem de ser obtidas diretamente dos "atores" em questão, por forma a permitir uma maior fiabilidade do resultado do modelo.

## 6.1. Transformação Digital

As abordagens tradicionais ao nível da segurança e cibersegurança, dos processos de planeamento, nos diferentes tipos de organizações com foco na produção, são feitos numa base de conhecimento e, experiência do pessoal envolvido nas atividades dessa produção. Estas unidades de tecnologias de operação, por norma são conhecedores e, especialistas, com base na experiência ganha e, não pelo de o terem feito por qualquer processo ou sistema de aprendizagem moderno.

Um dos maiores constrangimentos, identificados nesta atualização prende-se com a resistência à mudança dos intervenientes, dessa forma existe necessidade por parte da organização, de definir de forma clara e inequívoca, a estratégia, os valores e os objetivos, para que esta esteja imbuída do mesmo objetivo.

A estratégia definida pela administração, tem nos seus objetivos a Indústria 4.0, objetivos esses, que passam pela digitalização do chão de fábrica, levando que que venha a existir uma cooperação mais efetiva entre as tecnologias de operação e as tecnologias de Informação, reforçando o conceito base da Indústria 4.0. Esta digitalização tem associados muitos benefícios como a flexibilidade na automação, a manutenção preditiva, a produção zero defeitos, etc.

Esta estratégia é impulsionada pelo efeito globalização e pela pressão da concorrência, no sentido de inovarem, aumentarem a competitividade, e terem um melhor desempenho que os seus concorrentes. Para implementação da estratégia as organizações, apostam na implementação das tecnologias digitais, como as ferramentas que vão potenciar o crescimento da automação, eliminar os erros de processos, aumentar a produtividade, simplificar as operações de negócio, tornarem os seus processos assentes em cima de conhecimento intenso, redução de custos, na globalidade aumentar a inteligência do processo, resultando na produção de mais produto, com melhor qualidade e a custos mais competitivos.

Esta aceleração tecnológica em termos de digitalização do chão de fábrica, disponibiliza às organizações um alargado leque de oportunidades de inovação, na medida que lhes permitem melhorias significativas nos processos e na transformação das suas operações no sentido em que resulta não apenas em melhorias ao nível da produção, mas numa mudança de paradigma disruptivo ao nível das operações. Estas são razões que levam muitas organizações industriais a investirem fortemente, na digitalização dos seus processos, como uma das componentes mais relevantes da sua estratégia de transformação.

Esta transformação, tem início com implementação dos sistemas ciber-fisicos (CPS – Cyber-Physical Systems), nos ambientes fabris como forma de iniciar o processo de digitalização, com automatização e inteligência dos processos industriais [61]. Estes sistemas, facilitam as ligações entre o mundo físico das máquinas fabris, dispositivos de automação industrial e as tecnologias de operação, com o mundo dos computadores, datacenters e as tecnologias de informação, sendo um dos pressupostos subjacentes na Indústria 4.0, da digitalização do processo com ligação perfeita das máquinas e dispositivos físicos com as infraestruturas das tecnologias de informação.

Os sistemas ciber-fisicos trazem benefícios[61], como:

- Maior qualidade;
- Maior flexibilidade;
- Maior produtividade;
- Standartização no desenvolvimento;
- Redução no *Time-to-market*;
- *Benchmarking e* melhoria contínua;
- Competição global, entre as empresas mais fortes;
- Novas oportunidades laborais;
- Novos serviços e modelos de negócio.

O facto de as tecnologias de operação terem objetivos diferentes das tecnologias de informação (cf. Figura 42), sendo que as TO’s priorizam a disponibilidade em termos de linha de produção, as TI’s priorizam a confidencialidade, por exemplo a proteção do direito de propriedade intelectual.


**Figura 42: Prioridades TI's versus TO's**
Fonte: Criação do Autor

Esta "não alinhamento" entre equipas, coloca em causa vários indicadores dentro das organizações como:

- Dificuldades de alinhamento nos cumprimentos, dos objetivos da organização;
- Dificuldades de implementação uma política comum de cibersegurança;
- Dificuldades de flexibilidade entre equipas;
- Dificuldades numa resposta rápida no *time-to-market;*
- Dificuldades na otimização de custos;
- Ineficiências operacionais;
- Perda de vantagem competitiva.

As dificuldades existentes entre as TO's e as TI's, levam à criação de dificuldades nas organizações, que as tornam, menos produtivas face à concorrência bem como mais frágeis em termos de segurança, pelo facto de não existir, este alinhamento.

Conforme ocorreu nas revoluções industriais anteriores, a quarta revolução industrial, resultante na Indústria 4.0, vai também ter o seu tempo de "maturação", no sentido das organizações, poderem implementar, as medidas necessárias para se tornarem mais competitivas face à concorrência.

## 6.2. Simulador do Modelo (MI)2 I4.0

Este trabalho, pretende contribuir com um modelo que permita às organizações que tenham nos seus objetivos a digitalização do chão de fábrica. Este modelo, pretende definir passos que permitam aos administradores em conjunto com as respetivas equipas de tecnologias de informação com as equipas de tecnologias de operação, responder aos objetivos da organização. A Figura 43, (pag.78) mapeia estes passos, que devem de estar refletidos na estratégia da organização.

Neste âmbito, por forma a garantir que as organizações estão *compliance*, foi desenvolvida, um modelo que define os seguintes *major blocks:*

**Visão I4.0**- As organizações definem a forma como se diferenciam das demais. Para tal endereçam questões como "O que a organização pretende ser no futuro?", para definir a direção da organização. Por norma a visão realça os valores e as aspirações, que se

encontram no ADN da própria organização. A Visão tem como objetivo incentivar os colaboradores, bem como os acionistas e também os clientes. Exemplo da Visão do Instituto Politécnico de Leiria:

"Ser reconhecido por uma formação de qualidade em ciências empresariais, capaz de antecipar e responder aos desafios do mercado de trabalho e por ter capacidade de apresentar soluções em termos de investigação e de prestação de serviços." [62]

Ou numa perspetiva com foco mais empresarial, temos o exemplo da Tesla:

"to create the most compelling car company of the 21st century by driving the world's transition to electric vehicles."[63]

Este módulo pretende assim definir uma visão assente em cima da Indústria 4.0, com a aplicabilidade das infraestruturas da Internet of things e, todas as mais valias associadas à analítica possível de obter e que permitem a organização, obter vantagens competitivas face aos concorrentes diretos.

**Missão** – A missão guia a organização no seu dia-a-dia, focam-se no "hoje", com o que a organização faz, responde à questão "Quem somos?" definindo e mapeando a identidade da organização. Exemplos de definição de missões de organizações:

Instituto Politécnico de Leiria

"Promover a criação e disseminação de conhecimento em ciências empresariais através do desenvolvimento de competências e capacidades na qualificação de pessoas, investigação e prestação de serviços de qualidade, promotoras da competitividade organizacional."[62]

Tesla

"to accelerate the world's transition to sustainable transport." [63]

**Valores** – Os valores refletem os pressupostos por detrás da visão e da missão. Os valores dão dignidade e direção à missão, exemplo:

Instituto Politécnico de Leiria

"Exigência, atualidade, inovação e co-criação de valor." [62]

**Objetivos** – Tem duas componentes, uma primeira onde são definidas condições a atingir no futuro e, uma segunda componente que se foca em questões críticas e milestones, para alcançar as condições previamente definidas.

As tecnologias de operação e as tecnologias de informação, aplicam a estratégia definida pela administração e cumprem os objetivos conjuntos, que foram definidos pela organização.

Para que se cumpram os objetivos, existe a necessidade de coordenação e alinhamento entre estas duas unidades (TO e TI). Para almejarem esse alinhamento, são definidos os requisitos de negócio, o desenho da arquitetura a implementar, tendo por base a necessidade conjunta de uma infraestrutura comum ao nível da segurança.

Após esta definição da solução a implementar, as TO e as TI, são responsáveis pela implementação dessa solução, por forma a conseguirem garantir o cumprimento dos objetivos, salvaguardando assim os interesses comuns da organização.

A cooperação entre as TI's e as TO's trazem sinergias para a organização:

1º Criação de um único *single pane of glass*, permitindo ganhos de eficiência e eficácia pelo facto de existir uma única solução de segurança, transversal à organização;

2º Agilidade à organização, por de uma forma mais célere conseguir ajustar a produção à procura. Este ajuste pode ser com base na quantidade, ou com base na variedade de produtos;

3º Organização mais competitiva, por se ajustar à procura reduzindo o desperdício da produção;

4º Redução dos custos ao nível do *procurement*, pelo facto de existirem sinergias entre as TO e as TI, otimizando os custos de aquisição dos equipamentos ativos a implementar.

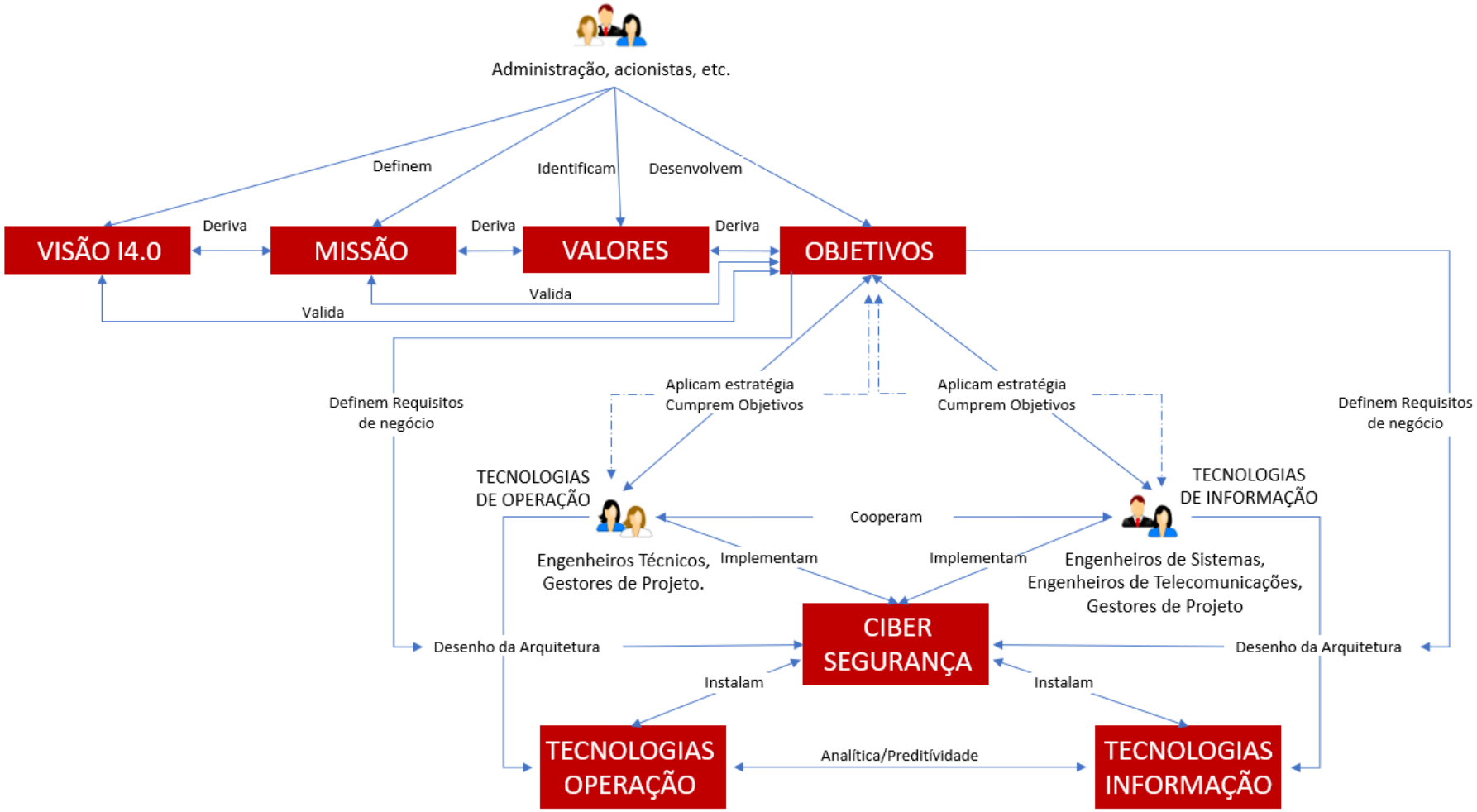



**Figura 43: Modelo (MI)$^2$4.0 na implementação de uma estratégia da Indústria 4.0**
**Fonte: Criação do Autor**

O modelo desenvolvido endereça três áreas primordiais de análise, ou seja, a Administração da Organização, as Tecnologias de Informação e, as Tecnologias de Operação.

Este modelo correlaciona as questões apresentadas, com as respostas dadas pelos utilizadores do modelo. As respostas têm uma avaliação ponderada e que permite com isso, o modelo definir ações ou apresentar os resultados correlacionados com a resposta dada o que permite às empresas, avaliar o seu grau de maturidade na implementação da estratégia na definição dos objetivos da Indústria 4.0. Esta tabela tem como objetivo o alinhamento da estratégia da empresa com a visão da mesma na Indústria 4.0, os valores resultantes dessa visão e os objetivos.

O modelo para além de permitir obter o estado de maturidade em relação à Indústria 4.0, fornece informações orientadoras em cada uma das respostas obtidas, bem como sugestões de ações a tomar para que a organização, possa prosseguir os seus objetivos na persecução da implementação da estratégia orientada à Indústria 4.0, conforme a Figura 44.

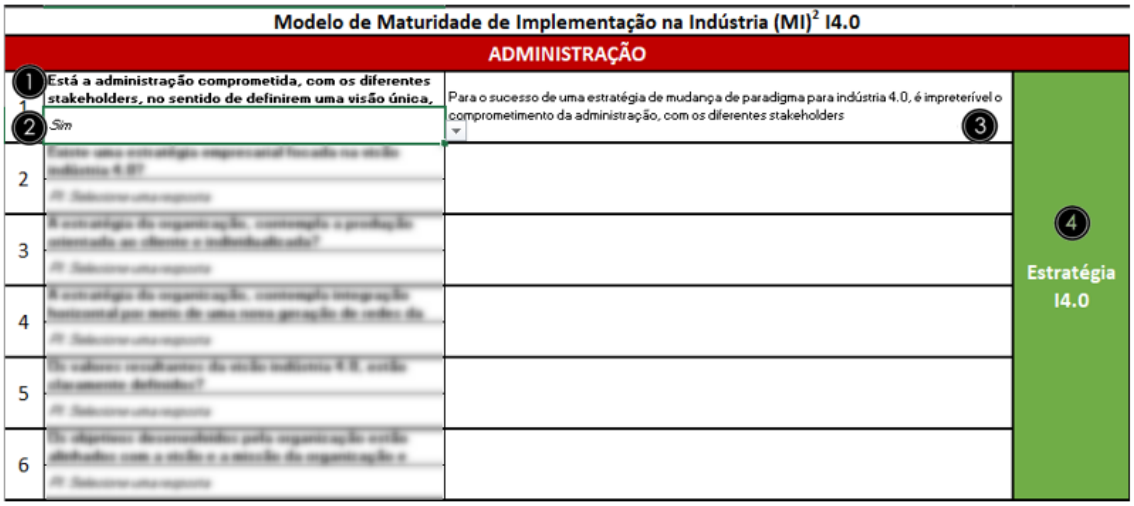



**Figura 44: Modelo (MI)2 I4.0 - Inquérito**

Legenda:

1- Questões de avaliação
2- Respostas diretas (Exemplo: 1. Sim, 2. Não, 3. Não tenho a certeza)
3- Informação que permite ao auditor percecionar o estado da arte, em cada uma das respostas
4- Resultado que vai sendo afinado ao longo do preenchimento das respostas.

O modelo permite assim percecionar o estado da arte em cada um dos blocos e no final, gerar um resultado ponderado global que agrega, a avaliação resultante dos três blocos avaliados.

Para além desta avaliação, que permite obter um resultado no final da realização da mesma, o modelo para além deste resultado, apresenta também linhas orientadores de

ações a realizar em função da resposta dada a cada uma das questões, conforme o exemplo da Figura 45.


**Figura 45: Modelo (MI)2 I4.0 – Ações**

Legenda:

1- Relatório de ações ou resultados a aplicar
2- Ação ou resultado originado pela resposta dada
3- Informação sobre o resultado que vai sendo afinado ao longo do preenchimento das respostas.

No exemplo abaixo na Figura 46, é possível verificar a mudança de estados em função das respostas dadas à mesma questão, no bloco da administração, com diferentes ações a serem tomadas em cada um dos casos.


**Figura 46: Modelo (MI)2 I4.0 – Mudança de Estados**

O modelo pretende servir de base às diferentes indústrias (Exemplos: automóvel, naval, aérea, papel, farmacêutica, alimentar, vidro, etc.) pelo que a visão, é resultado da estratégia que terá na sua génese a digitalização do chão de fábrica, sendo os valores e os objetivos resultantes desta estratégia, mapeados com a respetiva indústria.

Os objetivos variam de indústria para indústria, sendo que os mesmos vão ter na sua génese, a estratégia que definiu a visão. Estes objetivos vão delinear a competitividade da organização e o crescimento da mesma.

Estes objetivos, tem também a função de garantir que as tecnologias de operação e as tecnologias de informação, vão cooperar no sentido de cumprirem os objetivos e, vão coordenar esforços, na implementação de soluções de segurança/cibersegurança, que salvaguardem a integridade da informação das organizações, bem como a proteção da propriedade intelectual (por forma a evitar a espionagem industrial).

### Indicadores usados no bloco da Administração

**Tabela 7: Indicadores de classificação (MI)$^2$4.0 - Administração**
**Fonte: Criação do Autor**

| Questões | Descrição |
|---|---|
| Está a administração comprometida, com os diferentes stakeholders, no sentido de definirem uma visão única, na organização? | Para o sucesso de uma estratégia de mudança de paradigma para indústria 4.0, é impreterível o comprometimento da administração, com os diferentes stakeholders |
| Existe uma estratégia empresarial focada na visão indústria 4.0? | Para o sucesso da implementação de uma estratégia, é importante o alinhamento empresarial numa visão com foco na indústria 4.0, com a digitalização do chão de fábrica |
| A estratégia da organização, contempla a produção orientada ao cliente e individualizada? | As estratégias com a produção orientada ao cliente e individualizada, permitem que as organizações, possam ajustar oferta mediante as oscilações do mercado |
| A estratégia da organização, contempla a integração horizontal por meio de uma nova geração de rede da cadeia de valores global? | Verifica-se uma rede de criação de valores que são redes otimizadas em tempos real que garantem a integração da transparência, oferecem um elevado nível de flexibilidade para responderem mais rapidamente a problemas e falhas permitindo assim uma otimização global |

| | |
|---|---|
| Os valores resultantes da visão indústria 4.0, estão claramente definidos? | Os valores I4.0 resultam da identificação dos mesmos pela administração e estão intrinsecamente correlacionados com a visão |
| Os objetivos desenvolvidos pela organização estão alinhados com a visão da organização e consequentemente a indústria 4.0? | Os objetivos desenvolvidos estão em consonância, com a visão e os valores, aplicados pela organização na prossecução da indústria 4.0 |

## Indicadores Tecnologias de Operação

**Tabela 8: Indicadores de classificação (MI)$^2$4.0 – Tecnologias de Operação**
**Fonte: Criação do Autor**

| Questões | Descrição |
|---|---|
| Os sistemas das Tecnologias de Informação e as Tecnologias de Operação, convergem em conformidade com os objetivos da organização e cooperam para os atingir | Existe uma preocupação das tecnologias de operação de cumprir com os objetivos da organização e de convergir com as TI's no sentido de os atingir. |
| É considerado o potencial de agilizar e reduzir o time-to-market através do exponencial das tecnologias? | Um processo de produção profundamente automatizado, com capacidade de gerar conhecimento pelos dados que gera e a informação que disponibiliza, garante competitividade à organização e diferenciação, mantendo-se alinhada com os seus objetivos. |
| Existe capacidade de recolha de informação preditiva da linha de produção/chão de fábrica? | A implementação de uma solução assente em cima de sensores, que permitem a organização ter "visibilidade" e preditividade sobre o seu chão de fábrica, garante-lhe vantagem competitiva sobre as suas congéneres |
| Está previsto o uso de ferramentas de Inteligência Artificial e de machine learning, para garantir a análise dos dados, no sentido de os converter em informação relevante para a organização? | Os dados são a "água" dos dias de hoje, porque na realidade existem em grande quantidade, havendo necessidade de os filtrar, para a obtenção da informação desejada e essa informação é diferenciadora para os objetivos da organização. |

| | |
|---|---|
| Existe uma preocupação ao nível das tecnologias de operação de garantirem a segurança lógica do chão de fábrica em conjugação com as tecnologias de informação? | A segurança é o denominador comum para a implementação das soluções IIoT e Indústria 4.0. Ao ter a preocupação de colmatar esta necessidade a organização está em linha com os seus objetivos |
| A equipa das tecnologias de operação tem formação suficiente para tomar medidas no caso de um incidente de cibersegurança? | A organização ao dotar os seus colaboradores com formação por forma a saber como atuar aquando da ocorrência de um incidente de cibersegurança, permite que a mesma se posicione num patamar elevado de eficiência e eficácia, para alcançar os seus objetivos, desta forma a organização mantem-se em linha com os seus objetivos |
| Os fornecedores usam o próprio equipamento de hardware ou software, durante as intervenções no local? | Ao limitar o uso de equipamentos externos na sua infraestrutura a organização, controla potenciais riscos evitando expor-se aos mesmos. Desta forma a organização posiciona-se com um elevado grau de responsabilidade, garantindo o fornecimento aos seus clientes, trabalhando para os seus objetivos. |

## Indicadores Tecnologias de Informação

**Tabela 9: Indicadores de classificação (MI)²4.0 – Tecnologias de Informação**
**Fonte: Criação do Autor**

| Questões | Descrição |
|---|---|
| Os sistemas das Tecnologias de Informação e as Tecnologias de Operação, convergem em conformidade com os objetivos da organização e cooperam para os atingir | A preocupação das Ti's convergirem com as TO demonstra a preocupação desta atingir os objetivos definidos pela administração |
| Existe um repositório central contendo esquemas de equipamentos, desenhos de infraestrutura de TI e layouts de rede do sistema dentro da instalação? | O repositório atualizado, permitirá que as instalações/fábrica não interrompam o seu ciclo de produção, permitindo à organização o cumprimento dos seus deveres perante os seus clientes, com entrega de encomendas nas datas previstas, mantendo em linha com os objetivos definidos. |

| | |
|---|---|
| Identifica equipamentos críticos nas suas instalações, ou na sua fábrica, que possam causar disrupção nas operações no caso de serem comprometidos? | Os equipamentos críticos devem ser protegidos com firewalls, hardware seguro que não permita a transferências para USBs ou outros dispositivos de media externos. Esta medida permite que a organização possa continuar com a operação, mantendo-se em linha com os objetivos definidos. |
| A fábrica ou as instalações possuem procedimentos de resposta a incidentes de cibersegurança? | Medidas de resposta a incidentes previamente conhecidas pelas equipas, permitem que estas possam agir em conformidade de forma rápida e assertiva, garantindo assim uma reposição de serviço mais rápida, minimizando o impacto do incidente. |
| A sua organização disponibiliza formação básica de consciencialização de cibersegurança aos colaboradores? | A formação dos colaboradores é importantíssima pois é uma das ações que permite criar uma camada de "awareness" para situações delicadas de ameaças. A Organização ao implementar estas medidas, acautela potenciais ataques. |
| O equipamento do chão de fábrica é verificado regularmente ou automaticamente em busca de problemas de cibersegurança (por exemplo, malware, etc.) | A organização ao ter a capacidade de agendar a verificação automática do equipamento e selecionar essas configurações, elimina erros dos colaboradores, bem como garante que as mesmas irão ser realizadas pela automação. Esta medida permite que a organização se mantenha em linha com os seus objetivos |
| Estão previstas políticas de segregação das redes (ex. VLAN's), acessos remotos através de VPN's e autenticação dos utilizadores com o uso por exemplo de 2FA (dois fatores de autenticação). | A organização ao implementar estas medidas de segurança, adiciona uma camada de segurança no sentido de proteger o negócio. Esta medida permite que a organização se mantenha em linha com os seus objetivos. |

O simulador do modelo, decompõe-se assim nos seguintes módulos principais, conforme apresentado na Figura 47 :

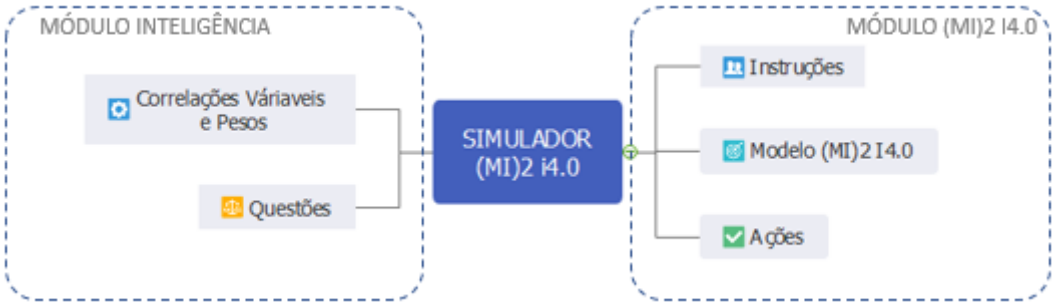



**Figura 47: Simulador (MI)2 I4.0**
**Fonte: Criação do Autor**

O Módulo de Inteligência, inclui o bloco de "Questões" que estão na base do modelo e o bloco de "Correlações Variáveis e Pesos", que está na base da inteligência do modelo, e descrito na Figura 48, onde são realizadas as correlações das respostas em conjugação com o "peso" das mesmas, que se encontra definido no simulador, concebido para o efeito.

| **Administração** | | | Mínimo | Máximo | Indicador maturidade | Estratégia I4.0 |
|---|---|---|---|---|---|---|
| Resultado Total | [illegible] | | [illegible] | [illegible] | [illegible] | Estratégia I4.0 |
| Nº de perguntas | [illegible] | | [illegible] | [illegible] | [illegible] | Alguns indicadores de uma estratégia I4.0 |
| Resultado obtido | [illegible] | | [illegible] | [illegible] | [illegible] | Não existe foco na estratégia I4.0 |
| Estratégia Tipo | Estratégia I4.0 | | [illegible] | [illegible] | [illegible] | Responda a uma questão |

**Figura 48: Correlações Variáveis e Pesos**
**Fonte: Criação do Autor**

O Módulo (MI)2 I4.0, subdivide-se em três blocos, o primeiro "Instruções", que permite ensinar os utilizadores a trabalharem com o modelo. Um segundo bloco, que é o "Modelo (MI)2 I4.0", a painel principal que permite que os utilizadores possam responder às questões e automaticamente perceberem, se a sua organização se encontra num dos três estágios:

1. "Estratégia I4.0";
2. "Alguns indicadores de uma estratégia I4.0";
3. "Não existe foco na estratégia I4.0".

O bloco das "Ações" reflete o resultado das respostas dadas no bloco "Modelo (MI)2 I4.0" e, permite aos utilizadores aferirem o resultado das suas respostas e/ou terem como resultado ações que podem despoletar no sentido de as usarem para implementar as mesmas nas suas organizações, por forma a aproximar a estratégia destas de uma estratégia mais orientada à Indústria 4.0.

É possível verificar pela Figura 49 que em função da resposta, que tem um peso associado, o resultado da estratégia varia em função dessa resposta (mudando a cor associada a cada uma), bem como descrição que resultada da opção escolhida.

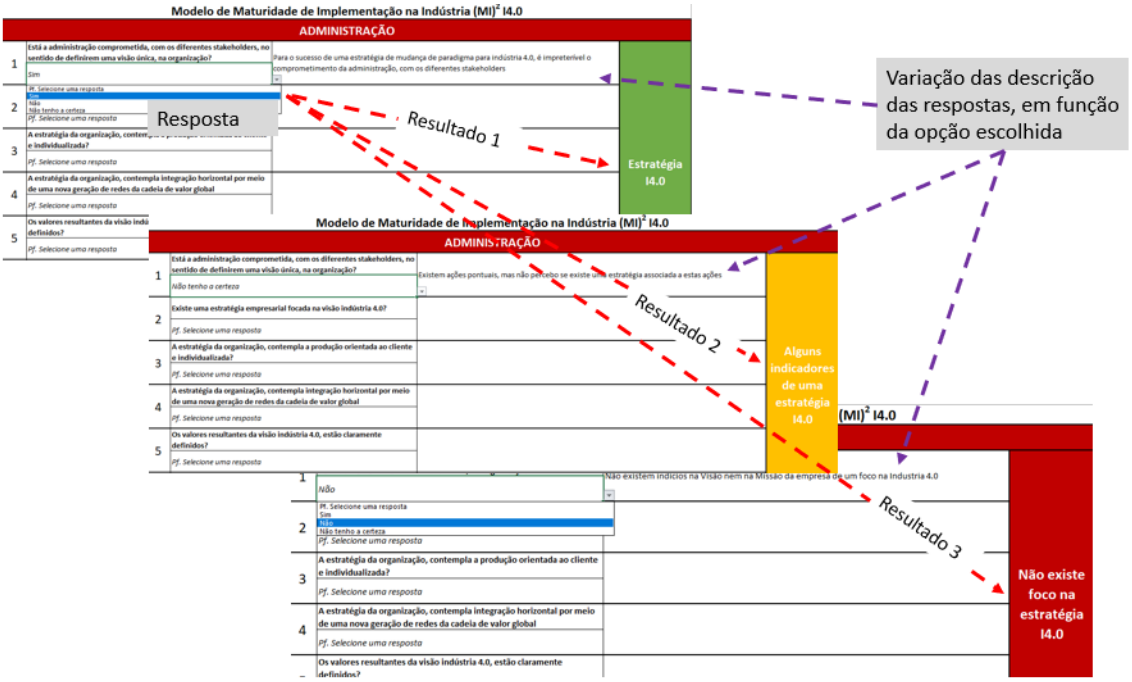



**Figura 49: Bloco "(MI)2 I4.0"**
**Fonte: Criação do Autor**

Após a seleção das respostas em cada uma das áreas (Administração, Tecnologias de Operação e Tecnologias de Informação), são gerados resultados e ações que permitem as organizações agir em conformidade, para estar alinhada com a Indústria 4.0, conforme apresentado na Figura 50.

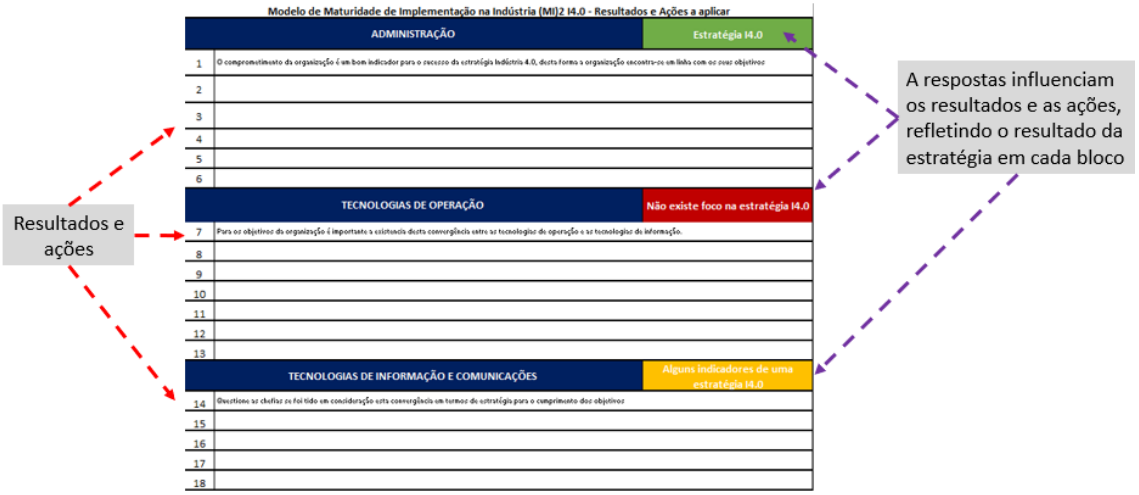



**Figura 50: Bloco "Ações"**
**Fonte: Criação do Autor**

Conforme apresentado Figura 51 é apresentado o resultado do simulador, após o preenchimento do mesmo.

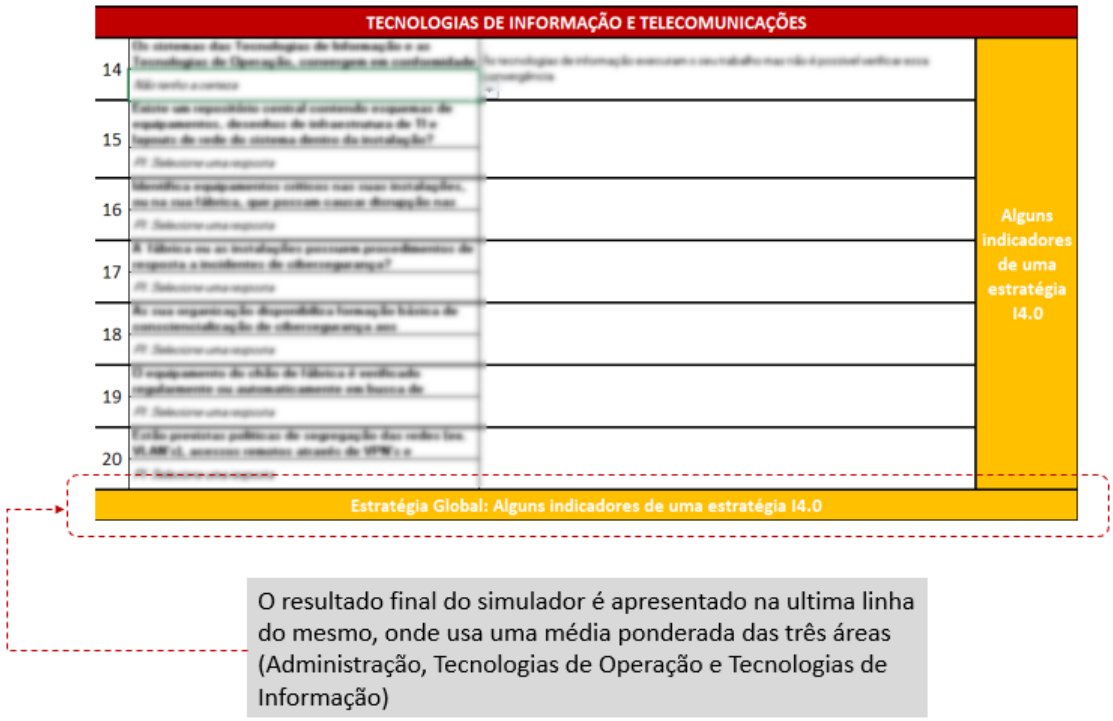



**Figura 51: Simulador - Resultado final**
**Fonte: Criação do Autor**

## 6.3. Aplicabilidade em caso de uso

Por questões de confidencialidade não é possível, identificar as organizações em estudo, nestes dois casos de uso, sendo no entanto, o mesmo estudo replicável a qualquer organização que pretenda avaliar o seu estado de maturidade, face a um tema relevante e pertinente para as organizações que se querem afirmar, nesta revolução industrial 4.0.

### 6.3.1. Caso de uso – Indústria || Aplicado às Utilities[6]

Este primeiro caso de uso aplicado a um dos setores verticais das *utilities* permitiu reforçar, todos os desenvolvimentos que foram observados ao longo de todo o processo corroborando, a conclusão no desfecho final do projeto em questão. A análise realizada pretende aferir se a organização em estudo, tinha um foco delineado uma estratégia da Indústria 4.0. Em nenhuma altura, será feita referência ao nome da organização ou a eventuais detalhes do projeto, por questões de confidencialidade.

O modelo desenvolvido conforme resumido na Figura 52, contempla três blocos distintos, o primeiro que incide sobre a responsabilidade de administração no processo, o segundo bloco incide sobre as equipas de tecnologias de operação e, um terceiro bloco que incide sobre as equipas de tecnologias de informação. O resultado da análise é obtido através da conjugação do resultado obtido dos três blocos.

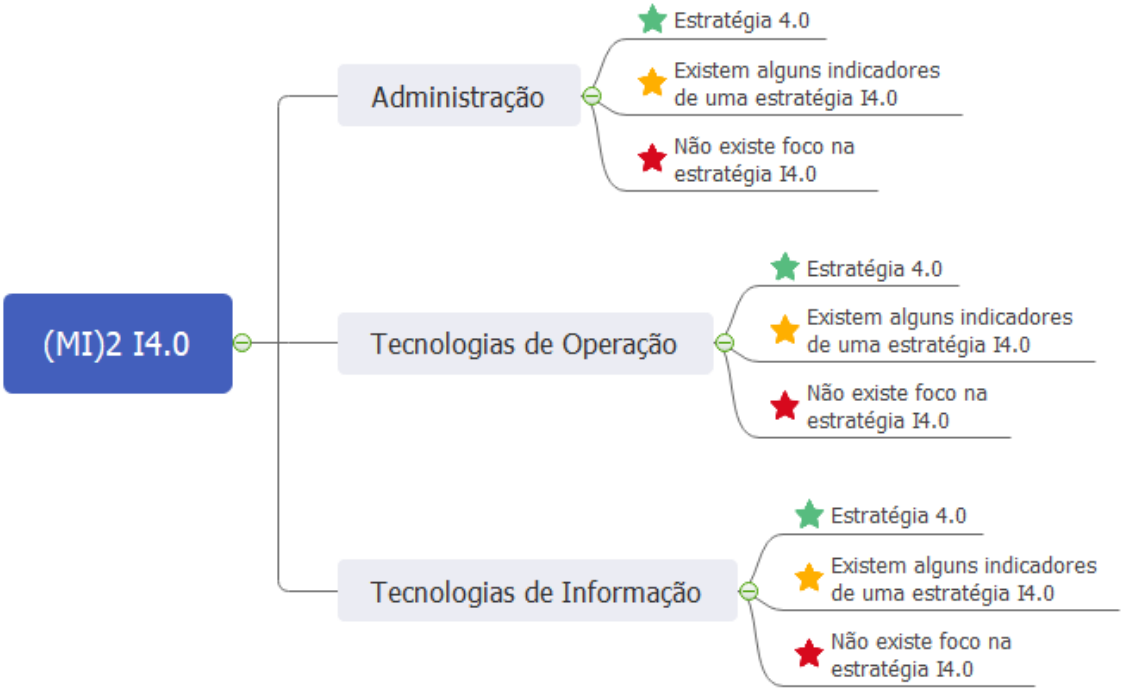



**Figura 52: Modelo (MI)2 I4.0 – Blocos**
**Fonte: Criação do Autor**

[6] Utilities – Setor que inclui o setor das águas, gás e energia.

A análise realizada sobre o bloco de administração resultou, na identificação de alguns indicadores que indiciam a existência de uma estratégia orientada à Indústria 4.0, cf. Figura 53.

**Modelo de Maturidade de Implementação na Indústria (MI)$^2$ I4.0**

| ADMINISTRAÇÃO | | | |
|---|---|---|---|
| 1 | **Está a administração comprometida, com os diferentes stakeholders, no sentido de definirem uma visão única, na organização?**<br>*Não* | Não existem indícios na Visão nem na Missão da empresa de um foco na Industria 4.0 | **Alguns indicadores de uma estratégia I4.0** |
| 2 | **Existe uma estratégia empresarial focada na visão indústria 4.0?**<br>*Não tenho a certeza* | É importante reconhecer a existencia da estratégia, o facto de esta não ser precetivel indicia eventualmente um fraco compromisso com a mesma. | |
| 3 | **A estratégia da organização, contempla a produção orientada ao cliente e individualizada?**<br>*Sim* | Existe uma estratégia que permite a organização reagir de forma rápida à procura | |
| 4 | **A estratégia da organização, contempla integração horizontal por meio de uma nova geração de redes da cadeia de valor global**<br>*Sim* | Verifica-se uma rede de criação de valores que são redes otimizadas em tempos real que garantem a integração da transparência, oferecem um elevado nível de flexibilidade para responderem mais rapidamente a problemas e falhas permitindo assim uma otimização global | |
| 5 | **Os valores resultantes da visão indústria 4.0, estão claramente definidos?**<br>*Não* | Estes objetivos não estão mapeados com a visão e não é possivel relacioná-los com os objetivos | |
| 6 | **Os objetivos desenvolvidos pela organização estão alinhados com a visão e a missão da organização e consequentemente a indústria 4.0?**<br>*Sim* | Os objetivos desenvolvidos estão em consonância, com a visão e os valores, aplicados pela organização na prossecução da indústria 4.0 | |

**Figura 53: Modelo de Maturidade de Implementação da Indústria 4.0 – Administração**
**Fonte: Criação do Autor**

A análise do bloco sobre as Tecnologias de Operação, refletiu uma realidade diferente onde não foram identificados indicadores, que permitam identificar o posicionamento desta equipa, com o focus numa estratégia orientada à Indústria 4.0 cf. Figura 54.

| TECNOLOGIAS DE OPERAÇÃO | | | |
|---|---|---|---|
| 7 | **Os sistemas das Tecnologias de Operação e as Tecnologias de Informação, convergem em conformidade com os objetivos da organização e cooperam para os atingir**<br>*Não* | As tecnologias de operação trabalham com o intuito de atingir os seus objetivos, com foco apenas no seu silo. | **Não existe foco na estratégia I4.0** |
| 8 | **É considerado o potencial de agilizar e reduzir o time-to-market através do exponencial das tecnologias?**<br>*Sim* | Verifica-se um elevado nível de automação por forma a tornar e dotar a produção de conhecimento cognitivo e altamente autónomo. | |
| 9 | **Existe capacidade de recolha de informação preditiva da linha de produção/chão de fábrica?**<br>*Não* | As infraestruturas não estão preparadas no sentido de recolherem informação, que lhes permita atuarem de forma proativa, em relação a eventos e oscilações que possam causar paragens não programadas e com isso afetar entregas a clientes, com custos associados. | |
| 10 | **Está previsto o uso de ferramentas de inteligência artificial e de machine learning, para garantir a análise**<br>*Não* | Não está previsto a implementações de plataformas de inteligência artificial e/ou machine learning. | |
| 11 | **Existe uma preocupação ao nível das tecnologias de operação de garantirem a segurança lógica do chão de fábrica em conjugação com as tecnologias de informação?**<br>*Não* | Existe uma preocupação da organização de ter segurança do perimetro, sem acautelar a segurança ao nivel lógico do chão de fábrica. | |
| 12 | **A equipa da tecnologias de operação tem formação suficiente para tomar medidas no caso de um incidente de cibersegurança?**<br>*Não* | Se um evento de cibersegurança ocorrer, pode haver problemas com um shutdown seguro e sem danos. Além disso, se as funções não forem devidamente articuladas e ninguém souber com quem entrar em contato com relação a possíveis soluções para o sistema, o shutdown pode ser prolongado. | |
| 13 | **Os fornecedores usam o próprio equipamento de hardware ou software, durante as intervenções no local?**<br>*Sim, os fornecedores trazem seus próprios equipamentos, laptops e dispositivos de armazenamento (por exemplo, pen drives, cartões SD etc.), que usam para reparar os sistemas* | Permitir que os fornecedores tragam hardware e software para suas instalações / Fábrica pode resultar em um risco maior de vírus ou malware entrarnos seus sistemas. Como resultado, entender exatamente o que os fornecedores trazem para o local é fundamental para manter um perímetro seguro em torno das instalações e dos ICS. | |

**Figura 54: Modelo de Maturidade de Implementação da Indústria 4.0 – Tecnologias de Operação**
**Fonte: Criação do Autor**

A nível das equipas das Tecnologias de Informação, verificaram-se alguns indicadores com uma base na estratégia orientada Indústria 4.0, cf. Figura 55.

| TECNOLOGIAS DE INFORMAÇÃO E TELECOMUNICAÇÕES | | | |
|---|---|---|---|
| 14 | **Os sistemas das Tecnologias de Informação e as Tecnologias de Operação, convergem em conformidade com os objetivos da organização e cooperam para os atingir**<br>*Não tenho a certeza* | As tecnologias de informação executam o seu trabalho mas não é possivel verificar essa convergência | **Alguns indicadores de uma estratégia I4.0** |
| 15 | **Existe um repositório central contendo esquemas de equipamentos, desenhos de infraestrutura de TI e layouts de rede do sistema dentro da instalação?**<br>*Não tenho a certeza* | É importante entender se existe um repositório central para esquemas de equipamentos, desenhos de infraestrutura de TI e layouts de rede do sistema. Equipamentos e esquemas de TI ajudam no caso de uma paragem de emergência. Se os fornecedores precisarem de aceder e inadvertidamente limparem o sistema, será necessário ser minucioso e verificar todos os componentes do sistema. | |
| 16 | **Identifica equipamentos criticos nas suas instalações, ou na sua fábrica, que possam causar disrupção nas operações no caso de serem comprometidos?**<br>*Sim* | Os equipamentos críticos são os sistemas que, no caso de ficarem inoperacionais, desligariam toda a fábrica. Ser capaz de identificar esses sistemas diminuirá o risco de interrupção. | |
| 17 | **A fábrica ou as instalações possuem procedimentos de resposta a incidentes de cibersegurança?**<br>*Não* | Sem um procedimento de resolução de incidentes de cibersegurança, a equipa pode não estar ciente das medidas apropriadas a serem tomadas e podem ocorrer grandes interrupções, incluindo o desligar total ou parcial da fábrica | |
| 18 | **As sua organização disponibiliza formação básica de consciencialização de cibersegurança aos colaboradores?**<br>*Sim* | A formação regular dos colaboradores na conduta adequada de funcionamento nos equipamentos da empresa pode ajudar a prevenir downloads acidentais de vírus e outras vulnerabilidades do sistema. | |
| 19 | **O equipamento do chão de fábrica é verificado regularmente ou automaticamente em busca de problemas de cibersegurança (por exemplo, malware, etc.)**<br>*Não tenho a certeza* | É importante perceber a capacidade das suas instalações fazerem inspeções de forma regular ou automática, em busca de problemas de cibersegurança no sentido de garantir a integridade dos sistemas e evitar riscos de segurança. | |
| 20 | **Estão previstas politicas de segregação das redes (ex. VLAN's), acessos remotos através de VPN's e autenticação dos utilizadores com o uso por exemplo de 2FA (dois fatores de autenticação)**<br>*Sim* | Uma das preocupações subjacentes à implementação de soluções IIoT ou com foco na Industria 4.0 é minizar as vulnerabilidades ao expandirmos ao superficie de ataque, pelo que as medidas de segurança básicas (ex. criação de VLAN's, VPN's, 2FA, etc.) são medidas pertinentes | |
| **Estratégia Global: Alguns indicadores de uma estratégia I4.0** | | | |

**Figura 55: Modelo de Maturidade de Implementação da Indústria 4.0 – Tecnologias de Informação**
**Fonte: Criação do Autor**

No final do bloco é apresentado (barra amarela) o estado de maturidade da organização. No caso em análise verificam-se a presença de alguns indicadores, que demonstram a existência de um início de uma estratégia orientada à Indústria 4.0.

Com base nas respostas dadas no preenchimento do modelo, são sugeridas ações em cada um dos módulos, no sentido de ajudar as organizações na definição da estratégia com foco na Indústria 4.0. A Figura 56, reflete as ações a tomar com a administração da organização no sentido corrigir/ajustar a estratégia.

| Modelo de Maturidade de Implementação na Indústria (MI)2 I4.0 - Resultados e Ações a aplicar | | |
|---|---|---|
| **ADMINISTRAÇÃO** | | **Alguns indicadores de uma estratégia I4.0** |
| 1 | Questionar a administração e os respetivos stakeholders, no sentido de perceber se existe uma estratégia, delineada na Industria 4.0 no sentido de se diferenciarem da concorrência. | |
| 2 | Questionar as chefias, qual o compromisso da organização no sentido de perceber a existencia ou não de uma estratégia com foco na Indústria 4.0 | |
| 3 | A estratégia orientada à produção orientada ao cliente e de forma indivualizada, garante agilidade à organização que lhe permite obter vantagens, face à concorrência, desta forma a organização encontra-se em linha com os seus objetivos | |
| 4 | As organização ao criar valor pela geração de rede da cadeia de valor global, garante competividade e desta forma a organização encontra-se em linha com os seus objetivos | |
| 5 | É importante para a organização, dar a conhecer o seu comprometimento em termos de visão, missão, valores e objetivos | |
| 6 | A definição clara dos valores da objetivos, marca de forma vincada o comprometimento da organização em os alcançar e, desta forma a organização encontra-se em linha com a sua visão e missão. | |

**Figura 56: Modelo de Maturidade de Implementação da Indústria 4.0 – Ações Administração**
**Fonte: Criação do Autor**

A Figura 57, apresenta as ações resultantes das respostas obtidas, no modelo $(MI)^2$ I4.0 na componente das tecnologias de operação.

| | TECNOLOGIAS DE OPERAÇÃO | Não existe foco na estratégia I4.0 |
|---|---|---|
| 7 | Para os objetivos da organização é importante a existencia desta convergência entre as tecnologias de operação e as tecnologias de informação. | |
| 8 | Um processo de produção profundamente automatizado, com capacidade de gerar conhecimento pelos dados que gera e a informação que disponibiliza, garante competitividade à organização e diferenciação, mantendo-se alinhada com os seus objetivos. | |
| 9 | Para responder de forma eficaz e eficiente, é importante que a organização, consiga ter dados que lhes permitam, serem proativas em termos de operação, por forma a garantir a continuidade da operação. | |
| 10 | A elevada quantidade de dados gerados pelas soluções de sensores instalados ao longo da linha de produção/chão de fábrica, são tratados por soluções de inteligencia artificial e/ou machine learning garantindo à organização a correta interpretação dos mesmo por forma a tomarem a melhor decisão, antecipando possiveis flutuações que possam vir a ocorrer na linha de produção. | |
| 11 | Muitas das soluções usadas ao nivel de segurança em termos de perimetro, não fazem a verificação de protocolos industriais usados no chão de fábrica, como pofinet, modbus, etc. É recomendado a criação de layers diferenciados ao longo da rede para garantir a proteção da mesma e minimizar potenciais ataques contra a mesma. | |
| 12 | Forme os colaboradores para responder a um evento de cibersegurança para ajudar a evitar o tempo de inatividade e, consequentemente minimizar os custos de reparação/recuperação, que representam as maiores despesas. | |
| 13 | Desenvolvimento de procedimentos de formação para fornecedores que trabalham no local, informando-os sobre as melhores práticas de cibersegurança. Recomenda-se também desenvolvimento de diretrizes sobre quais fornecedores de equipamentos podem trazer para a fábrica/instalações por forma a aumentar a segurança no local. | |

**Figura 57: Modelo de Maturidade de Implementação da Indústria 4.0 – Ações Tec. Operação**
**Fonte: Criação do Autor**

Em conclusão as ações a realizar, obtidas a partir do resultado das respostas obtidas no bloco das tecnologias de informação, conforme apresentado na Figura 58.

| | TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÕES | Alguns indicadores de uma estratégia I4.0 |
|---|---|---|
| 14 | Questione as chefias se foi tido em consideração esta convergência em termos de estratégia para o cumprimento dos objetivos | |
| 15 | Consulte as equipas de TI e de TO para determinar se existe ou não um repositório central dessas informações. Caso contrário, trabalhe com estas equipas para criar um repositório central, contendo informações sobre todos os sistemas de TI e ICS. Deverá de ser considerado manter este recurso offline, separado do sistema de TI da fábrica, (i.e. num computador isolado, num servidor ou num arquivo físico isolado), para garantir que as informações possam posteriormente ser acedidasis quando o sistema de TI for desligado, durante um ciber ataque ou uma eventual interrupção do sistema. | |
| 16 | Os equipamentos críticos devem ser protegidos com firewalls, hardware seguro que não permita a transferências para USBs ou outros dispositivos de media externos. Esta medida permite que a organização possa continuar com a operação, mantendo-se em linha com os objetivos definidos. | |
| 17 | Envolva uma equipa multifuncional para desenvolver um procedimento de resposta a incidentes de cibersegurança que descreva as funções, responsabilidades e o formação necessário para a equipa responder a eventos de cibersegurança. | |
| 18 | A formação dos colaboradores é importantíssima pois é uma das ações que permite criar uma camada de "awareness" para situações delicadas de ameaças. A organização ao implementar estas medidas, acautela potenciais ataques. | |
| 19 | Verificar com a equipa das tecnologias de informação para fazer um inventário de quais equipamentos têm software para fazer o scan em busca de problemas de cibersegurança e validar também com que frequência os scanners são executados. | |
| 20 | A organização ao implementar estas medidas de segurança, adiciona uma camada adicional de segurança no sentido de proteger o negócio. Esta medida permite que a organização se mantenha em linha com os seus objetivos. | |

**Figura 58: Modelo de Maturidade de Implementação da Indústria 4.0 – Ações Tec. Informação**
**Fonte: Criação do Autor**

O resultado do caso de uso resultou na conclusão de que existiam alguns indicadores de uma estratégia I4.0, indicadores esses que não eram suficientes, para posicionar a organização num patamar de uma estratégia I4.0, conforme é possível verificar na Figura 59.

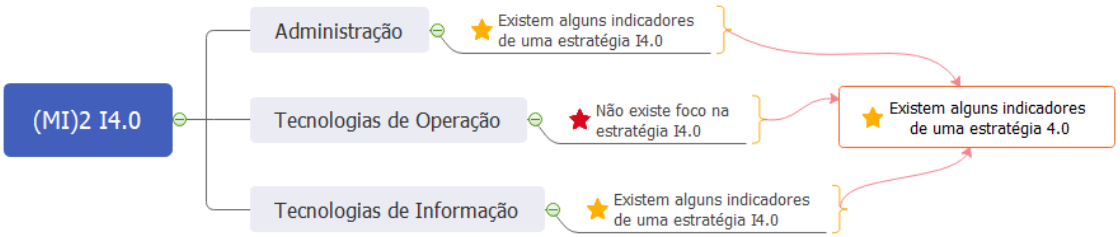



**Figura 59: Resultado caso de uso Indústria com modelo (MI)2 I4.0**
**Fonte: Criação do Autor**

Esta análise do caso de estudo desta organização, permitiu concluir que existem bases para a persecução de uma estratégia focada na Indústria 4.0.

Verificaram-se algumas debilidades ao nível das tecnologias de operação, que se encontravam numa fase de maturidade inicial, sendo que as tecnologias de informação e a administração, se encontram numa fase intermédia, ou seja, numa fase mais madura, para poderem integrar de forma mais rápida uma estratégia focada na Indústria 4.0.

O modelo desenvolvido, permitiu corroborar o use case, com a aplicabilidade prática do mesmo num exemplo real ao nível das organizações.

### 6.3.2. Caso de uso – Smart Buildings || Aplicada ao Setor Financeiro e Seguros

O segundo caso incide sobre uma nova área associada aos *smart buildings*, onde existe uma tendência de investimento, no sentido de rentabilizar o "custo do dinheiro" de forma mais célere. O caso em concreto incide sobre o setor financeiro e de seguros, sendo que em nenhuma altura, será feita referência ao nome da organização ou a eventuais detalhes do projeto, por questões de confidencialidade.

A análise realizada, usa o modelo desenvolvido (MI)$^2$ I4.0, "tripartido" conforme apresentada no primeiro use case e reforçada pela Figura 60, onde o resultado da análise é obtido através da conjugação do resultado obtido dos três blocos.

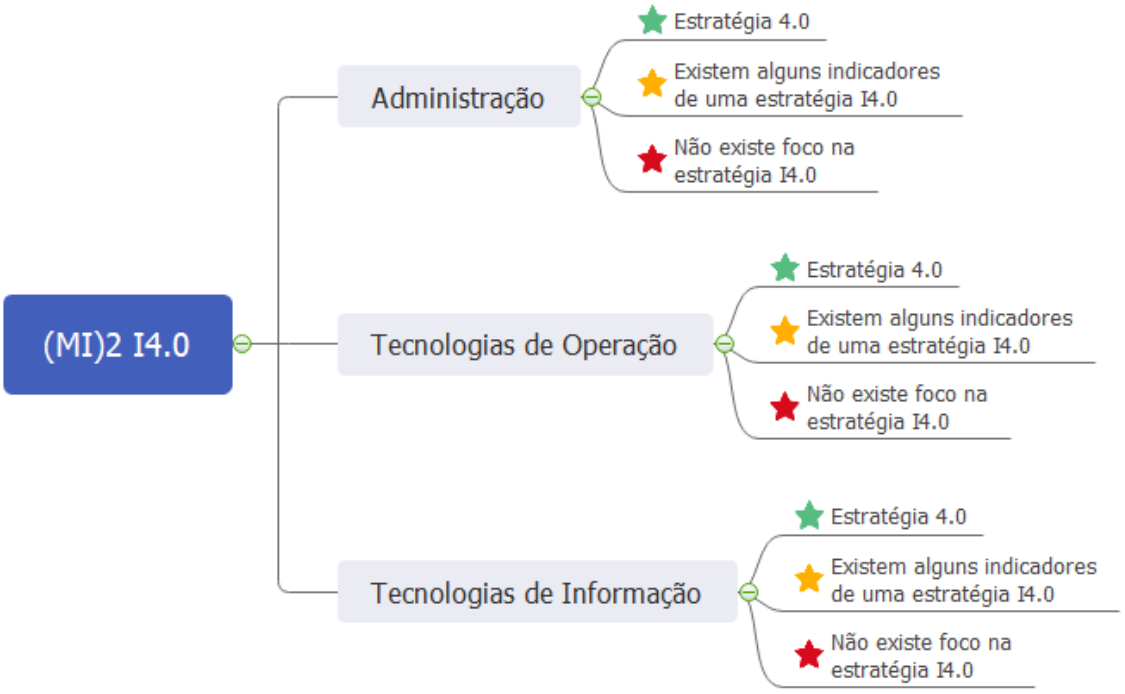



**Figura 60: Modelo (MI)2 I4.0 – Blocos**
**Fonte: Criação do Autor**

A análise realizada sobre o bloco de administração resultou, que a administração se encontra perfeitamente alerta para os desafios inerentes à Indústria 4.0 e mapeia essa necessidade na visão e objetivos da organização, cf. Figura 61.

| Modelo de Maturidade de Implementação na Indústria (MI)² I4.0 | | | |
|---|---|---|---|
| **ADMINISTRAÇÃO** | | | |
| 1 | **Está a administração comprometida, com os diferentes stakeholders, no sentido de definirem uma visão única,**<br>*Sim* | Para o sucesso de uma estratégia de mudança de paradigma para indústria 4.0, é impreterível o comprometimento da administração, com os diferentes stakeholders | Estratégia I4.0 |
| 2 | **Existe uma estratégia empresarial focada na visão indústria 4.0?**<br>*Sim* | Para o sucesso da implementação de uma estratégia, é importante o alinhamento empresarial numa visão com foco na indústria 4.0, com a digitalização do chão de fábrica | |
| 3 | **A estratégia da organização, contempla a produção orientada ao cliente e individualizada?**<br>*Sim* | Existe uma estratégia que permite a organização reagir de forma rápida à procura | |
| 4 | **A estratégia da organização, contempla integração horizontal por meio de uma nova geração de redes da cadeia de valor global**<br>*Sim* | Verifica-se uma rede de criação de valores que são redes otimizadas em tempos real que garantem a integração da transparência, oferecem um elevado nível de flexibilidade para responderem mais rapidamente a problemas e falhas permitindo assim uma otimização global | |
| 5 | **Os valores resultantes da visão indústria 4.0, estão claramente definidos?**<br>*Sim* | Os valores I4.0 resultam da identificação dos mesmos pela administração e estão intrinsecamente correlacionados com a visão | |
| 6 | **Os objetivos desenvolvidos pela organização estão alinhados com a visão e a missão da organização e consequentemente a indústria 4.0?**<br>*Sim* | Os objetivos desenvolvidos estão em consonância, com a visão e os valores, aplicados pela organização na prossecução da indústria 4.0 | |

**Figura 61: Modelo de Maturidade de Implementação da Indústria 4.0 – Administração**
**Fonte: Criação do Autor**

Num *Smart Building*, não existe o chão de fábrica, no entanto essa análise é efetuada sobre as tecnologias de operação, que tem como objetivo garantir toda a operacionalidade do edifício ao nível do HVAC, energia, etc. e, que usam no seu dia-a-dia protocolos industriais. A análise realizada sobre o bloco das Tecnologias de Operação resultou, na identificação de alguns indicadores, que indiciam a existência de uma estratégia orientada à Indústria 4.0, cf. Figura 62.

| **TECNOLOGIAS DE OPERAÇÃO** | | | |
|---|---|---|---|
| 7 | **Os sistemas das Tecnologias de Operação e as Tecnologias de Informação, convergem em conformidade com os objetivos da organização e cooperam para os atingir**<br>*Sim* | Existe uma preocupação das tecnologias de operação de cumprirem com os objetivos da organização e de convergir com as TI's no sentido de os atingir. | Alguns indicadores de uma estratégia I4.0 |
| 8 | **É considerado o potencial de agilizar e reduzir o time-to-market através do exponencial das**<br>*Sim* | Verifica-se um elevado nível de automação por forma a tornar e dotar a produção de conhecimento cognitivo e altamente autónomo. | |
| 9 | **Existe capacidade de recolha de informação preditiva da linha de produção/chão de fábrica?**<br>*Não tenho a certeza* | Não é totalmente claro que a informação recolhida da linha de produção/chão de fábrica, seja informação preditiva que permita a organização tomar medidas proativas. | |
| 10 | **Está previsto o uso de ferramentas de inteligência artificial e de machine learning, para garantir a análise dos dados, no sentido de os converter em informação relevante para a organização?**<br>*Sim* | É um cenário previsto que mapeia com a estratégia da organização para alcançar os objetivos definidos e permitem os dados recolhidos pelos sensores gerem informação mais precisa e ajustada. | |
| 11 | **Existe uma preocupação ao nível das tecnologias de operação de garantirem a segurança lógica do chão de fábrica em conjugação com as tecnologias de informação?**<br>*Não tenho a certeza* | Não é perceptivel o uso de firewalls para garantirem a segurança ao nivel do chão de fábrica. | |
| 12 | **A equipa da tecnologias de operação tem formação suficiente para tomar medidas no caso de um incidente de cibersegurança?**<br>*Não tenho a certeza* | Saber se a equipa está ou não designada e treinada na resposta a incidentes de cibersegurança pode ajudar a prevenir custos significativos. | |
| 13 | **Os fornecedores usam o próprio equipamento de hardware ou software, durante as intervenções no local?**<br>*Sim, os fornecedores trazem seus próprios equipamentos, laptops e dispositivos de armazenamento (por exemplo, pen drives, cartões SD etc.), que usam para reparar os sistemas* | Permitir que os fornecedores tragam hardware e software para suas instalações / Fábrica pode resultar em um risco maior de vírus ou malware entrarnos seus sistemas. Como resultado, entender exatamente o que os fornecedores trazem para o local é fundamental para manter um perímetro seguro em torno das instalações e dos ICS. | |

**Figura 62: Modelo de Maturidade de Implementação da Indústria 4.0 – Tecnologias de Operação**
**Fonte: Criação do Autor**

A nível das equipas das Tecnologias de Informação, verifica-se a existência de indicadores claros com uma base na estratégia orientada Indústria 4.0, cf. Figura 63.

| TECNOLOGIAS DE INFORMAÇÃO E TELECOMUNICAÇÕES | | | |
|---|---|---|---|
| 14 | **Os sistemas das Tecnologias de Informação e as Tecnologias de Operação, convergem em conformidade com os objetivos da organização e cooperam para os atingir**<br>*Sim* | Existe uma preocupação das tecnologias de informação de cumprir com os objetivos da organização e de convergir com as tecnologias de operação no sentido de os atingir. | Estratégia I4.0 |
| 15 | **Existe um repositório central contendo esquemas de equipamentos, desenhos de infraestrutura de TI e layouts de rede do sistema dentro da instalação?**<br>*Sim* | Equipamentos e esquemas de TI e TO's ajudarão no caso de uma paragem de emergência. Se os fornecedores precisarem de aceder e inadvertidamente limparem o sistema, será necessário ser minucioso e verificar todos os componentes do sistema. É importante manter este repositório atualizado à medida que se adicionam novas linhas de produção ou se atualizam equipamentos | |
| 16 | **Identifica equipamentos criticos nas suas instalações, ou na sua fábrica, que possam causar disrupção nas operações no caso de serem comprometidos?**<br>*Sim* | Os equipamentos críticos são os sistemas que, no caso de ficarem inoperacionais, desligariam toda a fábrica. Ser capaz de identificar esses sistemas diminuirá o risco de interrupção. | |
| 17 | **A fábrica ou as instalações possuem procedimentos de resposta a incidentes de**<br>*Sim* | Um procedimento de resposta a incidentes de cibersegurança ajuda a garantir que uma equipa tenha os recursos apropriados e reconheça as ações críticas necessárias para responder a vários incidentes, incluindo por exemplo, intempéries e ciberataques, caso ocorram. | |
| 18 | **As sua organização disponibiliza formação básica de consciencialização de cibersegurança aos colaboradores?**<br>*Não tenho a certeza* | É importante saber se as formações regulares estão a correr ou não. Sem formação, as atividades dos colaboradores podem representar um risco significativo para os ativos da empresa. | |
| 19 | **O equipamento do chão de fábrica é verificado regularmente ou automaticamente em busca de problemas de cibersegurança (por exemplo, malware, etc.)**<br>*Não tenho a certeza* | É importante perceber a capacidade das suas instalações fazerem inspeções de forma regular ou automática, em busca de problemas de cibersegurança no sentido de garantir a integridade dos sistemas e evitar riscos de segurança. | |
| 20 | **Estão previstas politicas de segregação das redes (ex. VLAN's), acessos remotos através de VPN's e autenticação dos utilizadores com o uso por exemplo de 2FA (dois fatores de autenticação)**<br>*Sim* | Uma das preocupações subajcentes à implementação de soluções IIoT ou com foco na Industria 4.0 é minizar as vulnerabilidades ao expandirmos ao superficie de ataque, pelo que as medidas de segurança básicas (ex. criação de VLAN's, VPN's, 2FA, etc.) são medidas pertinentes | |
| Estratégia Global: Estratégia I4.0 | | | |

**Figura 63: Modelo de Maturidade de Implementação da Indústria 4.0 – Tecnologias de Informação**
**Fonte: Criação do Autor**

No final do bloco é apresentado (barra verde) o estado de maturidade da organização. No caso em análise verificam-se a existência de indicadores, que demonstram um alinhamento claro de uma estratégia orientada à Indústria 4.0.

Com base nas respostas dadas no preenchimento do modelo, são sugeridas ações em cada um dos módulos, no sentido de ajudar as organizações na definição da estratégia com foco na Indústria 4.0. A Figura 64Figura 56, reforça os resultado obtidos com as respostas dadas pela a administração da organização e o seu comprometimento com estratégia.

| Modelo de Maturidade de Implementação na Indústria (MI)2 I4.0 - Resultados e Ações a aplicar | | |
|---|---|---|
| ADMINISTRAÇÃO | | Estratégia I4.0 |
| 1 | O comprometimento da organização é um bom indicador para o sucesso da estratégia Indústria 4.0, desta forma a organização encontra-se em linha com os seus objetivos | |
| 2 | A visão bem definida com foco na industria 4.0, por parte da organização permite a que a mesma se posicione melhor face às suas congéneres, desta forma a organização encontra-se em linha com os seus objetivos. | |
| 3 | A estratégia orientada à produção orientada ao cliente e de forma indivualizada, garante agilidade à organização que lhe permite obter vantagens, face à concorrência, desta forma a organização encontra-se em linha com os seus objetivos | |
| 4 | As organização ao criar valor pela geração de rede da cadeia de valor global, garante competividade e desta forma a organização encontra-se em linha com os seus objetivos | |
| 5 | A definição clara dos valores da organização, marca de forma vincada os quais pela mesma se rege, desta forma a organização encontra-se em linha com a sua visão e missão. | |
| 6 | A definição clara dos valores da objetivos, marca de forma vincada o comprometimento da organização em os alcançar e, desta forma a organização encontra-se em linha com a sua visão e missão. | |

**Figura 64: Modelo de Maturidade de Implementação da Indústria 4.0 – Ações Administração**
**Fonte: Criação do Autor**

A Figura 65, apresenta as ações resultantes das respostas obtidas, no modelo (MI)$^2$ I4.0 na componente das tecnologias de operação verificando-se a existência de alguns indicadores com foco na Indústria 4.0, reforçando as sugestões com ações a tomar para ajustar a sua estratégia nesse sentido.

| | TECNOLOGIAS DE OPERAÇÃO | Alguns indicadores de uma estratégia I4.0 |
|---|---|---|
| 7 | A preocupação das TO's convergirem com as TI's demonstra a preocupação desta atingir os objetivos definidos pela administração | |
| 8 | Um processo de produção profundamente automatizado, com capacidade de gerar conhecimento pelos dados que gera e a informação que disponibiliza, garante competitividade à organização e diferenciação, mantendo-se alinhada com os seus objetivos. | |
| 9 | Questione as chefias se a informação recolhida na linha de produção/chão de fábrica é, informação preditiva que possibilite a organização tomar medidas que possibilitem a tomada de decisão de forma proativa | |
| 10 | Os dados são a "água" dos dias de hoje, porque na realidade existem em grande quantidade, havendo necessidade de os filtrar, para a obtenção da informação desejada e essa informação é diferenciadora para os objetivos da organização. | |
| 11 | Questione as chefias no sentido de perceber se as medidas de segurança, contemplam o chão de fábrica. | |
| 12 | Trabalhe com as equipas das tecnologias de operação e a equipas das tecnologias de Informação para determinar se a equipa foi designada e formada para responder a problemas de cibersegurança. Se não tiverem formação, designe e forme a equipa para responder a um evento de cibersegurança para ajudar a evitar o tempo de inatividade e minimizar os custos de reparação que representam as maiores despesas. | |
| 13 | Desenvolvimento de procedimentos de formação para fornecedores que trabalham no local, informando-os sobre as melhores práticas de cibersegurança. Recomenda-se também desenvolvimento de diretrizes sobre quais fornecedores de equipamentos podem trazer para a fábrica/instalações por forma a aumentar a segurança no local. | |

**Figura 65: Modelo de Maturidade de Implementação da Indústria 4.0 – Ações Tec. Operação**
**Fonte: Criação do Autor**

Em conclusão as ações a realizar, obtidas a partir do resultado do bloco das tecnologias de informação, conforme apresentado na Figura 66.

| | TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÕES | Estratégia I4.0 |
|---|---|---|
| 14 | A preocupação das Ti's convergirem com as TO demonstra a preocupação desta atingir os objetivos definidos pela administração | |
| 15 | O repositório atualizado, permitirá que as instalações/fábrica não interrompam o seu ciclo de produção, permitindo à organização o cumprimento dos seus deveres perante os seus clientes, com entrega de encomendas nas datas previstas, mantendo em linha com os objetivos definidos. | |
| 16 | Os equipamentos críticos devem ser protegidos com firewalls, hardware seguro que não permita a transferências para USBs ou outros dispositivos de media externos. Esta medida permite que a organização possa continuar com a operação, mantendo-se em linha com os objetivos definidos. | |
| 17 | Medidas de resposta a incidentes previamente conhecidas pelas equipas, permitem que estas possam agir em conformidade de forma rápida e assertiva, garantindo assim uma reposição de serviço mais rápida, minimizando o impacto do incidente. | |
| 18 | Questionar o departamento das tecnologias de informação se ocorrem formações regulares de cibersegurança para colaboradores. Caso contrário, desenvolver procedimentos de formação para colaboradores que os formem sobre as melhores práticas de cibersegurança. | |
| 19 | Verificar com a equipa das tecnologias de informação para fazer um inventário de quais equipamentos têm software para fazer o scan em busca de problemas de cibersegurança e validar também com que frequência os scanners são executados. | |
| 20 | A organização ao implementar estas medidas de segurança, adiciona uma camada de segurança no sentido de proteger o negócio. Esta medida permite que a organização se mantenha em linha com os seus objetivos. | |

**Figura 66: Modelo de Maturidade de Implementação da Indústria 4.0 – Ações Tec. Informação**
**Fonte: Criação do Autor**

O resultado do caso de uso resultou na conclusão de que existe uma estratégia clara com foco na Indústria 4.0, sendo apenas necessário tomar algumas ações no sentido de convergir as tecnologias de operação, por forma a ficar em conformidade com o alinhamento da organização, conforme se conclui na Figura 67 .

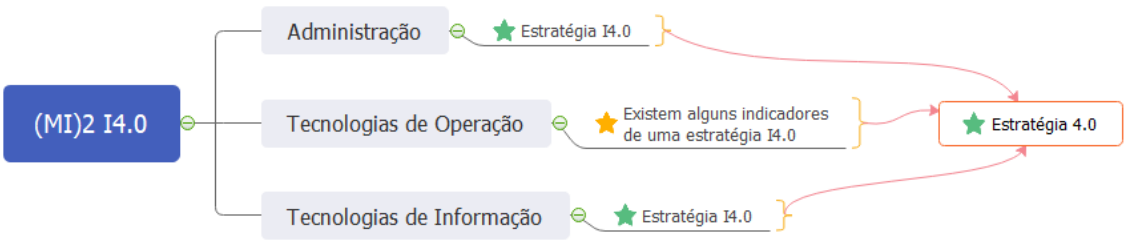



**Figura 67: Resultado caso de uso *Smart Buildings* com modelo (MI)2 I4.0**
**Fonte: Criação do Autor**

Das duas análises realizadas, foi possível verificar que no primeiro cenário a aplicação do modelo, identifica a necessidade de uma reformulação mais profunda, ao nível das tecnologias de operação e a necessidade e alguns ajustes ao nível da administração e das tecnologias de informação. O segundo cenário apresentado, apresenta-se num estado mais avançado, onde da análise realizada levava a que fossem considerados apenas alguns ajustes ao nível das tecnologias de operação.

Estas análises vêm assim corroborar a aplicabilidade do modelo, agilizando o processo das organizações na sua jornada em torno da Indústria 4.0, com a transformação digital contribuindo assim para a sociedade e as organizações em três vetores.

1. **Simplicidade** – Facilidade de recolha da informação pertinente das três unidades, para ser tratada pelo modelo;
2. **Agilidade** – Obtenção de "*feedback"* do modelo no que concerne às ações a tomar, no imediato;
3. **Valor** – Aumento da eficiência e eficácia da organização, resultante das ações implementadas que se traduzem nas melhorias no interior da organização, garantindo um maior retorno de investimento como resultado dessas ações, com impacto em todo o negócio como por exemplo ao nível de:
    - Vendas e Operações;
    - Melhoria do ciclo de vida do cliente;
    - Produção otimizada ao cliente;
    - Suporte ao cliente;

## 6.4. Síntese

Este capítulo, consolida a análise realizada ao longo deste trabalho, com a criação de um modelo que permitirá às organizações, a sua avaliação, aquando da definição das suas estratégias, ao nível de implementação da indústria 4.0.

Este modelo, tem em consideração o bem comum que é a organização e, tem no seu ADN o princípio subjacente de implementar uma estratégia focada na Indústria 4.0 e em simultâneo salvaguarda a componente ao nível de segurança, que vai ser garantida em consonância, pelas tecnologias de informação e as tecnologias e de operação, que garantem conformidade com os objetivos da organização.

O esquema resultante da análise, espelha o modelo a implementar sendo complementado pela matriz de avaliação, que permite posicionar a organização ao nível de implementação da estratégia.

O simulador permite às organizações avaliarem o seu grau de maturidade ao nível da Indústria 4.0, com resultados e ações em termos de conclusão da avaliação realizada. O simulador apresenta também o resultado da organização com base nas questões respondidas, bem como orienta a mesma com as ações, resultantes da avaliação.

É possível salientar outra das grandes valias a salientar do modelo, tem a ver com o facto de este poder ser endereçado e preenchido de forma célere (menos de trinta minutos) pela administração em colaboração com as tecnologias de operação e as tecnologias de informação, sem necessidade de ter que solicitar auditorias às consultoras para fazer essa primeira avaliação.

Após o preenchimento do modelo, o mesmo “emite”, pareceres/ações a executar pela organização em função dos resultados obtidos, ajudando as organizações, a poderem realinhar as suas estratégias com o foco na Indústria 4.0, potenciando assim a sua competitividade no mercado, bem como o aumento da eficiência e eficácia da mesma, na Indústria 4.0.

O modelo foi aplicado em dois casos de uso reais, que permitiu corroborar a aderência do mesmo, em termos de aplicação ao nível organizacional.

# 7. Conclusão

Aquando da criação dos Sistemas de Controlo Industriais modernos, há mais de 30 anos, o conceito de Cibersegurança, não existia, nem sequer estava preconizado em termos de linha temporal, no horizonte da segurança.

Com o advento do IoT e do IIoT, associado ao subsequente aumento dos Sistemas de Controlo Industrial, potenciado em simultâneo pela multiplicidade de interligação de redes como Ethernet, usadas nas TI's, ou Fieldbus usado nas Tecnologias da Operação, tem levado a que os Sistemas de Controlo Industrial, se encontrem, cada vez mais correlacionados com os dispositivos das tecnologias de informação e os processo de negócio, aumentando o risco de compromisso das funções de comando e controlo.

As organizações procuram ficar mais competitivas e com base nisso, procuram soluções que mapeiem com os requisitos do futuro da produção, incluindo redução de custos e redução de tempo para se adaptarem à procura do mercado, interoperabilidade através de elementos de software e hardware heterogéneos, integração e interoperabilidade através da organização na cadeia de produção, escalabilidade perfeita e económica, com a adição de recursos sem interromper as operações, reutilização de dispositivos e recursos de produção, conetividade automática, bem como melhores previsões e preditividade dos processo e interações, no sentido de responder à procura em tempo real.

Estas organizações, investem na tecnologia e nas soluções assentes na Internet das Coisas associado a uma estratégia, com foco na Indústria 4.0 que permita a obtenção das mais valias associadas a esta revolução. Para obtenção destas mais valias, é necessário interligar equipamentos que no passado, não se encontram conectados, estabelecendo novas oportunidades resultantes dessas interligações, como, computação assente em sensores (ligação entre o "mundo analógico" e a digitalização e/ou transformação digital), analítica industrial (conversão de dados em bruto em informação pertinente e relevante) e aplicações inteligentes a máquinas (processos de controlo inteligente e decisões proativas inteligentes), uso de soluções assentes em cima de inteligência artificial ou *machine learning*.

Esta convergência entre as TI's e as TO's, tem levantado diversas questões aos administradores das organizações, primeiro porque tem objetivos diferentes, pelo que dificulta a definição sobre quem recai a responsabilidade da Cibersegurança dos sistemas de SCI's, se esta deve de ser da responsabilidade dos Centros de Operação de Segurança (SOC's) das TI's, ou se recai sobre a responsabilidade da equipa das tecnologias de operação, que tem a responsabilidade do chão de fábrica.

Como o objetivo da dissertação passou pela conceção de um modelo, onde para além de dar informação importante para a estratégia da organização, que também reforçasse a sua componente de segurança criando sinergias entre as TI's e as TO's. Ao longo do trabalho, foram avaliadas diferentes *frameworks*, modelos de maturidade, tecnologias de comunicação, protocolos, vulnerabilidades que permitiram, convergir num modelo que

pudesse ser aplicado, na componente industrial, independentemente do setor em si (exemplo: automóvel, naval, alimentar, farmacêutica, energético, etc.).

O modelo desenvolvido, responde ao facto crescente de que os equipamentos SCI's mais antigos, serem cada vez mais interligados por Ethernet, originado pelo aumento da Indústria 4.0 e/ou da *Industrial Internet of Things*, onde não existe um controlo efetivo da segurança na transmissão dos dados.

O objetivo alcançado define de forma clara que o uso do modelo e a adoção das ações emitidas pelo mesmo, podem ajudar as organizações a tornarem-se mais competitivas e seguras no "palco" da Indústria 4.0.

É um facto que a Indústria 4.0, se encontra a dar os primeiros passos, pelo que a conjugação da Internet das Coisas com a Indústria 4.0, vem evidenciar que as vulnerabilidades associadas ao IoT, são bastante graves, uma vez que uma falha de segurança neste setor, pode colocar em causa vidas humanas e, por outro lado pode ter o "efeito" de causar elevados danos financeiros nas organizações, por paragem de linhas de produção ou danos de reputação, causados por ataques às organizações, levando a repercussões a nível mundial, pela dimensão das mesmas.

Esta dissertação, permitiu a criação de um modelo que permite ser adotado pelas organizações, no sentido aumentarem a sua competitividade pela a adoção das ações emanadas pelo modelo e de se acautelarem em termos futuros, por forma poderem percecionar o seu estado atual e nesse sentido, poderem tomar medidas ou corrigir estratégias, no sentido de minimizar o risco.

## 7.1. Trabalho Futuro

Como desenvolvimentos futuros, objetiva-se a inserção de estas conclusões em frameworks que possam vir a surgir, e/ou equipamentos que não tenham sido abordadas e que tenham surgido no mercado.

Teria interesse ao nível da cibersegurança, o desenvolvimento de plataformas assentes em cima de *blockchain*, no sentido de validar em termos de segurança, toda a cadeia de fornecedores do chão de fábrica.

Seria também relevante para desenvolvimentos de trabalhos futuros, a criação de soluções em cima de Inteligência Artificial e de *Machine Learning*, que possam permitir vir a consolidar a informação no *edge* destas redes, potenciando a realização de operações com elevadas quantidades de informação, levando à decisão no imediato sem necessidade de transmissão de todos os dados recolhidos para um core, onde seriam processados, analisados no sentido de obter uma decisão.

# Bibliografia ou Referências Bibliográficas


[1] ITU, “International Telecommunication Union,” 2020. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. [Accessed: 10-Nov-2019].

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[4] Microsoft, “Microsoft Iot Signals,” 2019. [Online]. Available: https://news.microsoft.com/2019/07/30/microsoft-announces-iot-signals-research-report-on-state-of-iot-adoption/. [Accessed: 18-Jan-2020].

[5] IDC, “The Growth in Connected IoT Devices,” *The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast*, 2019. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prCZ25694015. [Accessed: 12-Feb-2020].

[6] Research Gate, “Evolution of Data from Kilobyte-to Geopbyte.” .

[7] Cisco, “Index @ Www.Cisco.Com,” *2020*, 2020. [Online]. Available: http://www.cisco.com/. [Accessed: 25-Jan-2020].

[8] Kevin Ashton, “Rfid journal,” *That “Internet of Things” Thing In the real world, things matter more than ideas.*, 2009. [Online]. Available: http://www.itrco.jp/libraries/RFIDjournal-That Internet of Things Thing.pdf. [Accessed: 12-Oct-2019].

[9] Cisco, “Global Fixed and Mobile Internet Traffic Forecasts,” *2019*, 2011. [Online]. Available: https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~complete-forecast. [Accessed: 12-Nov-2019].

[10] “Embedded,” *The Internet of Things Myth: the search for a connectivity standard*. [Online]. Available: https://www.embedded.com/the-internet-of-things-myth-the-search-for-a-connectivity-standard/. [Accessed: 06-May-2020].

[11] “Introducing 5G technology and networks (speed, use cases and rollout).” [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G. [Accessed: 06-Sep-2020].

[12] “LTE-M vs NB-IoT – a guide exploring the differences between LTE-M and NB-IoTwe.” [Online]. Available: https://www.telenorconnexion.com/iot-insights/lte-m-vs-nb-iot-guide-differences/. [Accessed: 29-Sep-2020].

[13] Cisco, “Steven ’ s Famous Fourteen how not to Fail in WiFi.” [Online]. Available: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKEWN-

2439.pdf. [Accessed: 26-Sep-2020].

[14] "Wi-Fi Alliance Discover Wi-Fi Wi-Fi CERTIFIED 6." .

[15] "Wireless Connectivity Options for IoT Applications – Technology Comparison." [Online]. Available: https://www.bluetooth.com/blog/wireless-connectivity-options-for-iot-applications-technology-comparison/. [Accessed: 29-Sep-2020].

[16] "IoT Analytics," *Top 10 IoT applications in 2020*, 2020. [Online]. Available: https://iot-analytics.com/top-10-iot-applications-in-2020/. [Accessed: 12-Jun-2020].

[17] "Industrial Internet Consortium." [Online]. Available: https://blog.iiconsortium.org/2019/09/what-is-iiot-the-industrial-internet-of-things-primer.html. [Accessed: 12-Apr-2020].

[18] L. Bartevyan, "DLG expert report Industry 4.0," *Dlg*, 2015.

[19] H. Kagermann, W. Wahlster, and J. Helbig, "Securing the future of German manufacturing industry: Recommendations for implementing the strategic initiative INDUSTRIE 4.0," *Final Rep. Ind. 4.0 Work. Gr.*, no. April, pp. 1–84, 2013.

[20] "rfc791 Internet Protocol." [Online]. Available: https://www.rfc-editor.org/rfc/rfc791.html#ref-1. [Accessed: 28-Aug-2020].

[21] "The Internet Protocol Stack." [Online]. Available: https://www.w3.org/People/Frystyk/thesis/TcpIp.html. [Accessed: 26-Aug-2020].

[22] "BACnet." [Online]. Available: http://www.bacnet.org/Bibliography/EC-9-97/EC-9-97.html. [Accessed: 25-Aug-2020].

[23] Echelon Corporation, "Introduction to the LonWorks Platform." [Online]. Available: https://www.echelon.com/assets/blt893a8b319e8ec8c7/078-0183-01B_Intro_to_LonWorks_Rev_2.pdf. [Accessed: 25-Aug-2020].

[24] "The Legacy of KNX." [Online]. Available: https://www.knx.org/knx-en/for-professionals/What-is-KNX/KNX-History/. [Accessed: 25-Aug-2020].

[25] "IEEE 1901-2020." [Online]. Available: https://www.techstreet.com/standards/ieee-1901-2010?vendor_id=4953&product_id=1777803. [Accessed: 27-Aug-2020].

[26] "M-Bus." [Online]. Available: https://m-bus.com/. [Accessed: 26-Aug-2020].

[27] "Optigo." [Online]. Available: https://optigo.net/blog/what-are-bacnet-ethernet-ip-and-mstp. [Accessed: 26-Aug-2020].

[28] "Z-Wave." [Online]. Available: https://www.z-wave.com/. [Accessed: 27-Aug-2020].

[29] Echelon Corporation, "LonTalk Protocol Specification," pp. 1–112, 1996.

[30] "Modbus." [Online]. Available: https://www.modbus.org/faq.php. [Accessed: 28-

Aug-2020].

[31] Scheneider Electric, “Industrial Control Systems,” 2020. [Online]. Available: http://www.h-online.com/security/news/item/Backdoors-in-industrial-control-systems-1395141.html%3Fview=zoom;zoom=1. [Accessed: 06-Feb-2020].

[32] “Plattform-I40,” *Was ist Industrie 4.0*, 2020. [Online]. Available: http://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html;jsessionid=F1FB81BC6F692A562EFEBBD9E23B3283. [Accessed: 25-Mar-2020].

[33] C. Leyh, T. Schäffer, K. Bley, and L. Bay, “The Application of the Maturity Model SIMMI 4 . 0 in Selected Enterprises Full Paper Chair of Information Systems Chair of Information Systems,” *Twenty-third Am. Conf. Inf. Syst.*, no. August, pp. 1–10, 2017.

[34] S. Economic Development Board, “SIRI Manufacturing Transformation Insights Report 2019,” 2019.

[35] C. Leyh and T. Schäffer, “Klassifikation der unternehmensweiten Anwendungssystemlandschaft mit Fokus Industrie 4 . 0,” *Proc. zur Multikonferenz Wirtschaftsinformatik*, pp. 1651–1662, 2016.

[36] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The industrial internet of things (IIoT): An analysis framework,” Elsevier, 2018.

[37] T. L. P. White and T. L. P. White, “Trustworthy Software Essentials,” no. February, pp. 1–19, 2016.

[38] “International Society of Automation.” [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99. [Accessed: 25-May-2020].

[39] Cisco, “Purdue Model.” [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG/ch2_EttF.html.

[40] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2,” *NIST Spec. Publ. 800-82 rev 2*, pp. 1–157, 2015.

[41] NIST, “National Institute of Standards and Technology.” [Online]. Available: http://www.nist.gov/pml/data/xcom/index.cfm. [Accessed: 12-May-2020].

[42] ETSI, “European Telecommunications Standards Institute.” [Online]. Available: https://www.etsi.org/. [Accessed: 18-Apr-2020].

[43] IETF, “Internet Engineering Task Force.” [Online]. Available: https://www.ietf.org/about/. [Accessed: 12-Mar-2020].

[44] ISO, “International Organization for Standardization.” [Online]. Available: https://www.iso.org/about-us.html. [Accessed: 22-Apr-2020].

[45] TNO innovation for life, *THE IoT SECURITY LANDSCAPE*. 2019.

[46] "ENISA - European Union Agency for Cybersecurity," 2020. [Online]. Available: https://www.enisa.europa.eu/. [Accessed: 14-Mar-2020].

[47] W. Paper *et al.*, *Security and Resilience of Smart Home Environments Good practices and recommendations*, vol. 153, no. November. 2016.

[48] European Union Agency for Cybersecurity (ENISA), *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, no. November. 2017.

[49] European Union Agency for Network and Information Security (ENISA), *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, no. November. 2018.

[50] ENISA European Union Agency For Network and Information Security, *Towards secure convergence of Cloud and IoT*, no. September. 2018.

[51] ENISA, *IoT Security Standards Gap Analysis Mapping of existing standards against requirements on security and privacy in the area of IoT*, no. December. 2018.

[52] E. Lists, H. R. To, F. Wider, and T. O. F. Relevant, *Industry 4 . 0 Cybersecurity : Challenges & Recommendations*. 2019.

[53] MQTT, "MQTT." [Online]. Available: http://mqtt.org/. [Accessed: 18-Feb-2020].

[54] IETF, "Draft Ietf Core CoAP." [Online]. Available: https://tools.ietf.org/html/draft-ietf-core-coap-18. [Accessed: 17-Feb-2020].

[55] "XMPP." [Online]. Available: https://xmpp.org/. [Accessed: 25-Feb-2020].

[56] "AMQP." [Online]. Available: https://www.amqp.org/. [Accessed: 26-Feb-2020].

[57] W. Schulte, A. Velosa, and B. Lheureux, "Hype Cycle for the Internet of Things, 2019," *Gartner*, no. July 2019, pp. 1–32, 2019.

[58] J. Graham, "You will get chipped — eventually," 2017. [Online]. Available: https://eu.usatoday.com/story/tech/2017/08/09/you-get-chipped-eventually/547336001/. [Accessed: 17-Nov-2019].

[59] "Thousands Of Swedes Are Inserting Microchips Under Their Skin." .

[60] A. Velosa, D. Kutnick, B. Lheureux, and R. Williams, "Hype Cycle for the Internet of Things, 2020," *Gartner*, no. July 2020, pp. 1–62, 2020.

[61] G. Alasdair, *Industry 4.0 - The Industrial Internet of Things*, vol. 132. 2017.

[62] "Missão, Visão e Valores." [Online]. Available: https://www.ipleiria.pt/estg-dge/enquadramento/. [Accessed: 22-Aug-2020].

[63] "Tesla, Inc.'s Mission Statement & Vision Statement (An Analysis)." [Online]. Available: http://panmore.com/tesla-motors-inc-vision-statement-mission-statement-analysis. [Accessed: 23-Aug-2020].

# ANEXO A

Iniciativas Chave ao Nível de Segurança IoT

**Alliance for IoT Innovation (AIOTI)**

A Alliance for IoT Innovation (AIOTI) é um organismo que inclui os principais atores industriais da IoT - grandes empresas, PME bem-sucedidas e startups dinâmicas, bem como centros de pesquisa, universidades, associações e órgãos públicos europeus conhecidos. Em outubro de 2015, a Aliança publicou 12 relatórios sobre questões de política e normas da IoT. A AIOTI também forneceu recomendações detalhadas para futuras colaborações na Área de Foco da Internet das Coisas do programa Horizonte 2020-2017.

**URL:** https://aioti.eu

**Região/País:** Europa

**Membros:** Indústria e alguns institutos académicos

**Desafios Endereçados:** Cibersegurança e privacidade por defeito, padrões de Segurança IoT, Legislação à prova de "futuro"

**Cloud Security Alliance – IoT Working Group**

A cloud desempenha um papel importante na implementação bem-sucedida do IoT. Os serviços na cloud incluem recolha, tratamento e armazenamento de dados, análise de dados, gestão de inventário, gestão de sensores, serviços de visualização e monitorização, além de relacionamento com dispositivos gestão. O Grupo de Trabalho de IoT da Cloud Security Alliance concentra-se sobre como entender os casos de uso relevantes para implementações de IoT e definir orientações operacionais para profissionais de segurança por forma a protegerem as suas implementações.

**URL**: https://cloudsecurityalliance.org/group/internet-of-things/#_overview

**Região/País:** Global/Focado nos Estados Unidos

**Membros**: Indústria

**Desafios endereçados:** Sistemas Operativos Seguros, plataformas e cloud

**ENISA IoT e ENISA IoTSEC (SEG – Security Experts Group)**

A ENISA define Internet das Coisas como um conceito emergente que descreve um amplo ecossistema, onde dispositivos e os serviços interligados recolhem, trocam e processam dados para se adaptarem dinamicamente a um contexto. Com grande impacto na segurança, saúde e privacidade dos cidadãos, o cenário de ameaças referente à Internet das Coisas é extremamente amplo. Portanto, é importante entender o que precisa ser protegido e desenvolver medidas de segurança específicas para proteger a Internet das Coisas contra-ameaças cibernéticas. O grupo IoTSEC da ENISA é uma plataforma de

troca de informações e que reúne especialistas para garantir a segurança e a resiliência de todo o ecossistema da Internet das Coisas.

**URL:** https://resilience.enisa.europa.eu/iot-security-experts-group-1

**Região/País:** Europa

**Membros:** Governos e órgãos governamentais

**Desafios Endereçados:** Cibersegurança e privacidade por defeito, padrões de Segurança IoT, Legislação à prova de "futuro"

**ETSI – European Telecommunications Standards Institute**

O ETSI é uma Organização Europeia de Padrões (ESO – European Standards Organization) e um organismo reconhecido de padrões locais/regionais que lida com telecomunicações, radiodifusão e outras redes e serviços de comunicações eletrónicas. O ETSI tem um papel especial na Europa, apoiando regulamentos e legislação europeia através da criação de Normas Europeias harmonizadas. Somente os padrões desenvolvidos pelas três ESOs (CEN, CENELEC e ETSI) são reconhecidos como Normas Europeias (ENs). Embora o ETSI tenha sido fundado inicialmente para atender às necessidades da Europa, seus padrões agora são usados em todo o mundo.

**URL**: https://www.etsi.org/

**Região/País:** Europa

**Membros**: Indústria, governos e academias

**Desafios Endereçados:** Cibersegurança e privacidade por defeito, padrões de Segurança IoT

**GLOBALPLATFORM**

A GlobalPlatform é uma associação do setor, sem fins lucrativos, dirigida por mais de 100 empresas membros. O padrão *Trusted Execution Environment* (TEE) da GlobalPlatform define uma área segura no processador de um dispositivo ligado que armazena, processa e protege dados confidenciais. O GlobalPlatform também relaciona a ideia de Root of Trust às tecnologias SE (*Secure Element*) e TEE (*Trusted Execution Environmen*t).

**URL:** https://globalplatform.org/

**Região/país:** Global

**Membros:** Indústria

**Desafios Endereçados:** Avaliação e certificação, identificação de dispositivos e *Root of Trust*

**Global Cyber Alliance**

A Global Cyber Alliance é um esforço internacional intersectorial dedicado à erradicação do risco cibernético e à melhoria do mundo conectado. Os membros fundadores incluem a polícia de Londres, o procurador do distrito de Nova York e, o Center for Internet Security.

**URL:** https://www.globalcyberalliance.org/

**Região/país:** Global

**Membros:** Indústria, governos

**Desafios Endereçados:** Monitorização e analítica, avaliação e certificação

**GSMA – Global System for Mobile Communications**

A GSMA representa os interesses das operadoras móveis em todo o mundo, unindo mais de 750 operadoras com mais de 350 empresas no ecossistema móvel mais amplo, incluindo fabricantes de aparelhos, dispositivos, empresas de software, fornecedores de equipamentos e empresas de internet, como bem como organizações em setores adjacentes da indústria.

**URL:** https://www.gsma.com/

**Região/país:** Global

**Membros:** Indústria

**Desafios Endereçados:** Padrões de segurança IoT, Comunicações e Infraestruturas

**IETF – Internet Engineering Task Force**

A missão da IETF é melhorar a Internet, produzindo documentos técnicos relevantes de alta qualidade que influenciam a maneira como as pessoas projetam, usam e gerem a Internet.

**URL:** https://www.ietf.org/

**Região/país:** Global

**Membros:** Indústria, Academias

**Desafios Endereçados:** Padrões de segurança IoT, Comunicações e Infraestruturas

**Industrial IoT Consortium**

O Industrial Internet Consortium visa transformar negócios e sociedade, acelerando a Internet das Coisas Industrial (IIoT). A missão do IIC é fornecer uma IIoT confiável, na qual os sistemas e dispositivos do mundo estejam conectados e controlados com segurança para fornecer resultados em termos operacionais.

**URL:** https://www.iiconsortium.org/

**Região/país:** Global

**Membros:** Indústria, baseado nos Estado Unidos

**Desafios Endereçados:** Segurança da cadeia de fornecimento, suporte ao ciclo de vida do produto, padrões de segurança da Internet das coisas, SO e aplicativos seguros, comunicações e infraestrutura seguras, monitorização e análise de segurança.

**IoT Acceleration Consortium**

A criação de modelos de negócios inovadores por meio da utilização do IoT e, a realização de uma sociedade segura e protegida para o público, são objetivos importantes para o Japão. Com o objetivo de discutir os esforços ou medidas necessárias para atingir esses objetivos, o Ministério da Economia, Comércio e Indústria (METI) e o Ministério de Assuntos Internos e Comunicações (MIC) estabeleceram um Grupo de Trabalho de Segurança do IoT, no âmbito da Aceleração da IoT.

**URL:** http://www.iotac.jp/en/

**Região/país:** Japão

**Membros:** Academias, indústria

**Desafios Endereçados:** Desenvolvimento de padrões de segurança IoT

**IoTC - IoT Consortium**

O Internet of Things Consortium (IoTC) é uma associação de desenvolvimento de negócios para o ecossistema da Internet das Coisas (IoT). É composto pelos principais fundadores, executivos e empresas globais da IoT. A missão da IoTC é estimular o crescimento do mercado de IoT, liderando os esforços do setor por meio de parcerias estratégicas. A organização concentra-se em cinco setores verticais principais: casas inteligentes, automóveis, cidades, retalho e *wearables*

**URL:** https://iofthings.org/

**Região/país:** Global

**Membros:** Indústria

**Desafios Endereçados:** Responsabilidade pelo ecosistema industrial

**IoTACA – IoT Cybersecurity Alliance**

A aliança IOTCA é onde os principais fornecedores de segurança de IoT do setor e, os principais especialistas em IoT se reúnem para aumentar a conscienlização, estabelecer e compartilhar melhores práticas por forma a pesquisar e desenvolver métodos para holisticamente proteger o ecossistema do IoT, para o bem de todos.

**URL:** https://www.iotca.org/

**Região/país:** Global

**Membros:** Membros da indústria incluindo, AT&T, IBM, Nokia, Palo Alto Networks, Qualcomm, Symantec e Trustonic

**Desafios Endereçados:** Padrões de segurança no IoT, Sistemas Operativos seguros, Aplicações e Cloud, comunicações e infraestruturas seguras, Monitorização e analítica segura

**IoT -EPI IoT European Platforms Initiative**

A Iniciativa IoT-European Platforms Initiative (IoT-EPI) foi formada para construir um ecossistema assente no vibrante e sustentável IoT na Europa, maximizando as oportunidades de desenvolvimento da plataforma, interoperabilidade e partilha de informações. Com um financiamento total de 50M € e uma rede de parceiros de 120 empresas e organizações estabelecidas, os projetos IoT-EPI desenvolvem tecnologias inovadoras de plataforma e promovem a adoção de tecnologia através da construção de comunidades e negócios.

**URL:** https://iot-epi.eu/

**Região/país:** Europa

**Membros:** Parceiros e organizações da rede com sete projetos de investigação e inovação, Inter-IoT, BIG IoT, AGILE, SymbIoTe, TagITSmart!, VICINITY e bIoTope.

**Desafios Endereçados**: Responsável do ecossistema da indústria

**IoTSF – IoT Security Foundation**

O IoTSF (Internet of Things Security Foundation) tem como objetivo tornar seguro a interligação das "coisas" para que os muitos benefícios da IoT possam ser alcançados. O IoTSF é uma resposta internacional colaborativa, sem fins lucrativos, aos desafios complexos colocados pela segurança na expansão da componente IoT a nível mundial.

**URL:** https://www.iotsecurityfoundation.org/

**Região/país:** Global

**Membros:** Indústria

**Desafios Endereçados:** Padrões de segurança da IoT, avaliação e certificação, segurança da cadeia de fornecimento, suporte ao ciclo de vida do produto, aplicativos e SO seguros, comunicações e infraestrutura seguras, monitorização e análise de segurança

**ITU STUDY GROUP 20**

A ITU SG20 desenvolve padrões internacionais por forma a permitir o desenvolvimento coordenado de tecnologias de IoT, incluindo comunicações máquina a máquina e redes de sensores globais. Uma parte central deste estudo é a padronização de arquiteturas transversais aplicadas ao IoT bem como mecanismos, para a interoperabilidade de aplicativos e, conjuntos de dados IoT, usados por vários setores da indústria, orientados verticalmente.

**URL:** https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx

**Região/país:** Global

**Membros:** Governos, academias, indústria

**Desafios Endereçados:** Comunicações e infraestruturas seguras, padrões de segurança IoT

**LORA ALLIANCE**

A LoRa Alliance é uma associação sem fins lucrativos, que cresceu para mais de 500 membros, desde a sua criação em março de 2015. Estes colaboram e partilham experiências, por forma a promover e impulsionar o sucesso do protocolo LoRaWAN, como um padrão global aberto, em termos de segurança, ao nível da conectividade do IoT LPWAN.

**URL:** https://lora-alliance.org/about-lora-alliance

**Região/país:** Global

**Membros:** Indústria

**Desafios Endereçados:** Padrões de segurança IoT

**NIST IoT – National Institute of Standards and Technology**

O programa Cibersegurança para Internet das Coisas (IoT) do NIST apoia o desenvolvimento e a aplicação de padrões, diretrizes e ferramentas relacionadas para melhorar a cibersegurança de dispositivos interligado e, os ambientes nos quais eles são implementados. Ao colaborar com as partes interessadas do governo, da indústria, de organismos internacionais e das academias, o programa visa cultivar a confiança e promover a liderança dos EUA no campo do IoT.

**URL:** https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

**Região/país:** Estados Unidos

**Membros:** Indústria

**Desafios Endereçados:** Padrões de segurança IoT

### OCF - Open Connectivity Foundation

A OCF tem uma missão dupla de:

Fornecimento de especificações, código e um programa de certificação para permitir que os fabricantes possam produzir os produtos certificados pela OCF para o mercado, que possam inter-operar com os dispositivos IoT atuais e sistemas mais antigos.

Melhorar a experiência do utilizador final, fazendo uma ponte direta com outros ecossistemas garantindo a interoperabilidade com dispositivos compatíveis com a OCF.

As especificações OCF aproveitam os padrões e tecnologias existentes do setor, fornecem mecanismos de conexão entre dispositivos e, entre esses dispositivos e a cloud por forma a gerirem o fluxo de informações entre dispositivos, independentemente de seus, sistemas operativos, fornecedores de serviços ou de comunicações.

**URL:** https://openconnectivity.org/

**Região/país:** Global, com foco nos Estados Unidos e Canadá.

**Membros:** Indústria

**Desafios Endereçados:** Comunicações e infraestruturas seguras, padrões de segurança IoT

### OWASP IOT PROJECT

O Projeto Internet das Coisas do Open Web Application Security Project (OWASP) foi desenvolvido para ajudar os fabricantes, programadores e consumidores a perceber melhor os problemas de segurança associados à Internet das Coisas e, permitir que os utilizadores em qualquer contexto melhorem as decisões de segurança ao criar, implementar ou avaliar tecnologias de IoT. O projeto procura definir uma estrutura para vários subprojectos de IoT, como áreas de superfície de ataque, guias de testes aplicados à segurança e as principais vulnerabilidades nesta área.

**URL:** https://owasp.org/www-project-internet-of-things/

**Região/país:** Global

**Membros:** Indústria, voluntários

**Desafios Endereçados:** Comunicações e infraestrutura seguras, Sistemas operativos e aplicações seguras, padrões de segurança no IoT.

### PRPL FOUNDATION

A missão da Fundação prpl é: (a) desenvolver, apoiar e promover um consórcio de código aberto, orientado para a comunidade, com foco em permitir a segurança e, a interoperabilidade de dispositivos, incorporados na Internet das Coisas (IoT) alavancando a sociedade inteligente de o futuro; e B)realizar outras atividades, conforme apropriado, para promover os propósitos e alcançar as metas estabelecidas acima.

**URL:** https://prplfoundation.org/

**Região/país:** Global

**Membros:** Indústria, academias

**Desafios Endereçados:** Identificação de dispositivos e *root of trust*

### T2T (Thing-to-Thing) Research Group

O Grupo de Pesquisa *Thing-to-Thing* (T2TRG) pretende investigar, questões de pesquisa aberta, por forma a transformar a IoT em realidade, como uma Internet na qual "os nós" com poucos recursos, podem comunicar entre si e, com a Internet para participar em inovações sem permissão.

O foco do T2TRG está nas oportunidades de padronização no IETF, ou seja, começando na camada de adaptação que ligam os dispositivos ao IP e terminando na camada aplicacional com arquiteturas e APIs para comunicar e disponibilizar funções de dados e gestão (incluindo funções de segurança).

**URL:** https://datatracker.ietf.org/rg/t2trg/documents/

**Região/país:** Global

**Membros:** Membros da indústria

**Desafios Endereçados:** Comunicações e infraestruturas seguras, Sistemas Operativos seguros, padrões de segurança IoT

### Trusted Computing Group

O TCG (Trusted Computing Group) é uma organização sem fins lucrativos formada para desenvolver, definir e promover padrões globais abertos da indústria, neutros a fornecedores, incluindo uma *Root of Trust* baseada em hardware, para plataformas de computação confiáveis interoperáveis

**URL:** https://trustedcomputinggroup.org/

**Região/país:** Global

**Membros:** Membros da indústria

**Desafios Endereçados:** identificação de dispositivos, *root of trust*, aplicações e sistemas operativos seguros, padrões de segurança IoT.

**UEFI (Ùnified Extensible Firmware Interface) FORUM**

O UEFI Forum promove a inovação de firmware, por meio da colaboração do setor industrial e, da defesa de uma interface padronizada que simplifica e protege a inicialização da plataforma e as operações de inicialização do firmware. Estas especificações reconhecidas globalmente, trazem novas funcionalidades, bem como a segurança melhorada à evolução de dispositivos, firmware e sistemas operativos, além de facilitar a interoperabilidade entre plataformas e sistemas compatíveis, com as tecnologias de próxima geração. O Fórum UEFI defende uma interface padronizada por forma a simplificar e proteger a inicialização da plataforma, assim como a inicialização do firmware. A especificação UEFI inclui segurança melhorada durante a inicialização do sistema ("UEFI Secure Boot") através de uma cadeia criptográfica de confiança

**URL:** https://www.uefi.org/about

**Região/país:** Global, focado nos Estados Unidos

**Membros:** Indústria

**Desafios Endereçados:** Identificação de dispositivos, *root of trust*, Sistemas operativos seguros, aplicações e cloud

**WI-SUN ALLIANCE**

A Wi-SUN Alliance é uma associação da indústria dedicada à conectividade “perfeita”. O Wi-SUN procura promover padrões certificados que coordenam vários sistemas sem fio e, padronizam níveis de energia, taxas de dados, modulações e faixas de frequência, entre outras variáveis.

**URL:** https://www.wi-sun.org/

**Região/país:** Primeiramente a Ásia (Japão) mas numa forma global a indústria no seu todo

**Membros:** Indústria incluindo a Cisco e a Toshiba

**Desafios Endereçados:** Comunicações e Infraestrutura seguras

**ZIGBEE ALLIANCE**

Fundada em 2002, a Zigbee Alliance é um grupo de empresas que mantém e publica o padrão Zigbee, um conjunto de protocolos de comunicação baseado no IEEE 802.15.4.

**URL:** https://zigbeealliance.org/

**Região/país:** Global

**Membros:** Indústria

**Desafios Endereçados:** Comunicações e infraestruturas seguras