Produto 2

Roadmap tecnológico

Versão 2.0

2017

BNDES O banco nacional do desenvolvimento

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

BRASIL GOVERNO FEDERAL

Esclarecimentos sobre o *roadmap* tecnológico

"O documento referente ao *roadmap* tecnológico registrou as iniciativas desenvolvidas em âmbito global no tema de Internet das Coisas, não levando em consideração questões específicas de qualquer país. Os dados descritos neste documento foram encontrados em diversas fontes públicas, entre o período de dezembro de 2016 a fevereiro de 2017, dentre elas a Consulta Pública intitulada *Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil*.

Foram também consideradas informações coletadas por meio de entrevistas com especialistas de diversos setores relevantes para a implantação da Internet das Coisas no Brasil, bem como aquelas obtidas durante uma oficina realizada em fevereiro de 2017, com a participação de dezenove Instituições Científicas e Tecnológicas (ICTs). Esse esforço de colaboração envolvendo vários atores constituiu, assim, o sólido alicerce sobre o qual repousam os resultados apresentados.

Cabe ressaltar que as tendências tecnológicas relacionadas a IoT descritas no presente documento não representam a opinião ou o juízo de valor do Ministério da Ciência, Tecnologia, Inovações e Comunicações, do Banco Nacional de Desenvolvimento Econômico e Social ou dos membros do Consórcio. "

Índice

LISTA DE ACRÔNIMOS

3GPP	3rd Generation Partnership Project
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
API	Application Program Interface
BI	Business Intelligence
BLE	Bluetooth Low Energy
BOM	Bill Of Materials
CI	Circuito Integrado
CMOS	Complementary Metal-Oxide-Semiconductor
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
DEX	HIP Diet Exchange
DTLS	Datagram Transport Layer Security
ERP	Enterprise Resource Planning
GSM	Global System for Mobile communication
IEEE	Institute of Electrical and Electronics Engineers
IKEv2	Internet Key Exchange version 2
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
LPWAN	Low-Power Wide-Area Network
LoRa	Long Range Radio
LoRaWAN	Long Range Wide Area Network
LTE	Long Term Evolution
M2M	Machine-to-Machine
MCU	MicroController Unit
MEMS	Micro-Electro-Mechanical Systems
MPU	MicroProcessor Unit
MPW	Multi-Project Wafer
MQTT	Message Queuing Telemetry Transport
MTC	Machine Type Communication
MVNO	Mobile Virtual Network Operator
NAN	Neighborhood Area Network
NB-IoT	NarrowBand IoT
NFV	Network Function Virtualization
PAN	Personal Area Network
SDN	Software Defined Network
SO	Sistema Operacional
SoC	System-on-a-Chip
TLS	Transport Layer Security
UIT	União Internacional das Telecomunicações
WLAN	Wireless Local Area Network

1. CONTEXTO

O presente documento "*Relatório de Roadmap Tecnológico*" é um dos produtos do estudo "Internet das Coisas: um plano de ação para o Brasil", liderado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES), em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). O estudo, que tem por objetivo propor um plano de ação estratégico para o País em Internet das Coisas (em inglês, *Internet of Things* - IoT), está dividido em quatro grandes fases:

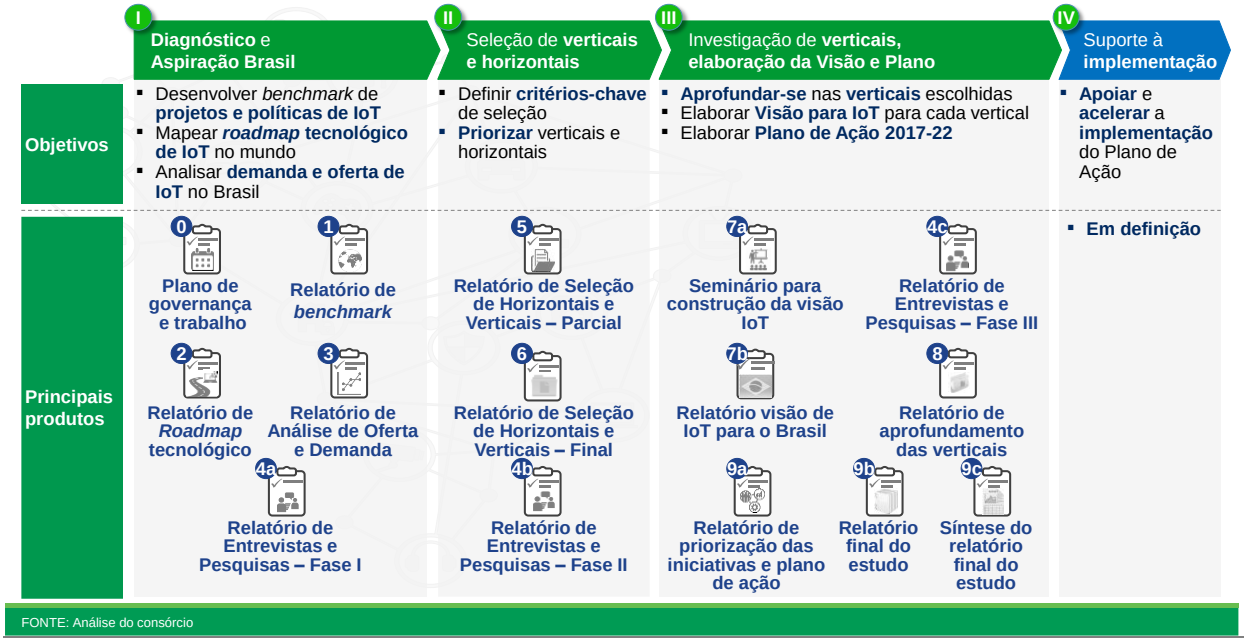
- **Diagnóstico Geral e aspiração para o Brasil:** Desenvolver *benchmark* de projetos e políticas de IoT, mapear o *roadmap* tecnológico de IoT no mundo e analisar a demanda e a oferta de IoT no Brasil;
- **Seleção de verticais e horizontais:** Definição de critérios-chave para seleção e priorização de verticais e horizontais;
- **Aprofundamento e elaboração de plano de ação (2017 - 2022):** Aprofundamento nas verticais escolhidas, elaboração de visão para IoT para cada vertical e elaboração de Plano de Ação 2017-22;
- **Suporte à implementação:** Apoio à execução do Plano de Ação 2017-22**.**

As 3 primeiras fases são compostas de 9 produtos principais, como descrito no QUADRO 1 a seguir. O presente documento representa o Produto 2 e está inserido na Fase 1 do estudo. Os principais objetivos do documento são:

- Descrever as tendências tecnológicas que podem potencializar o florescimento de IoT;
- Identificar os atores que estão na fronteira do conhecimento sobre o tema.

QUADRO 1

Fases e principais produtos do estudo "Internet das Coisas: um plano de ação para o Brasil"



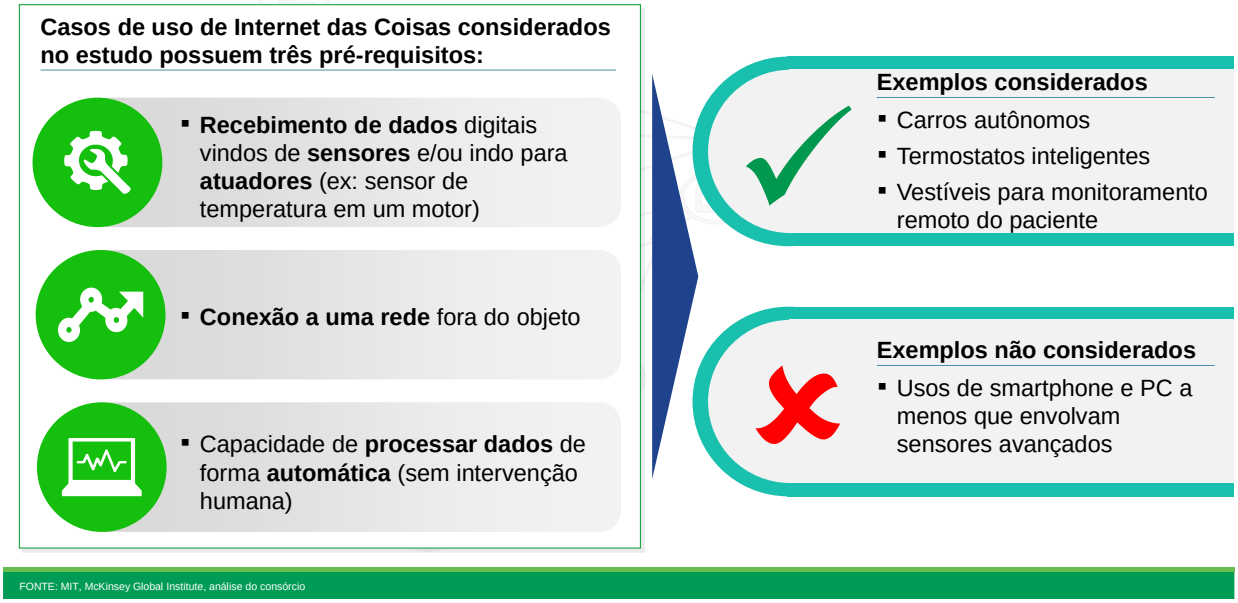
FONTE: Análise do consórcio

2. ALINHAMENTO CONCEITUAL

De acordo com a União Internacional das Telecomunicações (UIT)[1], Internet das Coisas é uma **infraestrutura global** para a sociedade da informação, que **habilita serviços avançados por meio da interconexão entre coisas** (físicas e virtuais), com base nas **tecnologias de informação e comunicação (TIC)**. Em sentido amplo, trata-se não apenas de conectar coisas, mas também de dotá-las do poder de processar dados, tornando-as "inteligentes". Neste sentido, a Internet das Coisas vem ganhando momento não devido ao surgimento de **tecnologias disruptivas**, mas sim por conta da **evolução de um conjunto de tecnologias já disponíveis**, que estão se tornando mais **acessíveis**, possibilitando sua **adoção em massa**. De forma geral, o estudo utilizou três requisitos básicos para que um caso de uso seja considerado IoT, como descrito no QUADRO 2 a seguir.

QUADRO 2

Pré-requisitos utilizados pelo estudo para que casos de uso sejam considerados IoT



FONTE: MIT, McKinsey Global Institute, análise do consórcio

Por exemplo, um trator passa não só a arar a terra, mas a coletar uma extraordinária quantidade de dados, que serão posteriormente analisados por uma aplicação hospedada em um *data center*, produzindo relatórios que permitem que um agricultor tome decisões sobre onde e quando plantar. Em uma linha de montagem, sensores fornecem dados que são analisados e alertam sobre o melhor momento para se realizar uma parada para manutenção. Dispositivos vestíveis (*wearables*) fornecem informações ao médico sobre

[1] União Internacional das Telecomunicações: agência das Nações Unidas para as tecnologias da informação e da comunicação (TIC).

indicadores relacionados à saúde de um paciente. Veículos autônomos conseguem se comunicar de modo a evitar acidentes.

A Internet das Coisas opera em espaços físicos denominados "Ambientes de aplicação", tais como residências, cidades e fábricas. A lente de Ambientes é relevante, uma vez que o impacto dos casos de uso normalmente transcende setores específicos. Outra razão para se utilizar a lente de Ambientes reside no fato de que a interoperabilidade e a interação entre diversos atores, pontos cruciais para o desenvolvimento de IoT, normalmente ocorre dentro de um mesmo Ambiente. O QUADRO 3 exemplifica os principais ambientes de aplicação de IoT.

QUADRO 3

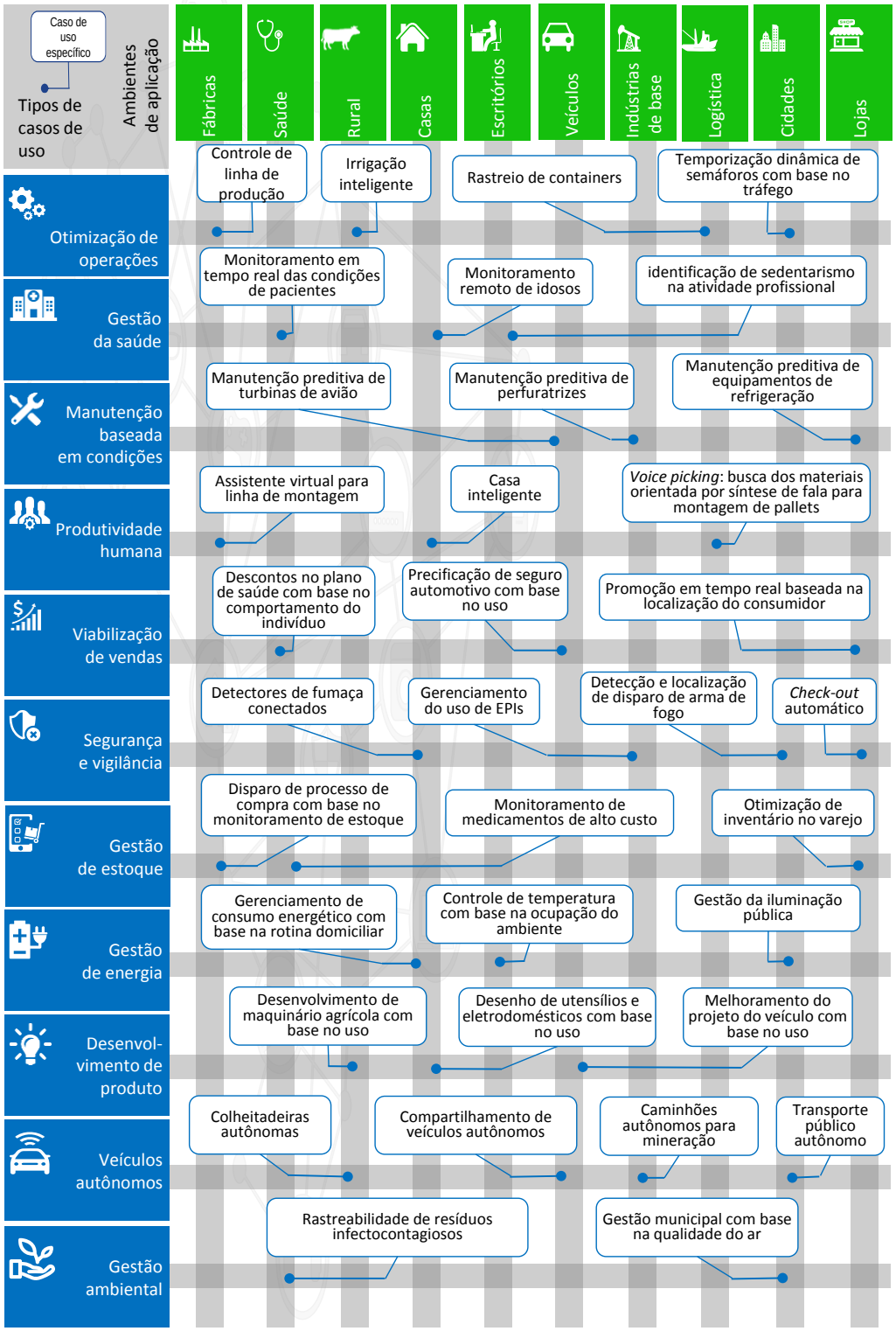
A Internet das Coisas é a rede de todos os objetos que se comunicam e se regulam de forma autônoma via internet

FONTE: Análise do consórcio

A Internet das Coisas já é uma realidade e tem gerado oportunidades tangíveis de geração de valor em diversos ambientes de aplicação de IoT. O QUADRO 4 descreve, de forma não exaustiva, exemplos de casos de uso de IoT aplicáveis aos principais ambientes, com base no relatório *Unlocking the potential of the Internet of Things*, elaborado pelo McKinsey Global Institute.

QUADRO 4

Exemplos de casos de uso nos principais ambientes de aplicação de IoT



O presente documento analisou as tendências nas camadas tecnológicas de IoT, bem como o posicionamento dos atores na cadeia de valor de IoT. As definições de "camadas tecnológicas" e "cadeia de valor" serão apresentadas a seguir.

2.1 Camadas tecnológicas

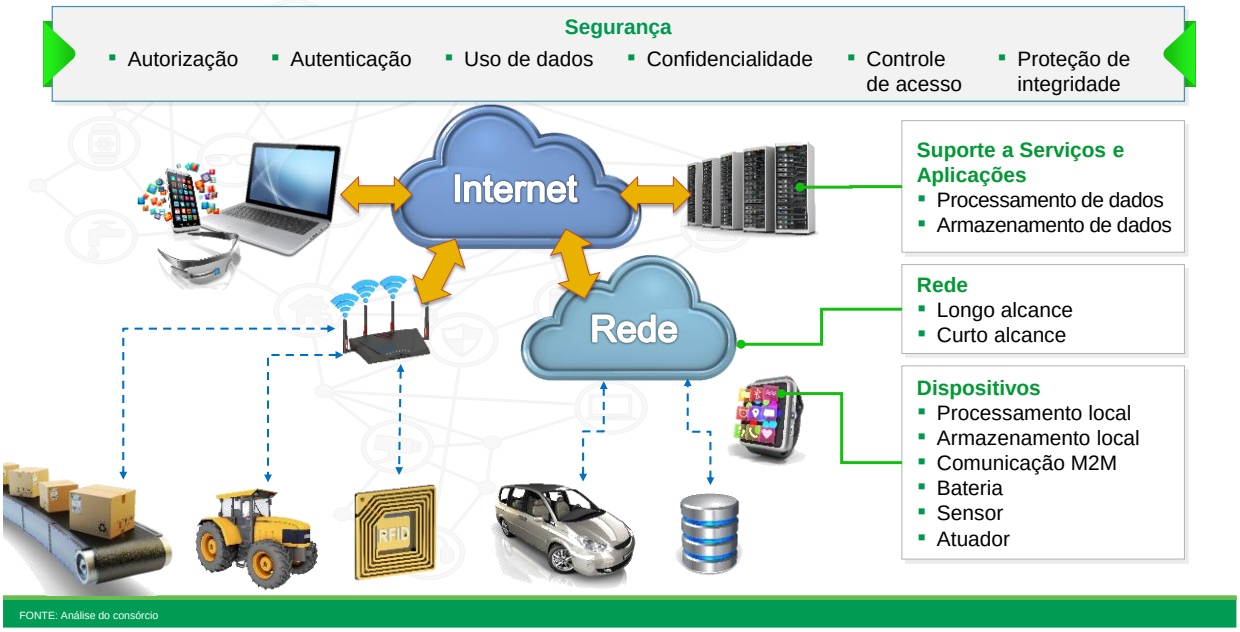
A diversidade de aplicações da IoT requer o desenvolvimento de inúmeras tecnologias, abrangendo desde o componente semicondutor, que permite a um sensor medir uma determinada grandeza física, passando por um *chip*, que transmite esse dado via radiofrequência, até um servidor que trata a informação, transformando-a em conhecimento e agregando-lhe valor. Nesse contexto, a IoT é impulsionada por tecnologias capacitadoras, cuja arquitetura é organizada em camadas, formando uma rede globalmente acessível de coisas, provedores e consumidores. No presente documento, foi utilizada a arquitetura de IoT definida pela União Internacional das Telecomunicações (UIT), baseada em 4 camadas tecnológicas:

- **Dispositivos:** Engloba os levantamentos referentes à evolução dos chips, sensores, atuadores e estruturas de armazenamento e captação de energia**;**
- **Rede:** Fornece funções de conectividade e controle do acesso e mobilidade para serviços de IoT;
- **Suporte a Serviços e Aplicações:** Provêm capacidades de suporte, como processamento ou armazenamento de dados, que podem ser utilizadas por diferentes aplicações de IoT, além de capacidades de suporte de escopo mais específico;
- **Segurança da Informação:** Apresenta tecnologias utilizadas para garantir a privacidade e a confiabilidade no envio de dados, que permearão todas as demais camadas;

As quatro camadas tecnológicas, assim como exemplos de soluções em cada camada, estão ilustradas no QUADRO 5 a seguir.

QUADRO 5

Principais camadas tecnológicas definidas pela União Internacional das Telecomunicações (UIT)



FONTE: Análise do consórcio

2.2 Cadeia de valor

A cadeia de valor de IoT é definida como o conjunto de oportunidades de geração de valor (por exemplo, novos negócios, conteúdo e serviços) desenvolvidas pelos atores do ecossistema de IoT. A cadeia de valor de IoT é formada por elos, que representam grupos de atividades desempenhadas para a entrega de valor aos clientes e usuários. Foram identificados seis elos da cadeia de valor de IoT (módulos inteligentes, objetos inteligentes, conectividade, habilitador, integrador e provedor de serviço), com base em análises da literatura especializada, validadas por especialistas. As descrições, principais atividades e exemplos de atores em cada elo da cadeia estão detalhados na tabela abaixo.

	Módulos Inteligentes	Objetos Inteligentes	Conectividade	Habilitador	Integrador	Provedor de Serviço
Descrição	Compreendem os elementos constitutivos dos objetos inteligentes, contemplando desde componentes básicos, tais como processadores, sensores, atuadores, memórias, *modems* e baterias, até dispositivos mais complexos. Em algumas situações, podem atuar como *gateways* de dispositivos com limitada capacidade de processamento e comunicação.	Consiste nos elementos tangíveis com os quais interagimos no universo da IoT.	Contempla fornecedores de equipamentos e provedores de serviços, que garantem a comunicação entre os elementos que compõem as soluções de IoT.	Oferece os sistemas de suporte para coleta, armazenamento, transformação, análise, visualização dos dados e gerenciamento dos objetos inteligentes	Combina diferentes sistemas, processos e objetos para atuarem conforme as regras de negócios do cliente. Na maioria dos casos, a integração é realizada através de interfaces padronizadas de programação de aplicativo (APIs)[2].	Presta serviços com base em solução fim-a-fim composta por hardware, software e conectividade[3].

[2] API: Application program interface; conjunto de rotinas, protocolos e ferramentas para a construção de aplicativos de software. Especifica como os componentes de software devem interagir, e são usadas ao programar componentes de interface gráfica do usuário.

[3] Soluções fim-a-fim: soluções desempenhadas em todos os elos da cadeia de valor de IoT.

	Módulos Inteligentes	Objetos Inteligentes	Conectividade	Habilitador	Integrador	Provedor de Serviço
Principais atividades	Fabricação de processadores, micro controladores, sensores, atuadores, memórias, *modems*, baterias e funcionalidades de segurança e de gerenciamento de *endpoints*.	Sensoriamento, comunicação, atuação, cognição, gestão remota, processamento e armazenamento de energia.	Fornecimento de equipamentos de infraestrutura e serviços de comunicação de dados.	Desenvolvimento e disponibilização de soluções (produtos e serviços) de armazenagem, tratamento de dados (BI[4], *Analytics*, etc.), virtualização e gerenciamento de dispositivos, e também fornecimento de infraestrutura para tais soluções.	Combinação de diferentes sistemas, processos e objetos, inclusive com vistas a atuarem conforme regras de negócios (privados ou públicos). As atividades são voltadas tanto para a integração entre aplicações e os processos de negócio, como entre a aplicação e os módulos inteligentes.	Empacotamento de serviços de IoT que atendam a necessidades de consumidores ou empresas. Criação de um relacionamento direto com os clientes, abrangendo suporte, precificação, faturamento e o provimento de uma solução fim-a-fim.

[4] BI: Business Intelligence: soluções e tecnologias que permitem que uma empresa ou organização aprenda sobre suas operações através de aplicações de relatórios e ferramentas de análise

	Módulos Inteligentes	Objetos Inteligentes	Conectividade	Habilitador	Integrador	Provedor de Serviço
Exemplos de atores	Fabricantes de: - Processadores; - Memórias; - Sensores; - Atuadores; - Agregadores / modems; - SIM cards; - Baterias; - Módulos embarcados; - *Gateways;* - Funcionalidade de segurança para *endpoints;* - Funcionalidade de gerenciamento de *endpoints.*	Fabricantes de: - Eletrodomésticos; - Veículos; - Estações de monitoramento; - Equipamentos de automação.	Provedores de: - Soluções de PAN[5] e NAN[6]; - Operadoras; - MVNO[7]; - Solução de segurança para redes; - Solução de gestão de rede; - Fabricantes de equipamentos de rede.	Provedores de: - Armazenamento de dados; - Orquestração de Dados; - Middleware; - *Analytics;* - Controle dos *endpoints;* - Solução de gerenciamento de *endpoints;* - Solução e funcionalidade de segurança (*endpoints*, armazenamento, aplicativos).	Provedores de: - Interfaces de APIs. - Orquestração de Serviços; - Integração com sistemas *back-end* (ERP[8]).	Provedores de Serviço para: - Consumidores; - Empresas.

[5] PAN: personal area network; rede de computadores utilizada para transmissão de dados entre dispositivos como computadores, telefones, tablets e assistentes digitais pessoais.

[6] NAN: neighborhood area network; ramo de hotspots Wi-Fi e redes locais sem fio (WLAN), que permitem aos usuários se conectar à Internet rapidamente e com menor custo.

[7] MVNO: mobile virtual network operator; provedor de serviços de comunicações sem fio que não possui a infraestrutura de rede sem fio sobre a qual presta serviços a seus clientes.

[8] ERP: Enterprise resource planning; Software de gerenciamento de processos de negócios que permite que uma organização use um sistema de aplicativos integrados para gerenciar o negócio e automatizar muitas funções de back office relacionadas à tecnologia, serviços e recursos humanos

3. TENDÊNCIAS TECNOLÓGICAS

Foi possível observar uma série de tendências relativas ao desenvolvimento de tecnologias em IoT em cada uma das camadas tecnológicas. Tais tendências, apresentadas na tabela a seguir, refletem a direção geral das tecnologias, com base nas evidências observadas durante a fase de pesquisa e coletas de insumos.

Tendências por camada tecnológica

Camada tecnológica	Tendências
Dispositivos	1. *Sensor nodes* de IoT tendem a continuar se valendo de unidades micro controladas (UMCs) como computador principal; a evolução destes deve ser marcada principalmente pela queda de custo em relação ao aumento de capacidade. 2. Alguns casos de uso devem demandar um alto desempenho computacional embarcado em objetos inteligentes. 3. Profissionais para o desenvolvimento de software embarcado devem ser cada vez mais requisitados pelo mercado. O diferencial destes profissionais provavelmente se dará pela proficiência no uso de projetos de código aberto de referência. 4. A grande diversidade de casos de uso de IoT deve estimular inovações em microeletrônica, como SoC customizado, e mecanismos como o MPW (*Multi-Project Wafer*), com potencial de viabilizar projetos de microeletrônica para IoT em *start-ups*. 5. *Gateways* devem ser utilizados para uma grande quantidade de casos de uso, prestando serviços (por exemplo, acesso à rede e segurança) aos dispositivos.
Rede	1. As tecnologias SDN (*Software Defined Network*) e NFV (*Network Function Virtualization*) devem minimizar o impacto da IoT no *core* das redes. 2. Para as tecnologias de conectividade de curto alcance *indoor*, tende a ser maior a adoção dos padrões 802.11 do IEEE[9], dada a hegemonia do WiFi para acesso à internet sem fio tanto no ambiente residencial como no corporativo. 3. Um volume considerável de casos de uso deve utilizar dispositivos móveis pessoais (*smartphones* e *tablets*) como *gateways* para sensores e atuadores sem fio, por meio da tecnologia BLE (*Bluetooth Low Energy*). 4. As diversas tecnologias para conectividade de longo alcance provavelmente coexistirão para atender a diferentes casos de uso, seja em faixa de frequência licenciada (com vantagem em áreas com cobertura adequada de rede celular), seja em faixa de frequência não licenciada (utilizada por atores que explorarem a vantagem de *first movers*). 5. O principal habilitador para tratar dos elementos conectados à rede deve continuar sendo o IPv6.

[9] IEEE: Institute of Electrical and Electronics Engineers: associação profissional de engenheiros elétricos e eletrônicos; busca o avanço educacional e técnico da engenharia elétrica e eletrônica, e disciplinas aliadas.

Camada tecnológica	Tendências
Suporte a Serviços e Aplicações	1. É provável que o modelo arquitetural de *Edge Computing* seja necessário para tratar de casos de uso que requerem baixa latência; *data centers* devem ficar cada vez mais automatizados, tendo suas funcionalidades virtualizadas e definidas por software. 2. Diversos protocolos de camada de aplicação possivelmente continuarão a ser utilizados, e o *middleware* deve ter um importante papel na interoperabilidade; é provável a coexistência de algumas soluções de *middleware* por vertical. 3. O desenvolvimento de soluções customizadas tende a ser facilitado na medida em que funcionalidades preexistentes em diversas plataformas em nuvem se tornem disponíveis. 4. Bancos de dados não relacionais tendem a ser comuns em diversos casos de uso, dada a tendência de IoT de gerar grandes quantidades de dados (*Big Data*) processados através de *machine learning* de *batch* ou *stream processing*, de acordo com a necessidade do tempo de resposta. 5. No que diz respeito à experiência do usuário, várias tecnologias tendem a se desenvolver, como realidade aumentada e os assistentes virtuais.
Segurança da Informação	1. Novas soluções de IoT tendem a ser cada vez mais voltadas para o princípio de *security by design*. 2. Os maiores desafios têm sido observados na camada de dispositivos, em particular aqueles restritos em termos de processamento, memória e comunicação, que demandam criptografia leve, com suporte complementar nos *gateways*. 3. A segurança das redes deve se dar pela adoção de variantes de protocolos de segurança IP para IoT já consolidados, tais como DTLS, IPsec, *Advanced Encryption Standard*, dentre outros. 4. Em um primeiro momento de implantação da IoT, a necessidade de segurança faz com que cada fabricante verticalize sua solução de segurança, dificultando o desenvolvimento do ecossistema de IoT. 5. Com o amadurecimento da IoT, a falta de padrões de segurança tem levado organismos de padronização a abordar o assunto de maneira segmentada, tratando grandes áreas temáticas, tais como saúde, transportes e cidades inteligentes. 6. A utilização da tecnologia *blockchain* em IoT pode permitir que as aplicações sejam desenvolvidas e utilizadas com um nível maior de segurança e privacidade, dadas as características intrínsecas desta tecnologia. Contudo, é prematuro afirmar que *blockchain* será escolhida para tratar os diversos desafios das implementações e casos de uso IoT de modo geral.

As tendências apresentadas acima serão detalhadas nos próximos subcapítulos. Com o objetivo de facilitar o entendimento, será utilizado um conjunto de casos de uso para contextualizar a aplicação das tendências. O QUADRO 6 a seguir descreve estes casos de uso, e suas respectivas necessidades em termos de tecnologias de IoT.

QUADRO 6

Exemplos de casos de uso utilizados para ilustrar as tendências tecnológicas observadas

Rastreio de contêineres	Compartilhamento de veículos autônomos	Manutenção preditiva de turbinas de avião	Irrigação inteligente	Casa Inteligente
▪ Mensagens enviadas por B*eacon bluetooth low energy* (BLE) identificam o contêiner a que está associado ▪ *Gateways* instalados em alguns pontos do trajeto (ex.: portos) recebem, processam a informação localmente, e a enviam para aplicação de rastreio através de conectividade com a Internet. A aplicação dever ser centralizada e acessível globalmente. ▪ Smartphones podem assumir a função dos *gateways* em áreas sem infraestrutura fixa de *gateways*.	▪ Diversos sensores, incluindo câmeras, são utilizados para detecção do ambiente ao redor do veículo ▪ O veículo deve ser capaz de tomar decisões localmente e de forma rápida para evitar acidentes. ▪ Também deve possuir conectividade para que a aplicação possa enviar as requisições dos usuários.	▪ Dados dos sensores das turbinas armazenados durante o voo devem ser descarregados e processados para indicar ações de manutenção ▪ Processamento dos dados não pode demorar mais que algumas poucas dezenas de minutos para que a aeronave receba o aval para iniciar o próximo voo.	▪ Restrição de espaço e custo demanda por dispositivo otimizado que congregue sensor de umidade, bateria, circuito de *energy harvesting* para painel fotovoltaico, bateria, processamento e módulo *wireless*. ▪ Para viabilizar a implantação em áreas extensas as Informações geradas devem ser captadas por poucas estações rádio base de grande cobertura. ▪ Dada a dificuldade de acesso à Internet os dados devem ser processados localmente.	▪ Através do uso de um *smart speaker* o morador solicita por comando de voz que o ventilador do cômodo seja acionado ▪ *Smart speaker*, conectado à Internet capta e envia o *stream* de áudio para a nuvem para que seja processado, ▪ Ventilador recebe da aplicação em nuvem um comando simples e de fácil processamento para que inicie o funcionamento.

FONTE: Análise do consórcio

3.1. Dispositivos

Na **Camada de Dispositivos, que inclui os dispositivos de acesso (como smartphones, sensores, dentre outros) e *gateways*,** estão concentradas as maiores restrições não-funcionais inerentes à IoT, em especial: custo, consumo energético e espaço físico. Isso gera alguns desafios, dentre eles:

- **Aumento significativo do custo total de objetos de baixo valor**: Em objetos de baixo valor, a adição de sensoriamento, inteligência e comunicação aumenta significativamente o custo total dos objetos, impactando casos de uso como rastreio de latas de refrigerante e identificação de violação de embalagens de alimentos congelados;
- **Restrições quanto ao consumo de energia**: Em grande parte dos casos de uso de IoT, não é possível conectar os objetos à rede elétrica. Portanto, objetos inteligentes precisam ser alimentados por bateria ou indução eletromagnética-um processo limitado em termos de fornecimento de energia. Desta forma, o consumo de energia deve ser suficientemente baixo. Esse desafio afeta casos de uso com objetos de menor tamanho, como uma pílula que mede a temperatura interna do paciente e transmite os dados para um aplicativo do *smartphone*.

Contudo, a evolução dos processos da integração de microeletrônica, ainda obedientes à lei de Moore[10], tem propiciado a superação desses desafios em um número cada vez maior de aplicações. As principais tendências da camada de dispositivos estão elencadas a seguir.

1. O crescimento nas vendas das **arquiteturas de micro controladores de 32 bits**, que já superam em valor de mercado as arquiteturas de 8 bits, é um efeito da IoT no mercado de semicondutores. Tais arquiteturas de 32bits são mais propícias para o desenvolvimento de objetos inteligentes, uma vez que estes não requerem apenas capacidade de processamento, mas também de comunicação, o que, por sua vez, demanda uma grande quantidade de protocolos e sistemas operacionais embarcados.

   Apesar dessa evolução, é provável que **arquiteturas mais robustas, como a de microprocessadores, não se tornem dominantes em *sensor nodes*** para a maioria dos casos de uso de IoT nos próximos anos. Assim, a massificação da implantação deve se dar menos pelo aumento na capacidade dos dispositivos (com a adoção de arquiteturas superiores a 32 bits e maior quantidade de memória), e mais pela redução de custos, posto que esta permite atender a um número maior de casos de uso.

[10] Lei de Moore: teoria que prevê que o número de transistores em um processador dobraria, em média, a cada dois anos, mantendo o mesmo (ou menor) custo e espaço

2. Dada a grande amplitude de aplicações de IoT, **alguns objetos devem demandar capacidade computacional bastante elevada**. Para exemplificar, os veículos autônomos terão capacidade computacional local similar à de servidores em *data centers*.

3. A massificação de aplicações baseadas em micro controladores tem um impacto na mão de obra. Arquiteturas micro controladas, mesmo de 32 bits, em geral não permitem de forma satisfatória o uso de linguagens de programação de alto nível, como Java e Python. Nesses ambientes prevalece, o uso de linguagem C/C++. Assim, restringe-se significativamente **o número de profissionais para o desenvolvimento de software embarcado capacitados em linguagens com C/C+**, hoje estimado em cerca de 500 mil em todo o mundo.

   Essa restrição de mão de obra também se configura como uma oportunidade para países que desejam atender a demandas de desenvolvimento de projetos de objetos inteligentes. Para tal, o investimento de recursos para formação de engenheiros de software embarcado pode resultar na criação de um diferencial estratégico. No entanto, a formação desse tipo de profissional pressupõe a capacitação necessária em projetos de código livre de referência, como sistemas operacionais de tempo real, que já implementam diversas funcionalidades necessárias à IoT. Desta forma, mais do que proficiência em linguagens de programação de menor nível, o profissional que desenvolve software embarcado para IoT deve realizar a customização de soluções já desenvolvidas para demandas específicas.

4. **Diante do amplo espectro de casos de uso de IoT, abre-se a oportunidade para novos atores no segmento de microeletrônica de propósito específico**. Embora as previsões de crescimento de dispositivos conectados à rede indiquem valores da ordem de dezenas de bilhões implantados nos próximos anos, os inúmeros casos de uso, com necessidades distintas, devem impedir uma predominância de um ou poucos tipos de objetos inteligentes. Isso se configura como um desafio para o desenvolvimento de componentes integrados para atender a um grande número de casos de uso diversos, uma vez que a previsão relativamente baixa de volume não justifica o alto investimento exigido por esses projetos.

   De forma geral, os casos de IoT podem ser agrupados em três blocos, de acordo com o volume de vendas e o número de casos de uso atendidos, como mostram o QUADRO 7 e a descrição a seguir:

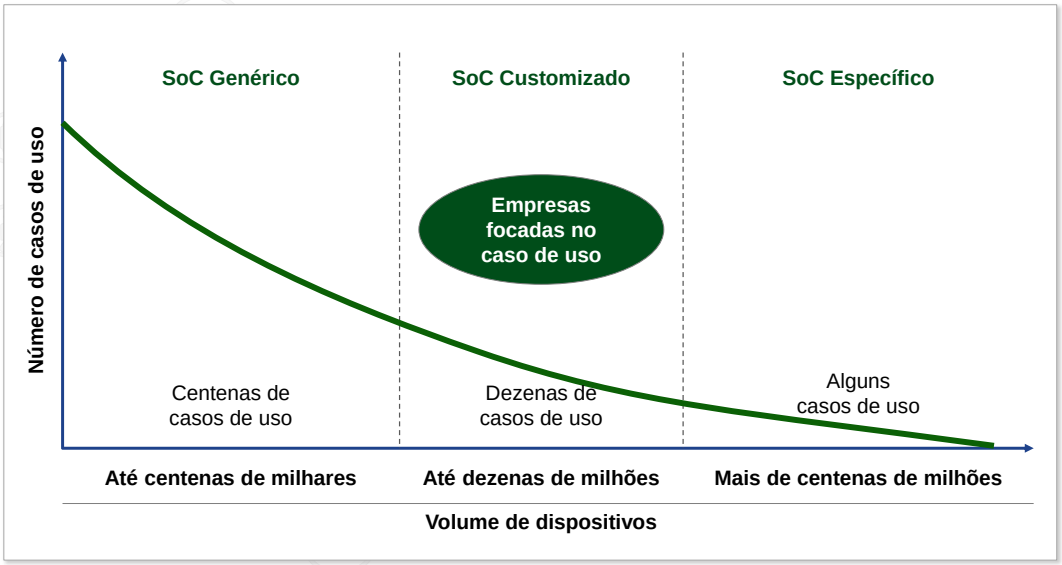
   - **SoC específico**: Pequeno número de casos de uso, que demandam um volume de vendas de centenas de milhões de SoCs[11]; nesses casos, é justificado o desenvolvimento de semicondutores específicos. Estão bem posicionadas nesse mercado grandes empresas de semicondutores;

[11] SoC: system-on-a-chip: circuito que integra os componentes de um computador ou de outros sistemas eletrônicos, como *smartphones*

- **SoC customizado**: Maior número de casos de usos (dezenas), com volumes de até dezenas de milhões de dispositivos por ano, o que abre espaço para inovações em microeletrônica, como SoCs customizados, que, no contexto de um ecossistema de IP (Intellectual Property), *cores* e técnicas de desenvolvimento ágil, permitem a criação em poucos meses de semicondutores mais competitivos que as soluções especializadas em nível de eletrônica discreta, e com desenvolvimentos que se pagam com volumes a partir da ordem de poucos milhões de unidades. Da mesma forma, técnicas como MPW (Multi Project Wafer)[12] tornam possível a viabilização das primeiras amostras com investimentos moderados. Neste caso, merecem destaque os atores cujo foco recaia na criação de soluções para o atendimento de casos de uso específicos;
- **SoC genérico**: Grande número de casos de uso (centenas), que devem gerar demandas na ordem de até centenas de milhares de unidades por ano. Neste caso, são utilizados SoCs genéricos, capazes de tratar de forma não ótima diversos casos de uso por meio da especialização em nível de eletrônica discreta e software embarcado.

QUADRO 7

Casos de uso versus volume de dispositivos



FONTE: Análise do consórcio

[12] Multi Project Wafer: serviço de protótipo que permite que vários clientes e projetos compartilhem recursos comuns, como wafers de engenharia, reduzindo os custos de design e prototipagem.

5. *Gateways* devem ser utilizados para uma grande quantidade de casos de uso, prestando serviços (por exemplo, acesso à rede e segurança) aos dispositivos. Os ***gateways*** de IoT devem ter por base o uso de processadores similares aos aplicados em microcomputadores, configurando um mercado mais concentrado e com poucas oportunidades locais em semicondutores. Contudo, também em razão da grande diversidade de casos de uso, deverá haver espaço para o desenvolvimento de soluções no âmbito da eletrônica, empacotamento mecânico e software que implemente funções complementares às capacidades, em geral limitadas, dos *sensor nodes*.

   A título de ilustração, algumas tendências observadas nesta camada podem ser exemplificadas por meio de casos de uso, como mostra o QUADRO 8.

QUADRO 8

Exemplos de relações entre casos de uso e tendências tecnológicas para a camada de dispositivos

Rastreio de contêineres	Compartilhamento de veículos autônomos	Irrigação inteligente	Casa Inteligente
Tendências 1 e 5	**Tendência 2**	**Tendências 3 e 4**	**Tendências 1, 3, 5**
▪ O módulo inteligente adicionado ao contêiner deve ter custo moderado e baixo consumo para permitir a implantação massiva e não tornar a operação inviável dada a troca frequente de bateria. ▪ Os gateways localizados em pontos importantes ao longo do trajeto auxiliam o objeto inteligente a enviar a sua localização para a aplicação em nuvem.	▪ A grande quantidade de sensores, em especial câmeras, gera uma grande quantidade de informação que requer alta capacidade de processamento local para a tomada de decisão.	▪ A heterogeneidade da IoT aliada a requisitos de baixo consumo energético, custo e restrições de espaço demandará por inovações em microeletrônica, como a criação de SoC customizados, SiP e MPW ▪ O desenvolvimento do software embarcado requer mão de obra especializada dada as especificidades deste componente customizado.	▪ Muitos eletrodomésticos possuem restrição de custo, o que limita a capacidade do processamento embarcado. ▪ Diversidade de eletrodomésticos requer software embarcado específico. ▪ *Smart speaker* atua como *gateway* que uniformiza a interface com o usuário e facilita as ações dos objetos.

FONTE: Análise do consórcio

3.2. Rede

Na **Camada de Rede, que inclui os equipamentos que promovem a conectividade entre os dispositivos e a nuvem,** há desafios bastante heterogêneos, uma vez que a IoT abrange inúmeros casos de uso para os quais os requisitos de rede são específicos, tais como:

- Para aplicações de tempo real, como a comunicação entre veículos autônomos, a latência de comunicação, assim como o tempo de resposta, são fatores cruciais que estão diretamente relacionados à rede;
- Aplicações que demandam baixo tráfego de dados e convivem com uma grande dispersão geográfica (por exemplo, agricultura de precisão) impõem um novo paradigma para a evolução das tecnologias, na contramão do que tem sido desenvolvido na última década, onde a maior capacidade de banda era o objetivo predominante.

Devido à diversidade de dispositivos e aplicações, com os mais variados requisitos de qualidade de serviço, a camada de acesso da IoT deverá ser de natureza heterogênea, com **tecnologias de acesso gerais e de nicho compondo um vasto ecossistema**. As principais tendências dessa camada são elencadas a seguir.

1. As tecnologias **SDN (*Software Defined Network*)**[13] e **NFV (*Network Function Virtualization*)**[14], que podem ser empregadas não apenas no *backhaul*, mas também no *core*, devem minimizar o impacto da IoT nas redes. Diferentemente do que ocorre com usuários humanos, a comunicação entre as máquinas, tem em geral um caráter periódico e regular, independentemente do período do dia, do dia da semana, do mês ou do ano. Se os dados, que podem ser da ordem de dezenas de bilhões de dispositivos, forem todos para a nuvem, simultaneamente, poderão gerar gargalos de rede. Ambas as tecnologias permitem reconfigurar a rede de maneira rápida e eficiente, reservando recursos e garantindo qualidade de serviço para as aplicações, conforme necessário.
2. Para as tecnologias de **conectividade de curto alcance *indoor*, tende a ser maior a adoção dos padrões 802.11 do IEEE**. Com o aumento expressivo de dispositivos WLAN em IoT, é provável que seja necessário utilizar uma maior quantidade de soluções baseadas em espectro não licenciado, assim como *femtocells*, para complementar os serviços celulares fornecido pelas operadoras por meio de novas tecnologias complementares às coberturas *outdoor*, por exemplo: LTE-U (*Long Term Evolution – LTE in Unlicensed spectrum*).

[13] Software Defined Network: técnica que permite aos administradores de rede gerenciar dinamicamente o comportamento da rede.

[14] Network Function Virtualization: utiliza tecnologias de virtualização de TI para virtualizar classes de funções de nó de rede em blocos de construção que podem se conectar em conjunto para criar serviços de comunicação.

3. Alguns casos de uso devem utilizar **dispositivos móveis pessoais** (*smartphones* e *tablets*) como ***gateways* para sensores e atuadores sem fio**, por meio da tecnologia BLE (*Bluetooth Low Energy*).
4. As **diversas tecnologias para conectividade de longo alcance devem coexistir para atender a diferentes casos de uso**, utilizando faixa de frequência licenciada (com **tecnologias padronizados pelo 3GPP**), ou não licenciada (**tecnologias** proprietárias ou semiproprietárias **em faixas não licenciadas como Sigfox e LoRa**).

   As primeiras implantações dessas redes de longo alcance têm sido baseadas em tecnologias proprietárias ou semiproprietárias. Entretanto, no médio e longo prazos, os padrões baseados no 3GPP, como o Narrowband IoT (NB-IoT), tendem a ganhar espaço onde houver cobertura de rede celular, uma vez que se valerão desta infraestrutura e da operação preexistente.

5. Com respeito aos protocolos, o **principal habilitador para tratar** dos elementos conectados à rede **deve continuar sendo o IPv6**. O IPv6 oferece uma série de vantagens, como o acesso a mão de obra familiarizada, o fato de ser o padrão mais utilizado da indústria, além de proporcionar uma série de melhorias de segurança em relação à versão 4. Para contornar as limitações em dispositivos restritos, têm sido desenvolvidos diversos protocolos, como 6LoWPAN (IPv6 *over Networks of Resource-constrained Nodes*), CoAP (*Constrained Application Protocol*) e MQTT (*Message Queuing Telemetry Transport*).

Algumas tendências observadas nesta camada podem ser exemplificadas por meio de casos de uso, como visto no QUADRO 9 a seguir.

QUADRO 9

Exemplos de relações entre casos de uso e tendências tecnológicas para a camada de rede

Rastreio de contêineres	Compartilha-mento de veículos autônomos	Manutenção preditiva de turbinas de avião	Irrigação inteligente	Casa Inteligente
Tendência 3 ▪ Em locais intermediários entre a origem e o destino dos containers, em que seja necessário fazer seu rastreio, o uso de dispositivos móveis como *gateways* será factível por meio da tecnologia BLE	**Tendências 4 e 5** ▪ Em ambiente de alta disponibilidade de redes de acesso celulares, a comunicação entre veículos autônomos se valerá da ampla cobertura provida pelas tecnologias baseadas no 3GPP ▪ A necessidade de tratar univocamente de veículo requererá a utilização de tratamento por IPv6	**Tendência 1** ▪ A transferência de grandes quantidades de informação extraídas dos inúmeros sensores das turbinas dos aviões será possível por meio do emprego de técnicas de virtualização de rede que permitem alocar dinamicamente os recursos a fim de evitar gargalos em momentos específicos	**Tendência 4** ▪ Em ambientes com cobertura deficitária de redes de acesso celular as soluções baseadas em tecnologias proprietárias ou semiproprietárias podem ser utilizadas para prover conectividade em áreas amplas	**Tendência 2** ▪ Em ambientes *indoor* as tecnologias baseadas no padrão 802.11 devem ser largamente empregadas, haja vista sua já predominância nesses ambientes, seja em uso residencial ou corporativo

FONTE: Análise do consórcio

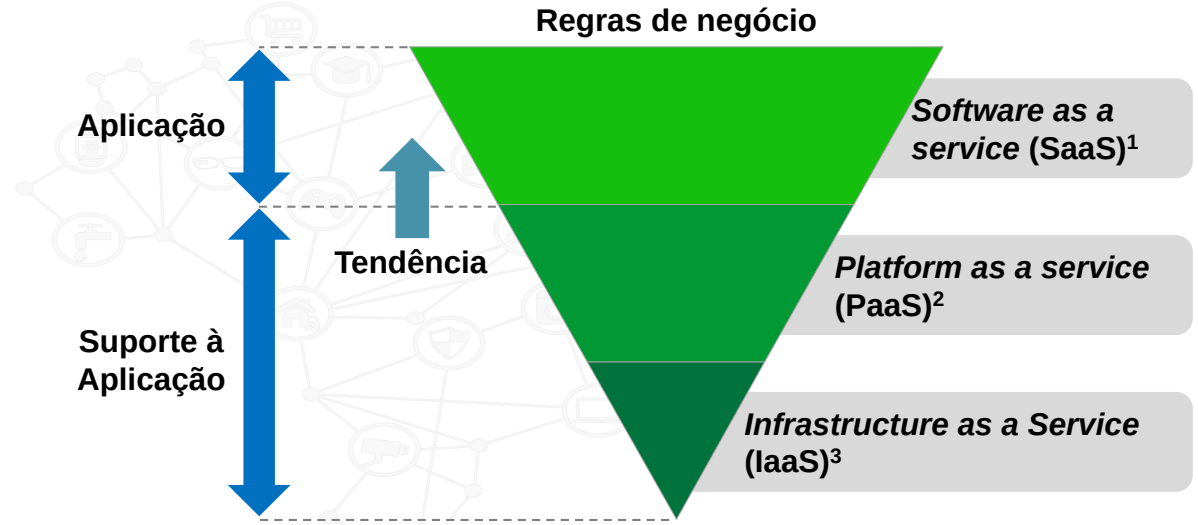
3.3. Suporte a serviços e aplicações

Nesta camada ocorre a concentração dos dados gerados e transmitidos pelos objetos inteligentes para serem processados e analisados, gerando o valor esperado dos casos de uso. Assim, há o desafio de se armazenar e tratar a imensa quantidade de dados, em especial quando existem rígidos requisitos de tempo de respostas a serem atendidos, por exemplo:

1. A IoT deve impactar diretamente a infraestrutura de *data centers*, fazendo com que estes evoluam para atender às novas aplicações. Desta forma, espera-se que sejam criados novos **micro *data centers* distribuídos** e mais próximos das bordas (*edge computing*), seguindo um modelo de *cloudlets*, onde ambientes de nuvem reduzidos executam aplicações especializadas no tratamento, filtragem inicial dos dados e resposta a demandas que exigem baixa latência e maior agilidade na resposta.
   Adicionalmente, esses *data centers* ficarão cada vez mais **automatizados,** tendo suas **funcionalidades virtualizadas e definidas por software**. Os modelos de armazenamento de dados devem ser unificados por meio de interfaces centralizadas e bem definidas.
2. Em relação ao ***middleware***, devido à natureza diversa dos casos de uso em IoT, **é provável que algumas arquiteturas coexistam por vertical**. Com o amadurecimento do ecossistema, tende a haver uma consolidação de alguns deles, tornando necessário interoperá-los. Esse fato deve redundar na padronização ou no surgimento de mediadores/orquestradores para facilitar a integração.
   Assim como **devem coexistir várias arquiteturas de *middleware***, também devem coexistir vários protocolos de comunicação, uma vez que cada um tem características específicas que justificam sua aplicabilidade a casos de uso bem definidos. Os produtos de *middleware* devem ser integráveis aos protocolos do seu nicho de aplicação.
3. O **desenvolvimento de soluções customizadas tende a ser facilitado** na medida em que **funcionalidades preexistentes em diversas plataformas em nuvem se tornem disponíveis**. Com isso, o desenvolvimento de aplicações tende a ter um *time-to-market* cada vez menor, dependendo menos de *expertise* em programação e mais de conhecimento dos negócios em si, como pode ser visto no QUADRO 10.

QUADRO 10

Tendência para desenvolvimento de aplicações de IoT



1 Modelo de entrega em que o software é licenciado em uma base de assinatura e é hospedado centralmente
2 Categoria de serviços de computação em nuvem que fornece uma plataforma que permite aos clientes desenvolver, executar e gerenciar aplicativos
3 Tipo de computação em nuvem que fornece recursos de computação virtualizados pela Internet

FONTE: Análise do consórcio

4. O armazenamento de dados em IoT é um problema de *Big Data*, devido ao volume de dados e, consequentemente, **bancos de dados não relacionais tendem a ser utilizados em diversos casos de uso**. Já os **bancos de dados relacionais devem continuar relevantes nos cenários em que os dados são estruturados ou podem ser pré-processados**. Outra forma de tratar o volume de dados vem da adoção do conceito de dados espaço-temporais, por ser uma forma relevante de dividi-los por local e horário de ocorrência. Essa evolução tende a alavancar os dados para diversos usos, como monitoramento de dados para prevenção, dados para valorizar a automação via validação e enriquecimento de dados, além dos mais diversos usos do *analytics*.

   A **Inteligência Artificial (IA)** é atualmente incorporada à própria aplicação, com o suporte de bibliotecas padronizadas. Alguns atores, no entanto, buscam oferecer, em suas plataformas, serviços de IA mais ou menos complexos. A adoção dessas plataformas, porém, tem sido restrita, devido ao fato de que o uso eficiente de IA demanda alto grau de customização para explorar características específicas de cada problema abordado.

   Outro ponto que merece destaque é como conciliar a alta demanda de mecanismos de IA com o **pequeno número de profissionais capacitados na área**. O uso de métodos baseados em *transfer learning* pode acelerar o desenvolvimento de aplicações de IA por meio do reuso de modelos, porém um maior desenvolvimento de técnicas de *meta-learning* pode vir a ser a solução adequada no médio e longo prazos.

Adicionalmente, considerando a necessidade de sistemas mais dinâmicos, deve ganhar relevância o **aprendizado a partir de fluxos de dados** (*stream*), em contraposição ao atual domínio das técnicas baseadas em grandes cargas de dados (*batch*). Formas de **aprendizado contínuo**, como aprendizado *online* e por reforço, tendem a crescer em relevância no médio prazo.

5. No que diz respeito à **experiência do usuário**, várias tecnologias tendem a se desenvolver, como **realidade aumentada**, **realidade virtual** e os **assistentes virtuais**.

Algumas tendências observadas nesta camada podem ser exemplificadas por meio de casos de uso, como visto no QUADRO 11 a seguir.

QUADRO 11

Exemplos de relações entre casos de uso e tendências tecnológicas para a camada de suporte a serviços e aplicações

Rastreio de contêineres	Manutenção preditiva de turbinas de avião	Irrigação inteligente	Casa Inteligente
Tendência 3	**Tendências 1 e 4**	**Tendência 2**	**Tendência 5**
▪ Aplicação desenvolvida em plataforma em nuvem (PaaS) com cobertura global e que provê diversas funcionalidades que simplificam o seu desenvolvimento	▪ Havendo indisponibilidade de rede o uso de técnicas como *edge computing* associado a *batch processing* permite atender os rígidos requisitos de tempo de processamento ▪ Por sua vez, o data center deve ser dinâmico para acomodar horários de pico no aeroporto	▪ Dadas as restrições de conectividade com a rede ampla, os dados são armazenados em *middleware* instalado localmente e especializado para casos de uso do ambiente rural, facilitando o desenvolvimento da aplicação que controla os aspersores de água que irrigarão a plantação com maior eficiência	▪ Através do uso de um *smart speaker* o morador solicita por comando de voz que o ventilador do cômodo seja acionado. O *stream* de áudio é enviado para a nuvem para que seja processado pelo sistema de assistente virtual que envia o comando para que o ventilador seja ligado

FONTE: Análise do consórcio

3.4. Segurança da informação

Independentemente da camada tecnológica, em um curto prazo de tempo, os dispositivos inteligentes ou "coisas" devem se tornar participantes ativos no ambiente, onde serão capazes de interagir e comunicar-se entre si, trocar informações coletadas e reagir aos acontecimentos do mundo físico sem intervenção direta do ser humano. Contudo, essa realidade traz inúmeros desafios referentes à segurança de IoT, como aumento da superfície de ataque à rede, restrição dos dispositivos no sentido de suportar técnicas e mecanismos robustos de segurança, mau uso por parte do usuário e até mesmo falhas de projeto do produto. Assim, a segurança pode ser considerada um dos principais desafios tecnológicos de IoT, compreendendo componentes críticos de qualquer solução. Por exemplo, a confidencialidade, a autenticidade e a privacidade dos interessados devem ser asseguradas para permitir a adoção em massa de IoT. As principais tendências dessa camada são elencadas a seguir.

1. Novas **soluções de IoT tendem a ser cada vez mais voltadas para o princípio de *security by design***, considerando desde a arquitetura a ser utilizada, passando pela definição e desenvolvimento da aplicação, da comunicação, do dispositivo, até a conscientização do usuário, seguindo os pilares da segurança em IoT: confidencialidade, integridade, disponibilidade, autenticidade e privacidade.
2. Os **maiores desafios têm sido observados na camada de dispositivos**, em particular dispositivos restritos em termos de processamento, memória e comunicação, que demandarão **criptografia leve** (*lightweight cryptography*). Uma alternativa é contar com **suporte complementar nos *gateways***, para assegurar proteção fim-a-fim.
3. No que diz respeito à **segurança das redes**, a adoção de variantes de protocolo de segurança IP para IoT com primitivas criptográficas de chave pública, tais como DTLS (*Datagram Transport Layer Security*), DEX (HIP *Diet Exchange*) e IKEv2, podem atender aos requisitos da IoT relacionados a escalabilidade e interoperabilidade. Adicionalmente, a **segmentação de rede**, técnica amplamente difundida e utilizada como melhor prática nas atuais redes, deve ser essencial em IoT, pois garante que os dispositivos conectados não prejudiquem a segurança da rede, evitando assim o acesso indevido e a possível propagação de *malware* por seu intermédio. Outra possível abordagem seria a utilização de mecanismos dinâmicos de segregação, como controle para conter um ataque e limitar os danos de um incidente.
4. Em termos de soluções de segurança fim-a-fim (entre o dispositivo e a aplicação), dada a falta de uma padronização amplamente adotada nesta área, observa-se a verticalização por fornecedor, o que desfavorece o amadurecimento de um ecossistema mais robusto, em que o usuário pode adquirir dispositivos e aplicações de fornecedores distintos que interoperem.
5. Com o amadurecimento da IoT, no que diz respeito à **gestão de segurança para IoT**, a falta de padrões tem levado organismos de padronização a **abordar o assunto de maneira segmentada**, tratando de grandes **áreas temáticas**, tais como casas, saúde, cidades e transportes inteligentes.

6. A utilização da tecnologia ***blockchain* em IoT pode permitir** que as aplicações sejam desenvolvidas e utilizadas com **um nível maior de segurança e privacidade**, descentralizando a confiança, **dadas as características intrínsecas da tecnologia**, tais como: segurança, rastreabilidade, imutabilidade e auditoria. Contudo, apesar de iniciativas de empresas e *startups*, considerando a maturidade que se encontra a tecnologia, **é prematuro afirmar que *blockchain* será escolhida para tratar os diversos desafios** das implementações e casos de uso IoT de modo geral.

Algumas tendências observadas nesta camada podem ser exemplificadas por meio de casos de uso, como visto no QUADRO 12 a seguir.

QUADRO 12

Exemplos de relações entre casos de uso e tendências tecnológicas para a camada de segurança

Rastreio de contêineres	Manutenção preditiva de turbinas de avião	Casa Inteligente
Tendência 2	**Tendências 1 e 4**	**Tendências 3 e 5**
▪ O uso de mecanismos de criptografia leve, associado a funcionalidades adicionais nos *gateways* provê solução em cenários onde os dispositivos são restritos em termos de processamento	▪ A melhor forma de abordar a segurança em IoT é implementá-la desde a concepção (*security by design*), da arquitetura a ser utilizada, passando pelo desenvolvimento da aplicação, da comunicação, do dispositivo até a conscientização do usuário, seguindo os pilares da segurança em IoT: confidencialidade; integridade; disponibilidade; autenticidade; e privacidade ▪ Dada a falta de um padrão de fato, o fabricante da turbina desenvolve todos os mecanismos de segurança o que obriga o usuário a ter que usar a aplicação de *analytics* deste fornecedor uma vez que este é o único software que consegue se valer dos dados desse hardware	▪ Protocolos existentes como DTLS, IPsec, dentre outros, são capazes de tratar de segurança de rede, ao passo que técnicas de segmentação podem ser usadas de maneira complementar para isolar eventuais ocorrências e impedir a propagação de ataques ▪ Um consórcio de fabricantes de eletrodomésticos foi formado para garantir a interoperabilidade destes através da definição de mecanismos comuns de segurança

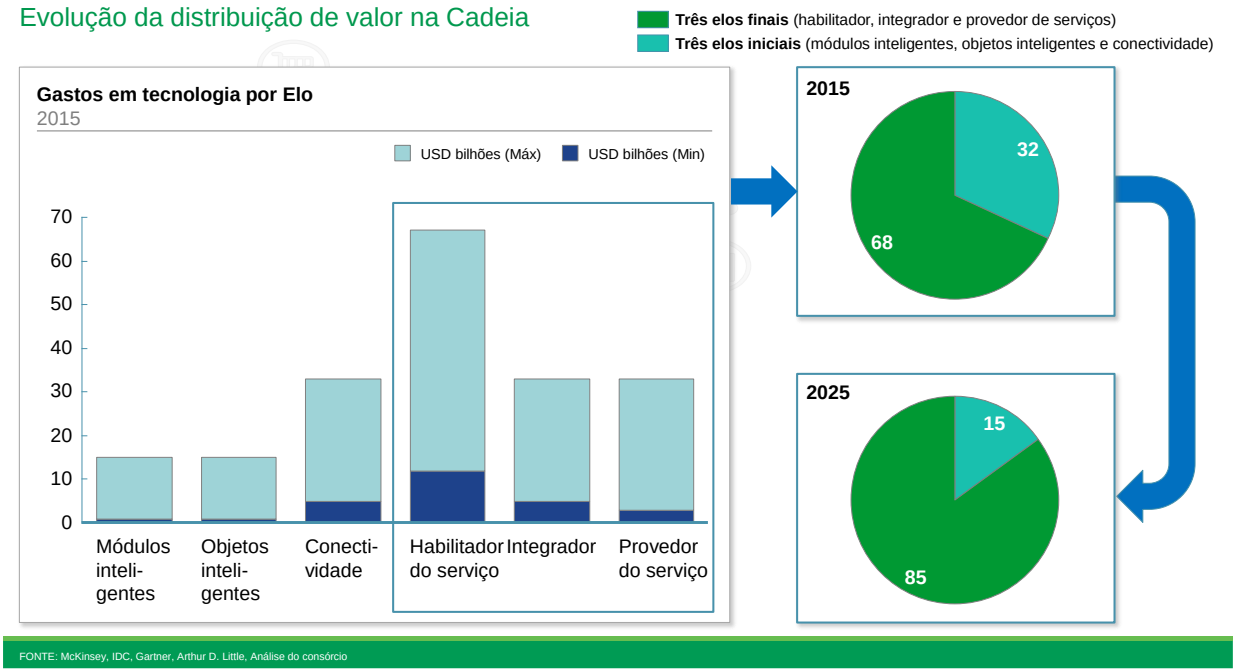
FONTE: Análise do consórcio

4. Cadeia de valor

Durante o levantamento dos principais atores da cadeia de valor de IoT, foram identificadas as seguintes tendências:

- Foi observada uma maior concentração do valor nos elos finais da cadeia, bem como a previsão da ampliação da relevância dos elos finais nos próximos anos. Por exemplo, os elos Habilitador, Integrador e Provedor de Serviços foram responsáveis por 68% dos USD 45 a 135 bilhões gerados na cadeia tecnológica global de IoT em 2015; em 2025, estima-se que a participação desses elos suba para 85% de um total de USD 273 a 777 bilhões, conforme indica o QUADRO 13 a seguir.

QUADRO 13



FONTE: McKinsey, IDC, Gartner, Arthur D. Little, Análise do consórcio

- Os grandes atores (mais de mil funcionários) operam, em geral, em mais de uma vertical e camada tecnológica, e estão buscando oportunidades de negócio em outros elos da cadeia. Empresas de menor porte, por outro lado, atuam principalmente em uma vertical específica, e na camada de Suporte a Serviço e Aplicação, ofertando, na maioria dos casos, soluções para análises computacionais, que podem ser customizadas para mercados de nicho. O elo Habilitador é o que apresenta a maior quantidade de novos entrantes. Com o desenvolvimento do mercado de IoT, podem surgir oportunidades para novos entrantes na camada de Suporte a Serviço e Aplicação, dada a presença de um grande número de novos entrantes (pequenos atores).
- A análise de oportunidades de nicho realizada para as iniciativas internacionais de IoT confirma que se trata de um ecossistema emergente. Nota-se que atores tem buscado

um posicionamento estratégico, explorando soluções que poderão atingir mercados mais amplos (*mainstream*), seja em verticais específicas ou em um conjunto delas. Dentre os atores analisados, 43% deles atuam no Brasil.

- Verificou-se maior número de alianças para padronização e difusão da IoT na camada de Rede e na camada de Suporte a Serviço e Aplicação. Além disso, grandes atores participam como patrocinadores de alianças em mais de uma camada, inclusive em camadas em que não atuam tradicionalmente.

5. Agradecimentos

Gostaríamos de agradecer aos seguintes pesquisadores e profissionais que contribuíram por meio de sua participação no Workshop Tendências Tecnológicas de IoT e entrevistas individuais:

Amanda Remes Mattiuz (VENTURUS) • André Santos (FIT) • Antônio Alberti (INATEL) •Antonio Alfredo Ferreira Loureiro (FCO/UFMG) • Arthur Henrique César de Oliveira (VON BRAUN) • Átila Xavier (CETUC) • Bruno Herrera (CERTI) • Carlos Rodrigues (CETUC) • Daniel Pereira (CESAR) • Eduardo Peixoto (CESAR) • Fabio Lima (FEI) • Felipe Cury (PARQUE TECNOLÓGICO DE SJC) • Fredy João Valente (UFSCAR) • Giordano Cabral (CESAR) • Guilherme Travassos (COPPETEC) • João Paulo Cruz Lopes Miranda (VENTURUS) • José Scodiero (SBMICRO) • Kiev Gama (CESAR) • Laisa Costa (LSITEC) • Lauzier Pereira de Araújo (VENTURUS) • Leandro Augusto da Silva (MACKENZIE) • Leandro Castro Nunes (MACKENZIE) • Leonardo Moreira Resende (FITEC) • Luciano Roncalio (CERTI) • Marcelo Abreu (VENTURUS) • Marcelo Nunes (PARQUE TECNOLÓGICO DE SJC) • Marcelo Sáfadi (PARQUE TECNOLÓGICO DE SJC) • Marlene Pontes (CETUC) • Marta Pudwell Almeida (CETUC) • Matheus Jacon Pereira (IPT) • Mauro Kendi Noda (IPT) • Mauro Miyashiro (ELDORADO) • Moacyr Martucci Jr. (USP) • Nilton I. Morimoto (LSITEC) • Paula Valeiro (FIT) • Renato Franzin (LSITEC) • Rodrigo da Rosa Righi (UNISINOS) • Rodrigo Filev Maia (FEI) • Rodrigo Goncalves Vaz (VAN BRAUN) • Sergio Soares (PORTO DIGITAL) • Tiagos Barros (CESAR) • Werter Padilha (Conselho Consultivo) • Wilhelmus van Noije (LSITEC).

Nossos sinceros agradecimentos também a todos que participaram enviando valiosas contribuições na Consulta Pública para "Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil".