



Tornando cidades inteligentes e IoT uma realidade na América Latina: um guia para os tomadores de decisão

Sobre a GSMA

A GSMA representa os interesses das operadoras móveis em todo o mundo, unindo mais de 750 operadoras com mais de 350 companhias do ecossistema móvel, incluindo fabricantes de terminais e equipamentos, companhias de software, fornecedores de equipamentos e companhias de Internet. Além de realizar estudos sobre a indústria móvel, a GSMA também produz eventos líderes da indústria móvel, como o Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas e a série de Conferências Mobile 360, atraindo mais de 160 mil visitantes únicos de todo o mundo.

PARA MAIS INFORMAÇÕES, POR FAVOR VISITE O WEBSITE CORPORATIVO DA GSMA EM WWW.GSMA.COM . SIGA A GSMA NO TWITTER: [@GSMA](https://twitter.com/GSMA).

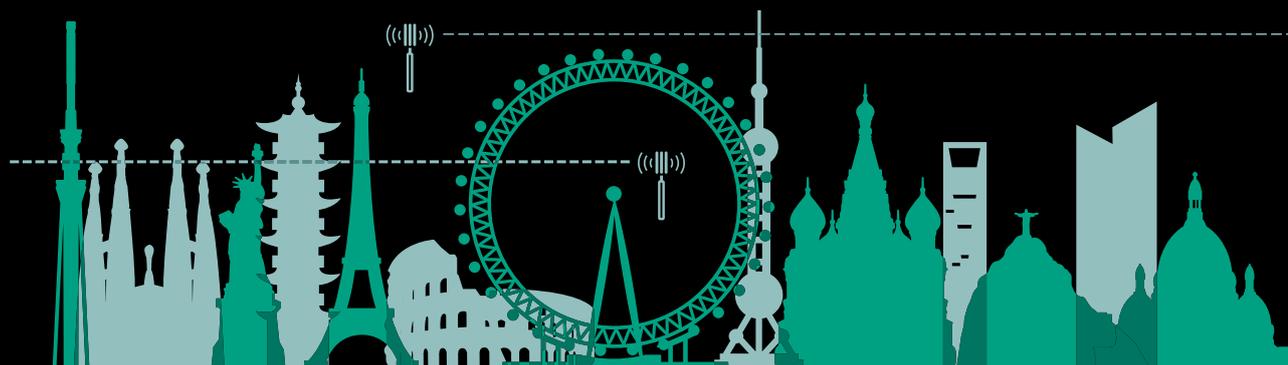
AUTORES

Philippe Moura

Senior Regulatory Manager, Latin America | Government & Regulatory Affairs | GSMA

Stefano Nicoletti

Policy Director - Technology Policy | Regulatory Affairs | GSMA



CONTEÚDO

• SUMÁRIO EXECUTIVO	4
• 1. UMA INTRODUÇÃO À INTERNET DAS COISAS	5
• 2. CONSIDERAÇÕES NA ELABORAÇÃO DE POLÍTICAS PARA A IOT 7	
» 2.1 Modelos de negócios e concorrência na IoT	7
» 2.2 Barreiras na política e regulação existentes para a IoT	9
• 3. O NÍVEL NACIONAL: RECOMENDAÇÕES PARA GOVERNOS NACIONAIS	10
» 3.1 Definir uma estratégia de longo prazo	10
» 3.2 Foster demand via government procurements	12
» 3.3 Abordar privacidade e segurança	13
• 4. O NÍVEL LOCAL: FAZENDO CIDADES INTELIGENTES	15
» 4.1 Promover a coordenação e criar um modelo de governança flexível com um líder independente	15
» 4.2 Desenvolver parcerias e buscar diversas opções de financiamento e investimento	16
» 4.3 Adotar tecnologias abertas e escaláveis e sistemas à prova do futuro	17
» 4.4 Dados abertos: Disponibilizar dados da cidade selecionados para terceiros por meio de portais para promover a transparência e estimular a inovação	18
• ANEXO 1: Lista de verificação de ações para os criadores de políticas de IoT	19
• ANEXO 2: Princípios e premissas para quantificar a IoT e seu impacto econômico em um país	20
• ANEXO 3: Padrões atuais da IoT por vertical	22
• ANEXO 4: Organismos de normatização da IoT	23



SUMÁRIO EXECUTIVO

- A Internet das Coisas traz uma enorme oportunidade para a América Latina. A oportunidade total de receita para a região até 2023 é de US\$ 33 bilhões, segundo a GSMA Intelligence. No entanto, o impacto global sobre o PIB é provavelmente muito mais substancial. Somente no Brasil, a McKinsey prevê que o impacto da IoT até 2020 será de pelo menos US\$ 50 bilhões no PIB do país.
- As soluções de IoT promoverão inovações em uma grande variedade de setores, como energia, saúde e transporte. Elas combinarão redes de comunicação e serviços “off-line” existentes, aumentando a produtividade, diminuindo o desperdício e melhorando o bem-estar dos cidadãos. Se os governos e os formuladores de políticas da América Latina quiserem aproveitar todos os benefícios da IoT e ajudar a eliminar a defasagem tecnológica entre a região e os países desenvolvidos, eles devem adotar as seguintes atitudes:
 - » Resistir à tentação de considerar os serviços da IoT como serviços tradicionais de telecomunicações. O legado regulatório, ou seja, as regulamentações estabelecidas para lidar com os serviços tradicionais de voz e dados, muito antes de a IoT se tornar realidade, serão frequentemente irrelevantes, sufocarão desnecessariamente a inovação na IoT, irão retardar a sua adoção e irão prejudicar os consumidores e os negócios na região.
 - » Facilitar o diálogo entre o regulador e os departamentos e a estratégia entre as várias administrações governamentais. Por exemplo, os reguladores de serviços como utilities e telecomunicações devem definir e trabalhar juntos sobre como promover o uso de medidores inteligentes; os ministérios de Transportes e Comunicações devem definir em conjunto como as redes de comunicação servirão as estradas; os planejadores de cidades inteligentes devem trabalhar juntos para definir as melhores práticas e trabalhar em padrões comuns.
- **UM PLANO DE 3 ETAPAS.** Para criar uma política de IoT, os formuladores de políticas devem criar, primeiro, um plano de três etapas que consiste em definir as necessidades e potencialidades do país, estimar o impacto positivo da IoT em diferentes áreas econômicas e verticais e, em seguida, planejar e implementar ações específicas para permitir esse crescimento.
- **GOVERNO COMO IMPULSIONADOR DE DEMANDA.** Os governos devem considerar seu potencial como impulsionadores de demanda e, quando possível, migrar para a utilização de soluções IoT direcionadas para serviços públicos - de utilities à mobilidade urbana e saúde. Desenvolver PPPs e buscar e/ou oferecer fontes de financiamento variadas pode ser um passo importante para garantir esse objetivo.
- **PADRÕES INTERNACIONAIS E MELHORES PRÁTICAS.** Ao considerar desafios como privacidade, segurança e padronização, os governos devem resistir à tentação de criar regras específicas e padrões nacionais para IoT.
 - » Uma lei geral de proteção de dados que se aplica horizontalmente a todos os setores e serviços - não apenas à IoT - é uma medida importante para garantir a confiança na IoT e garantir níveis consistentes de proteção para os usuários.
 - » No que diz respeito à segurança, é importante que os governos apoiem as melhores práticas e padrões liderados pelo setor, que estão em constante evolução para superar as ameaças, sendo, portanto, mais rápida e mais econômica a adaptação que se comparado a rígidos padrões nacionais.
 - » Os governos também devem observar a miríade de esforços que já estão sendo feitos pelo setor no desenvolvimento de padrões, e sua importância para a interoperabilidade dos serviços nos níveis nacional e internacional - portanto, a criação de padrões nacionais provavelmente seria contraproducente.
- **UMA ESTRUTURA DE GOVERNANÇA FLEXÍVEL E CONFIÁVEL.** No nível do município, é importante que os prefeitos criem um modelo de governança flexível com um líder independente (como um Diretor Executivo de Informações, CIO da sigla em inglês). Para os serviços municipais, os prefeitos devem sempre preferir soluções escaláveis e interoperáveis para evitar o aprisionamento (lock-in) pelos fornecedores. Finalmente, os prefeitos devem considerar a adoção de políticas de dados abertos para fomentar uma economia baseada em dados que possa ser facilmente usada por cidadãos, ONGs e entidades comerciais. Além de fornecer acesso unificado às informações de uma cidade, o compartilhamento de dados apoiaria a comunicação e a análise desses dados, viabilizando a criação de políticas mais transparentes e eficientes, e a criação de valor por meio do desenvolvimento de aplicativos e serviços inovadores.

1. UMA INTRODUÇÃO À INTERNET DAS COISAS

A Internet das Coisas (IoT) se destaca como um dos tópicos mais quentes em muitos setores e países da América Latina, que começaram a perceber as muitas possibilidades e benefícios que podem ser trazidos por um mundo mais conectado. Dos veículos conectados à manufatura totalmente automatizada, monitoramento em tempo real e tomada de decisões em fazendas, a IoT pode acelerar a inovação e o crescimento da produtividade. De fato, a IoT é um dos principais facilitadores para a próxima revolução da produtividade na indústria e nos serviços. O impacto positivo da IoT para cidadãos, consumidores, empresas e governos incluirá a melhoria da saúde e bem-estar individual, apoio a governos no fornecimento de uma infraestrutura melhor e na redução de custos de serviços como saúde, reduções nas emissões de carbono, o aumento do acesso à educação e outros serviços, e a melhoria da eficiência energética e da segurança nos transportes. Somente pelo seu

impacto positivo, a IoT deve ser um assunto importante para os formuladores de políticas. A GSMA Intelligence prevê que haverá mais de 1,3 bilhão de conexões IoT na América Latina até 2025 (veja a figura 1 abaixo).

Segundo a Machina, a oportunidade de receita total para a América Latina até 2023 é de US\$ 176 bilhões, dos quais US\$ 82 bilhões serão da própria aplicação (3% ou US\$ 5 bilhões corresponderiam à conectividade) e US\$ 94 bilhões aos serviços que podem ser gerados em relação a esse aplicativo, como monetização de dados, integração de sistemas e substituição de middleware. No caso do Brasil, a McKinsey prevê que o impacto da IoT até 2020 será de pelo menos US\$ 50 bilhões somente no PIB brasileiro!

Além do impacto econômico direto e da geração de receita, a IoT, como a maioria dos serviços de telecomunicações, pode gerar um impacto muito maior na economia. A Frontier Economics estima que um aumento

1. <https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-planodeacao-produto-8.pdf?MOD=AJPERES&CVID=IXysvoX&CVID=IXysvoX&CVID=IXysvoX&CVID=IXysvoX>

Figura 1: Conexões Totais IoT na América Latina, 2010-2025
Fonte: GSMA Intelligence

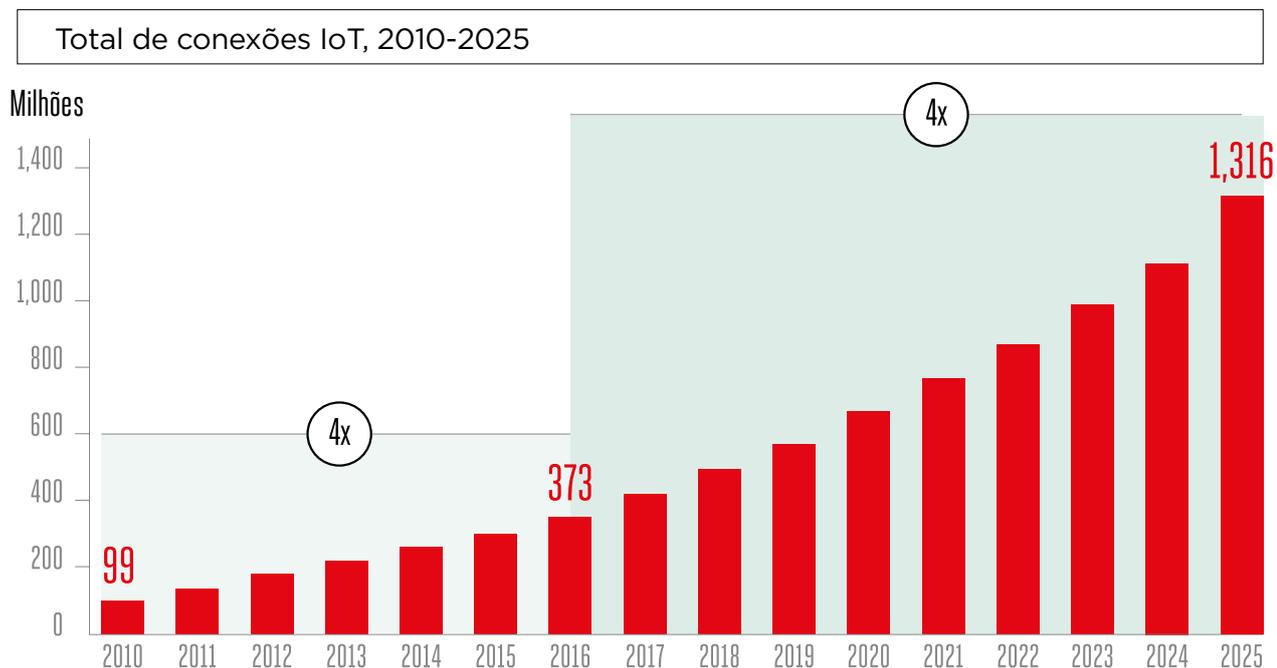
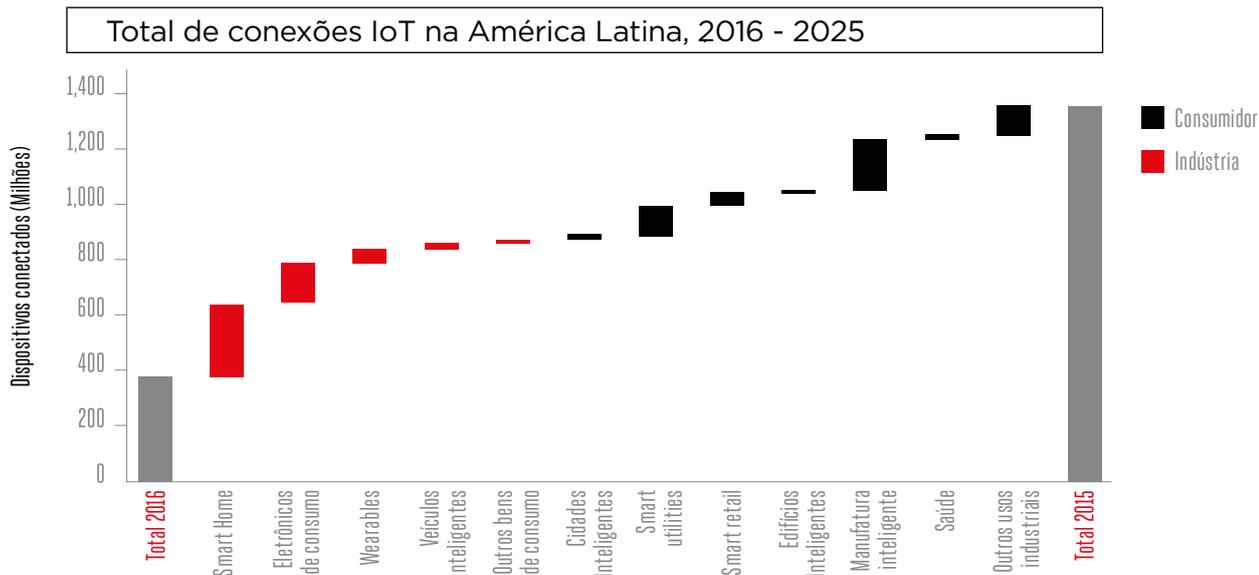


Figura 2: Total de conexões IoT na América Latina, adições de redes, 2016-2025
 Fonte: GSMA Intelligence



de 10% nas conexões máquina-a-máquina (M2M) leva a aumentos anuais de cerca de 0,7% no PIB e um aumento de 0,9% no Valor Agregado Bruto (GVA, da sigla em inglês) da indústria. O estudo é baseado em dados da OCDE e abrange uma amostra de seus países membros, incluindo México e Chile. Ainda, a A.T. Kearney prevê que a IoT levará a um aumento de produtividade global de US\$ 1,9 trilhão e a US\$ 177 bilhões em redução de custos até 2020. É importante ressaltar que a IoT terá um impacto importante tanto nas indústrias quanto nos consumidores, o qual, por sua vez, terá o maior crescimento esperado na região, particularmente em aplicações de casas inteligentes (veja a figura 2 abaixo).

Aqui estão algumas das questões que os formuladores de políticas devem começar a fazer agora para definir o caminho certo para liberar o potencial da IoT :

- Qual é o impacto estimado que a IoT pode trazer em meu país ou município em 5 anos?
- Quais são as áreas que mais podem se beneficiar da IoT (por exemplo, agricultura sustentável, manufatura, sistemas de distribuição de água, veículos inteligentes, saúde, etc.)?
- Como os formuladores de políticas (ministérios, agências reguladoras, congressos, governos locais) podem ajudar a criar um ecossistema de IoT sustentável que estimule a inovação e as startups locais?
- O que pode ser feito para garantir a continuidade de projetos de cidades inteligentes em diferentes administrações?
- Como as pequenas e médias empresas (PMEs) podem se beneficiar de um ecossistema de IoT sustentável?

2. https://www.frontier-economics.com/media/1167/201803_the-economic-impact-of-iot_frontier.pdf

3. Consulte o Anexo 1 para uma lista de verificação de considerações e ações para construir uma estratégia de IoT.

2. CONSIDERAÇÕES NA ELABORAÇÃO DE POLÍTICAS PARA A IOT

A Internet das Coisas descreve a coordenação de múltiplas máquinas, dispositivos e aparelhos conectados à Internet através de diversas redes. Esses dispositivos incluem objetos do cotidiano, como tablets e eletrônicos de consumo, e outras máquinas, como veículos, monitores e sensores equipados com comunicações máquina-a-máquina (M2M) que permitem enviar e receber dados.⁴ Na prática, então, a IoT não se trata apenas de adicionar conectividade às “coisas”, mas de usar essas coisas para capturar e processar dados, apoiando, assim, a tomada de decisões em tempo real e fornecendo insights através de Big Data e Analytics. Isso cria implicações importantes em termos de modelos de negócio, concorrência, tecnologia e formulação de políticas.

2.1 MODELOS DE NEGÓCIOS E CONCORRÊNCIA NA IOT

O ecossistema da IoT é competitivo e diversificado: players industriais, fabricantes de veículos, empresas de tecnologia, operadoras de telecomunicações e novos participantes e startups competem em um ou mais segmentos da cadeia de valor.

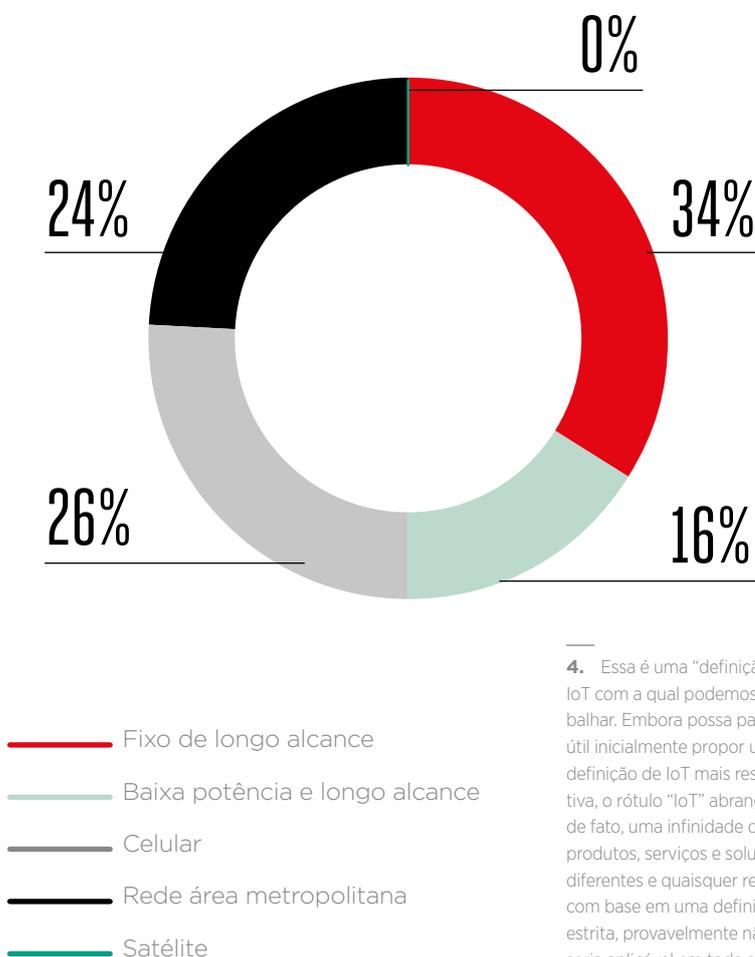
Existem algumas diferenças óbvias entre os serviços tradicionais de voz e dados e os serviços IoT, como o número de elementos conectados - que provavelmente é substancialmente mais alto no caso de dispositivos IoT - e a ênfase do serviço - que não é centralizado em pacotes de voz e dados no caso da IoT.

No mercado de conectividade em IoT, existe e continuará existindo uma competição muito saudável e dinâmica por infraestrutura (veja a figura 3 abaixo). A escolha do modelo de conectividade será impulsionada pelas características intrínsecas do dispositivo, sua mobilidade, sua localização, seus requisitos de largura de banda e sua complexidade.

Da estimativa de 1,2 bilhão de dispositivos conectados estimados na América Latina até 2023, apenas 306 milhões serão de longo alcance. Desses, estima-se que 79 milhões serão redes móveis tradicionais, 48 milhões de redes de longo alcance e baixa potência (em frequências licenciadas e não licenciadas), 73,5 milhões serão redes de área metropolitana, 100 milhões, conexões fixas, enquanto apenas pouco mais de 1 milhão serão via satélite.

Figura 3: Conexões de longo alcance na América Latina por tecnologia de conectividade em 2023.

Fonte: Elaboração própria sobre dados Machina/Gartner (2018).



4. Essa é uma “definição” de IoT com a qual podemos trabalhar. Embora possa parecer útil inicialmente propor uma definição de IoT mais restritiva, o rótulo “IoT” abrange, de fato, uma infinidade de produtos, serviços e soluções diferentes e quaisquer regras, com base em uma definição estrita, provavelmente não seria aplicável em toda a linha.

FIGURA 4: DIFERENÇAS EM MODELOS DE NEGÓCIO ENTRE SERVIÇOS TRADICIONAIS DE TELECOMUNICAÇÕES E IOT



A conectividade permite transferências de dados e é um elemento fundamental de um serviço IoT, mas é apenas um componente do produto final. O valor gerado pelos serviços IoT está essencialmente e intrinsecamente relacionado aos dados que os sensores registram e às análises deles derivados. Isso poderia ser, por exemplo: dados gerados por sensores para permitir ciclos de manutenção mais eficientes e análises preditivas em IoT industrial; dados sobre umidade do solo, combinados com informações sobre o clima, para possibilitar melhor irrigação em agricultura inteligente; dados sobre disponibilidade e localização de veículos em relação a usuários em potencial, no caso de compartilhamento de carros, para permitir um modelo de negócios inovador de “compartilhamento de produtos”.

Além disso, a receita média por usuário (ARPU) é muito menor em conexões IoT, já que muitos dispositivos IoT enviam e recebem apenas pequenas quantidades de dados. Um medidor inteligente, por exemplo, pode vir a compartilhar apenas alguns kilobytes a cada semana, ou mês, com a plataforma back-end. Isso significa que, quando se olha apenas para a receita das redes de comunicação, a IoT costuma gerar menos tráfego e receitas significativas por dispositivo, chegando a US\$ 2 por mês, e até menos em alguns casos.

Outra diferença fundamental é como o ecossistema é construído (veja a figura 4 abaixo). Enquanto a maioria dos provedores de comunicação vendem diretamente para seus próprios clientes planos tradicionais de voz e dados, no caso da IoT, a cadeia de relacionamentos pode ser muito mais complexa, começando com a venda dos fornecedores aos provedores de serviços, que por sua vez vendem para o cliente final (seja consumidor ou outra empresa).

As muitas particularidades da IoT exploradas acima resultam em uma

variedade de modelos de negócios que podem ser desenvolvidos, tais como:

- Cobrança de taxas iniciais e contínuas, semelhantes a modelos mais tradicionais, em que as taxas iniciais refletem o custo do dispositivo e as taxas em andamento destinam-se a cobrir as taxas de serviço;
- Cobrança de taxas contínuas, de modo que nenhuma taxa inicial é cobrada e os custos são baseados em uso;
- Cobrança somente de taxa inicial, que consiste em um custo inicial de instalação que também cobre taxas de serviço;
- Economia de compartilhamento, em que uma solução de IoT é projetada para reduzir custos e uma parcela do valor economizado é paga ao provedor de serviços.

2.2 BARREIRAS NA POLÍTICA E REGULAÇÃO EXISTENTES PARA A IOT

Outro desafio importante na formulação de políticas para IoT é a superação das barreiras na política e regulação existentes, que afetam a IoT de maneira direta ou indireta, e levam a distorções no mercado e a danos à concorrência e à inovação. Embora discutir em profundidade essas barreiras não esteja dentro do escopo deste documento, vale a pena destacar dois aspectos importantes: o legado regulatório sobre a conectividade, e a tributação.

Um dos requisitos essenciais para a IoT é a conectividade, que está intrinsecamente relacionada à infraestrutura de telecomunicações do país. A regulamentação pesada do setor de telecomunicações poderia efetivamente impedir o desenvolvimento da IoT, e uma

revisão profunda das leis e regulamentações que regem o setor é necessária, incluindo questões como espectro, recursos de numeração, certificação de dispositivos e outras regras específicas do setor de telecomunicações.⁵ Em última instância, a regulamentação deve permitir que os serviços de IoT e sua implantação sejam relevantes, rápidos e inovadores.

Além disso, os impostos e taxas aplicados à maioria dos serviços (inclusive à conectividade) foram criados considerando a economia dos serviços tradicionais e muitas vezes não se aplicam à IoT - de fato, a cobrança de impostos altos pode impedir efetivamente sua massificação e a adoção de soluções IoT para governos, empresas e consumidores. Devido à receita média muito baixa por usuário (ARPU), os impostos e taxas, no que diz respeito à sua aplicação às soluções IoT, devem ser redesenhados para minimizar o impacto no preço, de modo a não tornar muitos serviços economicamente inviáveis. Para essa finalidade, formuladores de política podem considerar opções como reduções tributárias ou feriados regulatórios.

5. Para uma revisão das melhores práticas sobre a regulamentação da IoT, consulte a base de conhecimento da GSMA: <https://www.gsma.com/iot/iot-knowledgebase>

3. O NÍVEL NACIONAL: RECOMENDAÇÕES PARA GOVERNOS NACIONAIS

Depois de compreender algumas características-chave da IoT que afetam a formulação de políticas, é fácil entender por que a IoT pode ser um desafio para os tomadores de decisão no Congresso, no governo central e nos reguladores nacionais. Diversos governos ao redor do mundo já tomaram medidas para apoiar o crescimento da IoT. Os governos da América Latina podem assumir o importante papel de construir o ecossistema e ser um grande impulsionador da demanda. Para esse fim, os formuladores de políticas devem considerar cuidadosamente as três recomendações abaixo.

3.1 DEFINIR UMA ESTRATÉGIA DE LONGO PRAZO

Embora as diferenças entre modelos de governança de um país para outro possam ser atribuídas ao contexto doméstico, o papel do governo na IoT deve ser o mesmo em todos os países: estimular a construção de um ecossistema de IoT forte. Isso, por sua vez, significa adotar ações para incentivar a inovação e reduzir o risco de investir e inovar, incluindo, mas não limitado a: investimentos diretos, incentivos fiscais, contratos governamentais, apoio à formação de clusters e aceleradores, criação de programas de apoio ao desenvolvimento e à adoção da IoT por pequenas e médias empresas (PMEs).

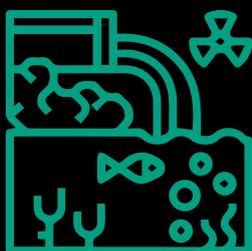
Para melhor entender exatamente quais ações tomar e como avaliar sua relevância,

FIGURA 5: UM PLANO DE POLÍTICA DE IOT EM TRÊS ETAPAS



Caso do Brasil: planejando uma política de IoT

Em um processo iniciado em 2014 com a criação da então chamada Câmara M2M (atualmente Câmara IoT), o governo brasileiro criou um fórum permanente para discutir regularmente com o setor privado, e também com outras partes interessadas do governo, os principais desafios e prioridades para tornar possível o crescimento da IoT no país. Isso destaca a importância de envolver o setor privado desde o início, para ter uma melhor compreensão do risco e das oportunidades, bem como para facilitar o consenso.



IoT e SDGs

A IoT pode apoiar a concretização dos Objetivos de Desenvolvimento Sustentável (ODS) das Nações Unidas até 2030. Alguns projetos de IoT para apoiar essa meta incluiriam a redução do desperdício de água e eletricidade, o monitoramento de espécies ameaçadas e a mitigação das mudanças climáticas.



AGRICULTURA INTELIGENTE: MELHORANDO A PRODUTIVIDADE AGRÍCOLA

Segundo o Banco Mundial, o mundo precisará alimentar 9,7 bilhões de pessoas até 2050, o que significa um aumento na produção de alimentos de 50%. Uma maneira de aumentar a disponibilidade de alimentos é reduzir o seu desperdício. A Organização das Nações Unidas para Agricultura e Alimentação (FAO) estima que cerca de um terço dos alimentos produzidos no mundo para consumo humano a cada ano - aproximadamente 1,3 bilhão de toneladas - seja perdido ou desperdiçado. Nos países em desenvolvimento, 40% das perdas ocorrem nos níveis pós-colheita e processamento. Segundo a IBM, 90% de todas as perdas de safra são relacionadas ao clima, e a previsão de tempo através da aplicação de sistemas de agricultura de precisão, como os habilitados pela IoT, pode reduzir esse dano em cerca de 25%. Soluções relativamente simples podem ajudar a reduzir o desperdício e gerar valor para o agricultor.

Em 2018, a Telefonica assinou um acordo com a FAO para colaborar no desenvolvimento da inovação, digitalização e análise de dados no setor agrícola para promover o desenvolvimento da agricultura, segurança alimentar e nutrição, com projetos piloto sendo desenvolvidos em El Salvador e na Colômbia. Nos mercados em desenvolvimento, o agronegócio pode obter enormes benefícios da visibilidade total e em tempo real ao longo da cadeia de valor. Em Córdoba, Argentina, a Claro construiu uma parceria para desenvolver uma solução de IoT para um exportador agrícola que conecta máquinas e animais de fazenda a sensores, e analisa imagens de drones e de satélite. Os dados gerados, conseqüentemente, podem ser analisados por meio de um painel online com relatórios, gráficos e análises preditivas. Isso dá rastreabilidade aos produtos e ajuda o produtor a atender aos altos padrões de seus clientes internacionais.

os governos da América Latina devem primeiro passar por um processo de planejamento que consiste em três etapas: definição de escopo, priorização e implementação (veja a Figura 5 abaixo).

Na fase de definição do escopo, os governos devem procurar compreender as aspirações nacionais em relação à IoT, como o que o país deseja e pode alcançar realisticamente dentro de um prazo definido. É importante envolver o maior número possível de interessados nesta etapa por meio de consultas públicas abertas e criação e participação em fóruns e eventos relevantes. O Brasil, por exemplo, teve uma abordagem bem-sucedida ao criar o locus para a troca de opiniões com o setor privado, bem como com o ecossistema mais amplo (incluindo representantes de universidades e da sociedade civil). Nesse estágio, também é útil discutir os principais valores e objetivos estratégicos de longo prazo que deverão guiar as ações do governo, como crescimento econômico, melhoria da produtividade, melhoria e ampliação do acesso a serviços públicos, melhoria da resposta a desastres naturais, como inundações ou desmatamentos.

Na fase de priorização, os governos devem identificar quais verticais (por exemplo, agricultura, transporte, automotiva ou energia) podem produzir os maiores benefícios para o país quando um ecossistema completo de IoT é viabilizado. A quantificação de benefícios econômicos efetivos para o país deve observar melhores práticas do setor, e deve abrir caminho para a formulação de políticas baseadas evidências concretas. Por outro lado, a identificação de setores prioritários não deve significar a elevação de barreiras para outras indústrias, pois isso pode desacelerar a inovação e afetar os benefícios gerais que podem ser trazidos pela IoT.

Os resultados propostos na fase de

priorização devem ser submetidos a consulta pública, e receber insumos da indústria e do amplo ecossistema de IoT é essencial nessa fase. Como resultado desse processo, o governo deve apresentar uma política e uma estratégia preliminar para IoT que definam ações e cronogramas específicos e métricas de sucesso apropriadas (por exemplo, maior cobertura de serviços específicos, porcentagens de redução de custos, redução de CO2, vidas salvas etc.). No entanto, os governos devem resistir à tentação de “escolher pelo mercado” soluções tecnológicas específicas para implementar serviços de IoT, pois estas podem se tornar obsoletos muito rapidamente ou artificialmente vincular uma solução a um país ou provedor específico. É importante deixar o mercado e os usuários finais escolherem.

Durante a fase de implementação, as ações previamente acordadas devem ser monitoradas para aferir as metas. Tanto a nível central como local, é importante assegurar a existência de vias legais flexíveis para permitir aos gestores a flexibilidade e a independência necessárias para inovar. Isso pode ser alcançado por meio da criação de um departamento específico

para IoT, alocando orçamento dedicado, e criando estruturas de incentivo para o setor privado promover o investimento eficiente dos recursos dos contribuintes.

Finalmente, todas as agências governamentais relevantes devem reconhecer o aspecto inter-setorial do departamento de IoT e a evolução tecnológica extremamente dinâmica dessas soluções, ou correr o risco de definir políticas baseadas em silos, não conseguindo capturar sinergias com outros setores, aumentando o custo para os contribuintes e, finalmente, não conseguindo entregar resultados. Todas as agências relevantes (ministérios, secretarias e órgãos reguladores) devem, portanto, estar coordenados quanto a estratégias de longo prazo e objetivos, e trabalhar em conjunto para definir políticas, de modo a evitar duplicação de esforços.

3.2 PROMOVER A DEMANDA POR MEIO DE COMPRAS GOVERNAMENTAIS

A IoT pode ter um impacto positivo na redução do custo e no aumento da agilidade dos serviços do governo. Além disso, a IoT pode de fato ter um papel fundamental na superação dos desafios de infraestrutura do século 20 na América



IoT em uma agenda digital abrangente

Ao reconhecer a importância do ecossistema digital e a convergência digital, a liderança governamental na América Latina deve ter como objetivo construir uma agenda digital abrangente para apoiar a inclusão digital, uma estrutura regulatória harmonizada, novos investimentos, implantação de infraestrutura e digitalização de sua produção. Políticas voltadas para o futuro nesse sentido incluem a IoT como um de seus principais componentes. Em geral, as agendas digitais, incluindo a IoT, devem estar na plataforma de qualquer candidato político concorrendo a uma função pública importante na América Latina.

Latina, em temas como *smart utilities*, construção e manutenção de estradas e rodovias, alocação de recursos de segurança em centros urbanos superlotados, etc.

Como parte de uma estratégia de IoT bem-sucedida, os governos da América Latina podem desempenhar um papel fundamental na promoção da demanda por IoT e, portanto, estimular a criação de um ecossistema de IoT forte. Portanto, os governos precisam identificar áreas-chave com deficiências significativas (como segurança pública, mobilidade urbana ou assistência médica) e priorizar as soluções de IoT para ajudar a superar as barreiras existentes. Essas soluções podem ser usadas para otimizar os processos existentes ou para criar soluções inovadoras e econômicas.

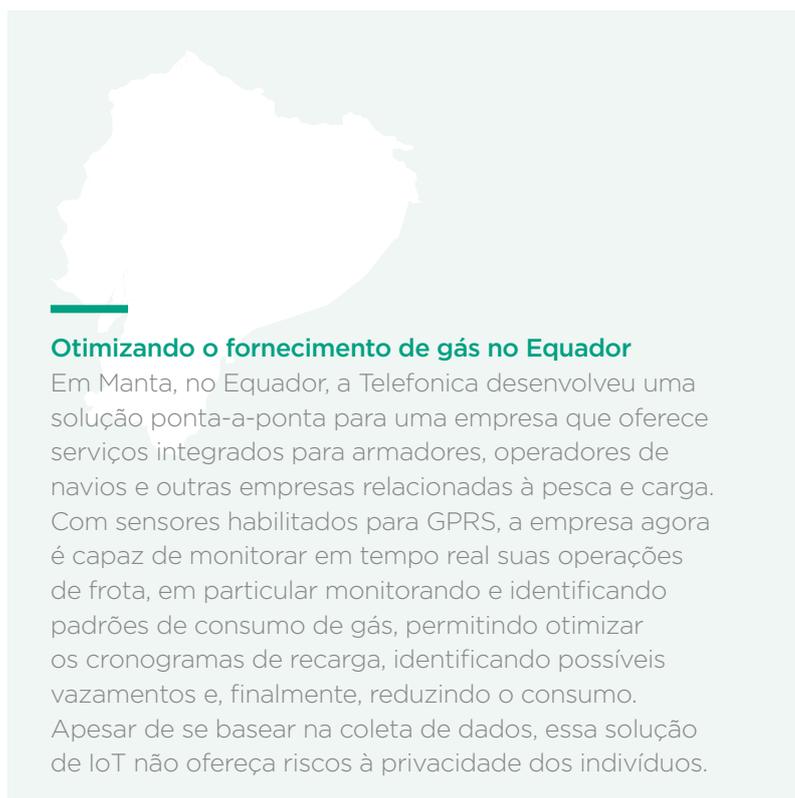
As regras para compras governamentais, por exemplo, podem priorizar as soluções de IoT, contanto que sejam econômicas e/ou possam oferecer mais benefícios do que as soluções tradicionais. Conforme explicado na seção 2.1, a IoT permite distintos modelos de negócios, incluindo o “compartilhamento de economia” (*savings-sharing*), o que pode ser uma forma de os governos concederem contratos de longo prazo sem incorrer em quaisquer novos custos. Isso pode ser, de fato, uma oportunidade para os governos não gastarem mais em qualquer área crítica, e ainda poderem reduzir custos e ter um maior retorno do investimento. Além disso, ao elaborar regras para compras governamentais, formuladores de políticas devem procurar evitar o “lock-in” de fornecedores e o risco de não interoperabilidade; para conseguir isso, os governos só devem adotar soluções com escalabilidade, preparadas para o futuro e tecnologicamente neutras.

3.3 ABORDAR PRIVACIDADE E SEGURANÇA

Uma das principais questões relacionadas

à IoT, que muitas vezes exige uma ação positiva dos formuladores de políticas, é a da privacidade. Embora os dados sejam de natureza global, a regulamentação da proteção de dados e da privacidade ainda permanece uma colcha de retalhos de disposições e requisitos não interoperáveis. Atualmente, existem mais de 100 leis nacionais e regionais de proteção de dados e, às vezes, mesmo dentro de um único país, a proteção de dados é regulada por vários instrumentos e regulamentações diferentes.

Formuladores de políticas da América Latina devem considerar o desenvolvimento de uma marco regulatório geral de privacidade e proteção de dados ou, se já tiverem uma, deveriam assegurar que ela seja compatível com a IoT, bem como com o ecossistema digital convergente e com a economia baseada em dados. Isso inclui revisar obrigações criteriosas sobre hipóteses para o processamento de



dados (como o consentimento explícito versus implícito) e para a transferência internacional de dados. Sempre que possível, os decisores na área da privacidade e proteção de dados devem procurar harmonizar as regras, particularmente no que respeita aos fluxos de dados transfronteiriços, para permitir a inovação, garantindo, ao mesmo tempo, um nível consistente de proteção para os usuários.

É importante observar, no entanto, que não há necessidade de um regulamento de privacidade de dados específico da IoT. Embora muitas soluções de IoT, como aquelas para uso agrícola e industrial, não coletem dados pessoais e não representem ameaça à privacidade dos usuários, onde a IoT coletará dados pessoais ou de identificação pessoal, os consumidores serão protegidos de forma mais consistente com um marco regulatório horizontal, especialmente se este for harmonizado com as melhores práticas internacionais em privacidade e outros marcos nacionais e regionais.

No que diz respeito à segurança e à IoT, é importante que os governos apoiem as melhores práticas e padrões liderados pela indústria. Como a IoT é uma indústria nascente, a criação de novos padrões de segurança, principalmente se forem padrões nacionais e não globais, poderia prejudicar a inovação e, em muitos casos, não fornecer o resultado desejado (ou seja, um dispositivo, serviço ou aplicativo IoT mais seguro). À medida que as ameaças evoluem, o mesmo acontece com as melhores práticas e padrões liderados pelo setor, que são mais rápidos e mais econômicos de se adaptar que rígidos padrões nacionais. Isso garante a flexibilidade necessária para que o ecossistema da IoT se adapte a novas ameaças e cenários. O papel do governo neste caso pode ser, por exemplo, promover programas de certificação voluntária.

DIRETRIZES DE SEGURANÇA DA GSMA PARA APLICATIVOS DE CIDADES INTELIGENTES

Os aplicativos de cidade inteligente baseados em IoT levantam os mesmos tipos de problemas de segurança cibernética que os atribuídos a serviços existentes de Internet, como proteger a disponibilidade, identidade, privacidade e integridade dos componentes de serviço. Um dos desafios únicos dos serviços IoT é como garantir essas propriedades em dispositivos que, na maioria das vezes, são de baixa complexidade, baixo consumo de energia, possuem longos ciclos de vida e são fisicamente acessíveis para ataques. Pode-se imaginar um parquímetro inteligente e conectado em uma cidade inteligente que precisa ser desenvolvido a baixo custo, tem que ser alimentado por uma fonte de energia solar, deve permanecer seguro por dez anos, e deve ser implantado em uma via pública acessível 24 horas por dia. É fácil ver que os desafios para a implementação segura de tal produto não são triviais e que muitos desafios relacionados à segurança física e cibernética precisarão ser resolvidos. O setor de telecomunicações móveis tem um longo histórico de fornecimento de produtos e serviços seguros para seus clientes. Para ajudar a garantir que novos serviços de IoT (incluindo serviços de cidades inteligentes) que estão chegando ao mercado sejam seguros, as operadoras de rede, juntamente com seus parceiros de rede, serviços e equipamentos, produziram um conjunto de diretrizes de segurança para compartilhar seus conhecimentos de segurança com os provedores de serviços. Os documentos de diretrizes da GSMA promovem uma metodologia para o desenvolvimento de serviços seguros de IoT para garantir que as práticas recomendadas de segurança sejam implementadas durante todo o ciclo de vida do serviço. Os documentos fornecem recomendações sobre como atenuar ameaças e pontos fracos comuns de segurança nos serviços de IoT.

Fonte: Diretrizes de Segurança GSMA (<http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines>)

4. O NÍVEL LOCAL: FAZENDO CIDADES INTELIGENTES

Na América Latina, a região mais urbanizada do mundo, com mais de 80% dos cidadãos vivendo em áreas urbanas, as cidades têm um papel importante a desempenhar no ecossistema da IoT. Devido ao seu tamanho, à distribuição geográfica, à dinâmica empreendedora e até mesmo aos desafios de infraestrutura, as cidades da região podem promover ativamente a implantação da IoT e aproveitar os benefícios trazidos por ela. As aplicações de IoT e cidade inteligente podem efetivamente preparar o caminho para as cidades latinoamericanas superarem os desafios do final do século 20 e se tornarem líderes do século 21, gerando benefícios socioeconômicos substanciais para cidadãos e empresas. Formuladores de políticas devem aproveitar ao máximo essa oportunidade, projetando e implementando projetos de cidade inteligente com uma estrutura de governança ágil baseada em sistemas abertos e escalonáveis, em uma visão longo prazo pensada em torno das necessidades dos cidadãos, e em uma cultura de abertura, inovação e transparência. Antes de estabelecer uma agenda para uma cidade inteligente, formuladores de políticas no nível municipal devem considerar as seguintes recomendações.

4.1 PROMOVER A COORDENAÇÃO E CRIAR UM MODELO DE GOVERNANÇA FLEXÍVEL COM UM LÍDER INDEPENDENTE

Para construir um projeto eficaz de cidade inteligente, a cidade deve começar por: (i) nomear um diretor de serviços, como um Diretor de Informações (CIO), com poderes

para desenvolver e executar uma visão estratégica construída para atender às necessidades dos cidadãos; (ii) adotar um quadro institucional ágil e mecanismos de governança apropriados; (iii) reconhecendo que em nível municipal não é necessário “reinventar a roda” sobre questões mais amplas, como segurança e padrões – ao contrário, é importante seguir as diretrizes já contidas em marcos nacionais e/ou regionais.

Definir o arcabouço correto e a governança dos projetos para garantir flexibilidade e prestação de contas é um passo inicial importante.

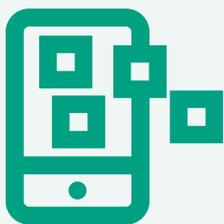
A maioria dos projetos de cidades inteligentes exige cooperação e troca de informações entre equipes que antes não trabalhavam juntas, como secretarias encarregadas de iluminação pública e gestão de resíduos, que deveriam adotar tecnologias semelhantes. A cooperação é, portanto, fundamental, seja entre secretarias municipais, empresas locais e cidadãos. Isso é particularmente aplicável quando sensores de IoT e Big Data são usados para criar um painel de controle dos vários serviços oferecidos pela cidade; isso, por sua vez, pode ser usado para identificar problemas críticos de infraestrutura e possíveis gargalos, o que ajudará a diagnosticar os principais problemas em tempo real, como eventos de segurança, desastres naturais e epidemias.

O líder do projeto, normalmente chamado de CIO, deverá ter a autoridade relevante para dirigir e supervisionar projetos de cidades inteligentes em toda a estrutura



BARCELONA: UM COORDENADOR DE CIDADE INTELIGENTE

Uma das cidades inteligentes mais avançadas da Europa, Barcelona tem um coordenador de cidade inteligente há muitos anos. Seus objetivos são supervisionar iniciativas de cidades inteligentes e coordená-las entre departamentos e, mais importante, definir uma visão estratégica de longo prazo para a cidade.



SINGAPURA: CIO E GOVTECH

Uma das cidades inteligentes mais avançadas do mundo, Singapura atribuiu a seu CIO a responsabilidade pela agência GovTech, formada para supervisionar a inovação para a estratégia Smart Nation. O CIO está liderando vários projetos avançados de cidades inteligentes, incluindo o Virtual Singapore e o Beeline, um aplicativo para cidadãos sem acesso fácil a serviços públicos, que faz buscas de rotas de ônibus.

municipal para evitar a fragmentação ou a duplicação de esforços. Para agir com eficiência, ele deverá ter o nível apropriado de independência e ser direcionado para objetivos estratégicos, como recursos ou economia de energia.

Um CIO deverá produzir e implementar uma estratégia capaz de unir os órgãos competentes de uma cidade, superando a falta de cooperação, o receio de trocar dados, o financiamento insuficiente e, finalmente, a resistência cultural nas secretarias do município. Em vez de se concentrar na tecnologia ou na solução em particular, o CIO precisa entender as necessidades dos cidadãos, entender as várias opções e estratégias de longo prazo, e ser capaz de comunicar efetivamente os benefícios de cada abordagem.

4.2 DESENVOLVER PARCERIAS E BUSCAR DIVERSAS OPÇÕES DE FINANCIAMENTO E INVESTIMENTO

Uma das barreiras mais reconhecidas para implementações de cidades inteligentes na América Latina é a falta de recursos dentro do governo local. A percepção de uma administração local limitada por recursos levou, compreensivelmente, muitos decisores municipais a fecharem a porta para projetos potencialmente inovadores em suas respectivas jurisdições.

No entanto, conforme explicado na seção 2.1, um dos aspectos inovadores da IoT é sua diversidade de modelos de negócios. Quando comparadas a muitas ofertas tradicionais de serviços públicos, as soluções de IoT podem oferecer novas oportunidades para os governos locais com um modelo de negócios baseado em compartilhamento de economia (savings-sharing), por exemplo, que não teria custos iniciais para o governo local.

Depois de realizar uma análise de custo-benefício sobre as alternativas inteligentes para fornecer serviços públicos tradicionais (de concessionárias a gerenciamento de tráfego), os governos locais devem buscar parcerias com o ecossistema da IoT para implantar soluções custo-eficientes, tecnologicamente neutras e escalonáveis. Além das compras governamentais diretas, as autoridades locais podem procurar desenvolver modelos diferentes de parcerias público-privadas (PPPs). Ao autorizar o

ILUMINAÇÃO INTELIGENTE NO BRASIL E NA COLÔMBIA

Caraguatuba é uma cidade litorânea do estado de São Paulo com mais de 110 mil habitantes. Em 2017, tornou-se uma das primeiras cidades do Brasil a desenvolver uma PPP para iluminação pública. O projeto tem como meta a troca de 100% das 18.000 lâmpadas de rua por LEDs inteligentes que podem alimentar informações em um painel, e que podem ser monitorados pelo governo local. Os novos postes de luz em Caraguatuba também estão aptos a serem utilizados no futuro para outras aplicações de cidade inteligente. Na Colômbia, a Claro está trabalhando com um município para pilotar um projeto de iluminação inteligente que permitirá que as luzes das ruas diminuam de acordo com a hora do dia, a estação do ano e a presença de pedestres. Elas também poderão enviar alertas de manutenção e antecipar possíveis falhas.

setor privado a assumir a responsabilidade pela prestação de um serviço público, os governos locais podem definir os princípios para a oferta do serviço (como qualidade, interoperabilidade e escalabilidade) e monitorar sua implementação. Isso não apenas reduz os riscos operacionais de o governo implantar essa infraestrutura e serviços, mas também pode ajudar a garantir a eficácia de custo da solução.

4.3 ADOTAR TECNOLOGIAS ABERTAS E ESCALÁVEIS E SISTEMAS À PROVA DO FUTURO

Cidades contêm centenas de sistemas e serviços. Nem todos os serviços precisam se tornar inteligentes, mas os ter conectados por uma infraestrutura comum e tecnologias baseadas em padrões é uma pedra fundamental com base na qual a evolução a longo prazo de uma cidade inteligente pode ser construída. Como a tecnologia implantada precisará durar décadas, ela deve ser custo-eficiente e flexível o suficiente para crescer (escalabilidade) e suportar muitas mudanças e novos serviços no futuro (à prova de futuro).

Quando um serviço de IoT é escalável, isso significa que a solução tecnológica pode ser adotada para serviços adjacentes com relativa facilidade e com custos reduzidos de implantação, de modo a maximizar a economia de escala e escopo que o investimento inicial pode gerar.

As soluções de tecnologia móvel, particularmente as ilustradas no box abaixo, são por definição escaláveis, pois capitalizam uma cobertura existente já fornecida para serviços de voz e dados e, portanto, os custos marginais de adicionar soluções IoT que usam as mesmas redes serão reduzidos.

Para ser à prova de futuro, uma solução IoT deve envolver uma escolha de tecnologia robusta o suficiente para suportar as futuras evoluções e evitar o risco de que a solução se torne obsoleta muito rapidamente, e, dessa forma, aumentando os custos de manutenção e vinculando a administração a um único fornecedor.

As tecnologias Mobile IoT oferecem a vantagem de utilizar uma grande variedade de fornecedores e contar com especificações tecnológicas globais definidas pelos órgãos de padronização do setor, que são atualizadas regularmente para atender a novos casos de uso e são testadas em todo o mundo.

Finalmente, vale a pena notar que muitos componentes de uma solução de cidade inteligente (por exemplo, redes de comunicação, segurança cibernética, ferramentas de análise de dados, etc.) podem ser aplicados e compartilhados em diversos serviços: desde a medição inteligente até o gerenciamento de tráfego e iluminação de rua inteligente. Compartilhar

CIDADES INTELIGENTES E A TECNOLOGIA MÓVEL: REDES MÓVEIS PARA IOT



As operadoras móveis podem ser parceiras experientes das cidades da América Latina. Elas podem permitir soluções de cidade inteligente seguras, escaláveis e robustas. Além de estarem bem posicionadas para entender a dinâmica dos municípios e as melhores práticas internacionais, as operadoras móveis geralmente têm uma presença comercial no município e administram redes avançadas, seguras e com escalabilidade.

A conectividade móvel IoT pode ativar aplicativos do tipo on/off simples, como controles de lâmpadas de rua,

monitoramento da qualidade do ar, sensores de estacionamento e atualizações básicas de status para muitos tipos de sensores, incluindo aqueles alimentados por bateria e localizados em lugares inacessíveis, por anos. As principais vantagens das tecnologias Mobile IoT são o consumo de energia muito baixo (com duração da bateria superior a 10 anos para algumas aplicações), custos muito baixos de módulos, boa cobertura outdoor e indoor, além dos benefícios típicos das redes móveis: fácil escalabilidade, alto nível de segurança, fácil manutenção e integração em plataformas unificadas de IoT.

componentes dessa maneira é capaz de reduzir os custos de configuração e manutenção.

4.4 DADOS ABERTOS: DISPONIBILIZAR DADOS DA CIDADE SELECIONADOS PARA TERCEIROS POR MEIO DE PORTAIS PARA PROMOVER A TRANSPARÊNCIA E ESTIMULAR A INOVAÇÃO

Cidades geram uma abundância de conjuntos de dados que abrangem transporte, meio ambiente, saúde, demografia, acessibilidade e outras áreas. Seja usado por formuladores de políticas, pesquisadores, mídia, empresários, planejadores de eventos urbanos ou desenvolvedores de aplicativos, os dados das cidades são um ativo cada vez mais valioso que os gestores da cidade devem aproveitar. Ao mesmo tempo em que é importante proteger a privacidade e manter a confiança da sociedade, funcionários municipais devem tornar acessíveis esses dados valiosos para que possam ser facilmente usados por cidadãos e entidades comerciais para criar serviços inovadores.

Além de fornecer acesso único às informações de uma cidade, o compartilhamento de dados ajuda a comunicação e a análise, a elaboração de políticas mais transparentes e eficientes e, o mais importante, cria valor ao catalisar o desenvolvimento de aplicativos e serviços inovadores. Essa prática, que já é adotada por muitas cidades em todo o mundo, pode ajudar a viabilizar um ecossistema vibrante de big data na cidade.



DADOS ABERTOS EM CIDADES INTELIGENTES

Londres: A Greater London Authority disponibiliza 705 conjuntos de dados em seu data store em Londres.

Copenhague: A cidade oferece um serviço para a venda, compra e compartilhamento de uma ampla variedade de dados de várias fontes entre todos os tipos de usuários em uma cidade - cidadãos, prefeitura e empresas.

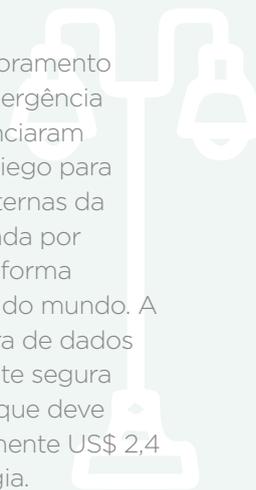
Singapura: Uma iniciativa do governo central, 'Data.gov.sg.', foi lançada em 2011 como um portal consolidado para disponibilizar publicamente conjuntos de dados de 70 agências governamentais. Mais de 100 aplicativos foram criados usando esses dados.

Melbourne: A cidade de Melbourne construiu um portal para disponibilizar dados em uma base não comercial. Melbourne está disponibilizando um catálogo crescente de conjuntos de dados agrupados em ativos e por categoria, como infraestrutura, economia e meio ambiente.

UMA PLATAFORMA, MUITOS SERVIÇOS

A aplicação de iluminação inteligente tem o potencial de ir além da economia de energia. Postes também podem ser usados como plataforma para outros serviços. Desde o lançamento de sua organização Smart Cities em 2015, a AT&T tem usado seus recursos e expertise em IoT para criar soluções impactantes para as cidades. Com a introdução da plataforma IoT da GE Predix, a AT&T pode usar iluminação LED externa em uma cidade para criar uma infraestrutura digital que ajude a resolver problemas como fluxo de tráfego e otimização de estacionamento, detecção de

tiroteios nas ruas da cidade, monitoramento da qualidade do ar e alertas de emergência climática. Recentemente, eles anunciaram um acordo com a cidade de San Diego para atualizar milhares de luminárias externas da cidade para a tecnologia LED ativada por sensores, tornando-a a maior plataforma inteligentes de Internet das Coisas do mundo. A AT&T atuará como a transportadora de dados e fornecerá conectividade altamente segura para a implantação de San Diego, que deve economizar à cidade aproximadamente US\$ 2,4 milhões em custos anuais de energia.



Anexo 1

Lista de verificação de ações para os criadores de políticas de IoT

TÓPICO	QUESTÕES	SIM	NÃO
1. Realize o exercício de escopo	1.1 Existem metas claras e objetivas (por exemplo, melhorar a produtividade, reduzir o congestionamento, reduzir a emissão de carbono, reduzir o custo da prestação de serviços públicos, melhorar a segurança no trânsito, entre outros) com a promoção da IoT no país ou município? Esses objetivos são enquadrados como produtos finais (como uma redução percentual no custo de um determinado serviço) sem definir uma solução ou um padrão técnico específico?		
	1.2 As circunstâncias nacionais ou locais (por exemplo, o atual nível de crescimento econômico, o dinamismo econômico, a infraestrutura de conectividade, as barreiras legais e regulatórias, a capacidade de investimento, etc.) são levadas em conta no exercício de definição do escopo? Tem sido usada uma análise de custo-benefício?		
	1.3 Todos os stakeholders relevantes - ministérios e agências reguladoras, bancos de desenvolvimento, operadoras móveis, fabricantes de dispositivos e equipamentos, associações industriais, entre outros - estão envolvidos nessa tarefa?		
2. Priorizar áreas de trabalho⁶	2.1 Os tomadores de decisão consideraram e/ou identificaram os principais setores, áreas, regiões geográficas e/ou serviços onde a aplicação da IoT poderia gerar o máximo de valor? Quais são eles?		
	2.2 Qual é o tamanho desse impacto (que pode ser expresso em moeda local ou como porcentagem do PIB) no curto (até 1 ano), médio (até 5 anos) e longo prazo (5 anos ou mais)?		
3. Considere os marcos de segurança e privacidade⁷	3.1 O país tem uma lei geral de proteção de dados? Em caso afirmativo, os tomadores de decisão avaliaram o impacto dessa estrutura nos serviços de IoT (inclusive no entendimento de até que ponto os dados coletados por um dispositivo ou serviço são dados pessoais)? No caso dos municípios, eles resistiram à tentação de criar regras locais e específicas de proteção ao consumidor?		
	3.2 A estrutura de privacidade baseia-se em princípios internacionalmente reconhecidos e toca em questões como o consentimento explícito (por exemplo, não exigindo um novo consentimento a cada passo do processamento de dados)?		
	3.3 O país tem uma estrutura de segurança cibernética? Em caso afirmativo, é baseado nas melhores práticas? ⁸		
4. Promover demanda	4.1 Existem salvaguardas contra o "lock-in" de fornecedores?		
	4.2 As soluções são baseadas em padrões internacionais e melhores práticas? Alternativamente, os tomadores de decisão evitaram impor tecnologias e padrões definidos nacionalmente?		
	4.3 As soluções são escaláveis e interoperáveis com outras soluções e provedores? Por exemplo, se amanhã os tomadores de decisão desejarem adicionar serviços e/ou cobertura adicionais, isso seria facilmente alcançado a custos relativamente baixos? Da mesma forma, os serviços são capazes de integrar perfeitamente serviços existentes e possíveis serviços futuros?		
5. Buscar (e/ou oferecer) diversas opções de financiamento	5.1 Os tomadores de decisão consideraram diferentes instrumentos para promover o investimento em IoT, como reduções de impostos, empréstimos sem juros, linhas de crédito, medidas específicas para áreas desfavorecidas e parcerias público-privadas?		
	5.2 Os tomadores de decisão buscaram parcerias com bancos de desenvolvimento nacionais, regionais ou internacionais?		
	5.3 Existe um período longo de retorno para linhas de crédito relacionadas à IoT?		
	5.4 Parcerias público-privadas favoráveis ao investimento foram consideradas?		
	5.5 As partes interessadas consideram o uso de modelos de negócios inovadores, como aqueles baseados em economia compartilhada?		
6. Identificar a correta estrutura institucional	6.1 O serviço da IoT foi lançado através de uma iniciativa cujo processo de tomada de decisões é suficientemente independente e flexível em relação aos departamentos tradicionais da administração pública? Em outras palavras, os tomadores de decisão são capazes de reagir em tempo hábil às necessidades do projeto e a possíveis mudanças?		
	6.2 Os tomadores de decisão são capazes de lidar com compras, consultorias externas e orçamento de forma independente?		
	6.3 Os tomadores de decisão são capazes de facilitar a comunicação com outras secretarias, agências, ou representantes governamentais (como, por exemplo, o Ministério das Comunicações que deve coordenar esforços com o Ministério dos Transportes e a autoridade reguladora de trânsito)?		
7. Indique um administrador para atuar como Diretor Executivo de Informações (CIO) com uma visão estratégica	7.1 Está claro para os tomadores de decisão em um município que o foco do administrador e seu plano devem estar nos serviços e nas necessidades dos cidadãos, e NÃO em soluções tecnológicas específicas? Da mesma forma, o executivo entende as necessidades da cidade e dos cidadãos e como elas podem evoluir? O executivo é capaz de entender as opções de tecnologia sem se concentrar na solução técnica?		
	7.1 O administrador tem uma estratégia de longo prazo para implantar os serviços? Ele permanecerá nessa posição por tempo suficiente (pelo menos de 3 a 5 anos) para permitir que uma estratégia de IoT seja totalmente implementada do zero? Além disso, ele é capaz de agir de forma independente, mas ainda permanecendo responsável por objetivos concretos (por exemplo, quantidade de economia de energia em um ano)?		

Anexo 2

Princípios e premissas para quantificar a IoT e seu impacto econômico em um país

Identificar e quantificar corretamente o fenômeno da IoT é o primeiro passo para estabelecer políticas bem definidas, baseadas em evidências, e com foco nos objetivos corretos. No entanto, a definição de IoT e de seu impacto econômico ainda estão em fase de evolução. Portanto, a GSMA entende que é necessário tentar homologar e padronizar essas definições

internacionalmente para que os institutos nacionais de estatística possam fazer comparações significativas e quantificar o impacto da IoT em seus países. Algumas sugestões, na forma de princípios e premissas, são oferecidas abaixo para apoiar as análises e estudos sobre o impacto econômico da IoT em um país ou setor econômico.

CONEXÕES

ITEM	RECOMENDAÇÃO
Definição da IoT	Definir o que é um dispositivo IoT pode ser uma tarefa complexa. Trata-se de uma indústria relativamente nova e muitas fontes oferecem definições diferentes. Normalmente, um serviço IoT irá combinar quatro elementos principais: (i) Rede / Conectividade, (ii) Dados, (iii) Sensores e (iv) Dispositivo. A conectividade de rede é o ativador fundamental de um dispositivo IoT e geralmente é fornecida pela Internet ou pelo menos por protocolo IP, mas redes fechadas também podem ser usadas. A conectividade geralmente não é usada para fornecer acesso generalizado à Internet ou a serviços de voz tradicionais. Os dados são outro elemento fundamental. Geralmente vêm de várias fontes (por exemplo, um termostato conectado combinando umidade, sensores de movimento, com previsões do tempo), mas também pode ser uma única fonte: um medidor inteligente que mede o consumo de gás. Os sensores podem ser unidirecionais ou atuadores (isto é, comunicação de duas vias), permitindo que o dispositivo reaja a uma condição específica (por exemplo, tanque de recarga quando o nível está baixo). Finalmente, o elemento "dispositivo" é onde os sensores são incorporados. Isto pode ser realizado através da adaptação de uma "velha" solução já disponível no mercado (por exemplo, um carro ou um trator) ou concebendo inteiramente um novo dispositivo (por exemplo, um leitor de glicose inteligente), cuja funcionalidade é possibilitada pela conectividade inovadora. Para estatísticas e previsões, a inteligência da GSMA define a IoT como: <i>"Dispositivos capazes de transmissão de dados bidirecional (excluindo sensores passivos e tags RFID). Inclui conexões usando vários métodos de comunicação, como celular, curto alcance e outros. Exclui PCs, laptops, tablets, e-readers, terminais de dados e smartphones."</i>
Serviços IoT versus outros serviços	A definição acima distingue, de forma importante, a IoT e outras conexões tradicionais de voz e dados, excluindo tablets, smartphones e similares. Uma orientação geral pode ser identificar o uso principal do serviço/dispositivo. Um serviço IoT deve ser caracterizado por um uso que não seja principalmente comunicação por voz e acesso generalizado à Internet. Isso não significa que o serviço IoT não possa ter tais funcionalidades, apenas que raramente são o foco do serviço (por exemplo, um serviço de chamadas de emergência no carro estabelecerá uma conexão automática de voz com serviços de emergência em caso de acidente, mas não para ser usado para fazer chamadas regularmente).
Dispositivos IoT vs. sensores vs. conexões	O mesmo objeto ou dispositivo pode ter múltiplos serviços, baseados em sensores independentes, que por sua vez possuem suas próprias conexões. Por exemplo, um carro (dispositivo conectado) pode ter vários sensores que utilizam redes de longa distância e/ou múltiplos SIMs. Comparar números de analistas diferentes pode ser confuso dependendo do que eles medem: um carro, muitos sensores embutidos conectados ao mundo externo, o tipo de conectividade que eles usam. Não há certo ou errado aqui, mas é importante ser consistente, particularmente quando comparamos dados de diferentes fontes e países. Dando ênfase ao mercado de conectividade, a GSMA Intelligence mede o número de conexões. (veja a definição acima)
Conectividade local vs. conectividade de longo alcance	Um único dispositivo pode combinar conexões de rede local e de longo alcance. Por exemplo, um dispositivo doméstico inteligente conectará o sistema interno por meio de Wi-Fi, Bluetooth ou ZigBee e também usará uma banda larga fixa ou móvel para conectividade de longa distância. Muitas outras arquiteturas de conectividade são possíveis. Por exemplo, alguns dispositivos usam apenas redes LPWA, satelitais ou fixas. A grande maioria dos dispositivos terá pelo menos um elemento de conectividade de curto alcance e "concentrado" em um gateway. No entanto, é importante distinguir entre áreas de curto e longo alcance e monitorar os mercados de conectividade separadamente e independentemente.



6. Consulte o Anexo 2, que contém os princípios de como medir este impacto econômico.

7. É importante que formuladores de políticas resistam à tentação de criar regras específicas de privacidade e segurança para a IoT; a melhor maneira de abordar a questão é apoiar os padrões internacionais aplicáveis e utilizar regras horizontais que sejam aplicadas de maneira consistente para todos os setores, promovendo, assim, um ecossistema mais confiável e protegido.

8. Consulte as Diretrizes de Segurança IoT da GSMA.

9. Consulte o Anexo 3, que lista os órgãos de padronização existentes para IoT.

Alternativas de longo alcance	As soluções de conectividade apropriadas fazem a diferença para a IoT. Além de redes fixas, satelitais e móveis, é importante considerar a conectividade de longo alcance e baixa potência. Estas podem ser licenciadas (em rede celular: tecnologias como NB-IOT ou LTE-M) ou soluções não licenciadas. Espera-se que as licenças LPWA e não licenciadas sejam as conexões de mais rápido crescimento para IoT.
Consumidor vs. Industrial	É importante agregar as várias verticais da IoT em duas categorias principais - Consumidor versus Industrial -, para facilitar a análise e comparações.
M2M vs conexões IOT	Definições de M2M e IoT são frequentemente usadas como sinônimos. A GSMA define as conexões Machine-to-Machine como: <i>“Um cartão SIM exclusivo registrado na rede móvel (...) que permite a transmissão de dados móveis entre duas ou mais máquinas. Exclui os dispositivos de computação em produtos eletrônicos de consumo, como leitores eletrônicos, smartphones, dongles e tablets.”</i> Comparando a definição com a fornecida acima para IOT, pode-se identificar as principais diferenças sendo: (i) M2M é fornecido na rede celular de longo alcance (ii) M2M é uma conectividade ponto-a-ponto entre as máquinas, enquanto a IoT pode incluir vários sensores conectados por meio de uma conexão de curto alcance. Por exemplo, no carro, vários sensores podem ser conectados em curto alcance (ou com fio) a um só gateway. O módulo de gateways contém um SIM que permite a conectividade celular M2M de longo alcance.

RECEITAS E IMPACTO ECONÔMICO

TÓPICO	RECOMENDAÇÃO
Receita total da IoT versus receita de Conectividade	A IoT é caracterizada por uma longa cadeia de valor e as receitas totais geradas pelo setor de IoT, que incluem o aplicativo, o dispositivo e o serviço propriamente dito, além de serviços como monetização de dados e integração de serviços. A conectividade IoT é um facilitador fundamental, mas provavelmente retém uma parcela relativamente pequena da receita associada ao setor total de IoT. Uma boa estimativa é de 2% a 5%, dependendo da empresa que faz a análise e da agregação de dados. O ponto chave para os formuladores de política é que políticas que viabilizam a IoT têm um alcance muito mais amplo na economia do que apenas a receita de conectividade. É importante que a entidade econômica e de estatística quantifique separadamente as receitas totais da indústria de IoT e as receitas de conectividade da IoT.
Receitas da IoT versus Benefícios socioeconômicos mais amplos	A IoT tem o potencial de produzir significativos benefícios socioeconômicos para a sociedade, como aumentar a produtividade, reduzir o congestionamento do trânsito, reduzir a emissão de carbono, reduzir os gastos da administração pública na provisão de serviços públicos essenciais como assistência médica e reduzir o consumo de energia. Políticas bem definidas e baseadas em evidências estabelecerão objetivos quantificáveis em cada uma dessas dimensões. Portanto, é importante que o departamento de estatísticas faça um esforço para ter essas definições e quantificar o impacto da IoT, de modo que seja possível fazer comparações internacionais e definir objetivos de política pública.

Anexo 3

Padrões atuais da IoT por vertical

TECNOLOGIAS CELULARES	VERTICAL	APLICAÇÕES	CARACTERÍSTICAS DA CONECTIVIDADE	PERFORMANCE
NB-IoT, LTE-M	Cidades Inteligentes	Iluminação inteligente, gestão de resíduos, estacionamento inteligente, bicicletas inteligentes, smart utilities	Baixo consumo de energia, ampla área de cobertura	<ul style="list-style-type: none">• Até 10 anos de duração de bateria¹⁰• Maior cobertura em comparação com LTE (até muitas vezes o raio de uma célula padrão dependendo das condições operacionais)
	Agricultura Inteligente	Qualidade da água, monitoramento de rebanhos, controle de pragas	Cobertura outdoor / rural, baixo custo, continuidade de serviço	<ul style="list-style-type: none">• Baixa potência e maior cobertura (como acima)• Facilidade de implantação• Baixo custo - os preços dos módulos caem rapidamente para US\$ 7 em 2025¹¹
Celular V2X (rede e modo direto)	Automotivo	Vehicle-to-everything (V2X), mapeamento, atualizações de software, infoentretenimento, telemetria	Ultrabaixa latência (aplicativos relacionados à segurança), cobertura onipresente, ampla base instalada	<ul style="list-style-type: none">• O C-V2X oferece mais de 450m no modo direto, ampla cobertura no modo rede• Até 90% de veículos com modems celulares embarcados até 2025
LTE	Drones	Gestão de Tráfego de veículos aéreos não-tripulados (UAV), registro de ID, geolocalização	Cobertura aérea	<ul style="list-style-type: none">• Até 122m. acima da cobertura aérea vertical ao nível do solo¹³

10. 3GPP- TR 45820
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2719>

11. <https://www.gsmaintelligence.com/research/2018/07/spurring-adoption-of-nb-iot-notes-from-china/685/>

12. <https://www.qualcomm.com/media/documents/files/accelerating-c-v2x-commercialization.pdf>

13. <https://www.qualcomm.com/news/onq/2017/05/03/qualcomm-technologies-releases-lte-drone-trial-results>

Anexo 4

Organismos de normatização da IoT

Dada a vasta natureza do setor, já existe uma ampla variedade de órgãos de padronização relacionados à IoT. Esta seção é focada naqueles mais relevantes da perspectiva da conectividade e da camada de serviço.

3GPP

O Third Generation Partnership Project (3GPP) é o órgão de especificação técnica do setor. Representantes de todas as sete principais organizações de desenvolvimento de padrões (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) participam do 3GPP. O 3GPP produz especificações técnicas para comunicações de conectividade que, por sua vez, são encapsuladas em padrões definidos por organizações de desenvolvimento de padrão.

O 3GPP cobre as tecnologias de redes de telecomunicações celulares, incluindo o acesso por rádio, a rede de transporte central e as capacidades de serviço - incluindo o trabalho em codecs, segurança, qualidade de serviço - e, portanto, fornece especificações completas do sistema. As especificações também fornecem ganchos para acesso “não-rádio” à rede principal e para interoperar com redes Wi-Fi.

Especificamente em IoT, a 3GPP produziu recentemente especificações técnicas para tecnologias de acesso por rádio para IoT de banda estreita (NB-IoT), e comunicação “Long term evolution machine type communication” (LTE-M) com o Release 13 (2016). As principais vantagens dessas especificações no contexto da IoT são:

- Baixo consumo de energia que permite que os dispositivos operem por 10 anos com uma só carga
- Baixo custo unitário do dispositivo
- Melhoria de penetração outdoor e indoor em comparação com as tecnologias de longo alcance existentes
- Conectividade segura e autenticação forte
- Transferência de dados otimizada (suporta pequenos blocos de dados intermitentes)
- Topologia e implantação de rede simplificada

- Integração em uma plataforma unificada/horizontal de Internet das Coisas (IoT)/Machine-to-Machine (M2M), quando implementado pela operadora

- Escalabilidade de rede para atualizações de capacidade

ONE M2M

A finalidade e meta do oneM2M é desenvolver especificações técnicas que atendam à necessidade de uma Camada de Serviço M2M comum, que possa ser prontamente incorporada em vários hardwares e softwares, e que seja confiável para conectar a miríade de dispositivos no campo com servidores de aplicativos M2M em todo o mundo. O oneM2M prepara, aprova e mantém o conjunto necessário de Especificações e Relatórios Técnicos para:

- Casos de uso e requisitos para um conjunto comum de recursos da camada de serviço;
- Aspectos da camada de serviço de alto nível com arquitetura de serviços detalhada, à luz de uma visão independente de acesso dos serviços de ponta a ponta;
- Protocolos/APIs/objetos padrão baseados nessa arquitetura (interfaces abertas e protocolos);
- Aspectos de segurança e privacidade (autenticação, criptografia, verificação de integridade);
- Acessibilidade e descoberta de aplicações;
- Interoperabilidade, incluindo especificações de teste e conformidade;
- Coleta de dados para cobrança de registros (para fins de faturamento e estatísticas);
- Identificação e nomeação de dispositivos e aplicativos;
- Modelos de informações e gerenciamento de dados (incluindo a funcionalidade de armazenar e assinar/notificar);
- Aspectos de gestão (incluindo gerenciamento remoto de entidades);

- Casos comuns de uso, aspectos de terminal/módulo, incluindo interfaces/APIs da Camada de Serviço entre Camadas de Aplicativo e de Serviço e Camada de Serviço e funções de comunicação.

ETSI

ETSI é o órgão regional de padrões reconhecido na Europa - European Standards Organization (ESO) - que lida com telecomunicações, radiodifusão e outras redes e serviços de comunicações eletrônicas. A ETSI está envolvida na padronização de muitas das tecnologias usadas para conectar “coisas” na IoT.

- M2M
 - ETSI é membro do oneM2M, a iniciativa de parceria global que visa fornecer uma interface M2M padronizada. Isto permitirá a conexão de diferentes dispositivos na IoT, independentemente da rede subjacente. O trabalho do oneM2M baseia-se nas atividades do comitê ETSI TC SmartM2M, que desenvolveu e agora mantém as especificações do ETSI para uma plataforma padronizada:
 - Requisitos (ETSI TS 102 689)
 - Arquitetura funcional (ETSI TS 102 690)
 - Descrições de interface (ETSI TS 102 921)
- Aplicativos IoT
 - Aparelhos inteligentes
 - Medição inteligente
 - Cidades inteligentes
 - Redes inteligentes
 - eHealth
 - Sistemas Inteligentes de Transporte
 - Automação Industrial Sem Fio
- Outros aspectos relacionados à IoT
 - Segurança para a IoT
 - Fontes de baixa energia na IoT
 - Requisitos de espectro radioelétrico
 - Módulos de comunicação embarcados
 - Multi-access Edge Computing
 - Gestão de Informação
 - Plataforma de cartão inteligente
 - Virtualização de Rede

INICIATIVA IEEE IOT

O Instituto de Engenheiros Elétricos e Eletrônicos (IEEE) também tem um papel na padronização da IoT, conhecido como IEEE IoT Initiative.

A missão da IEEE IoT Initiative é servir como ponto de encontro para a comunidade técnica global que trabalha na Internet das Coisas, para fornecer a plataforma onde os profissionais aprendem, compartilham conhecimento e colaboram nessa convergência abrangente de tecnologias, mercados, aplicativos e Internet.

IEEE IoT Initiative tem trabalhado em vários problemas, incluindo padrões para ethernet, coexistência de WPANs com outros dispositivos sem fio que operam em bandas de frequência não licenciadas, topologia de malha, smart grid, e-health e outros.

INTERNET ENGINEERING TASK FORCE (IETF)

IETF é uma comunidade internacional aberta de designers de redes, operadores, fornecedores e pesquisadores que desenvolvem padrões de internet para a evolução da arquitetura da Internet. Vários grupos de trabalho da IETF estão desenvolvendo protocolos que são diretamente relevantes para a IoT, ou seja, CoAP, TLS / DTLS.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

A ISO é uma organização internacional baseada na associação de órgãos nacionais de normatização, como a ABNT no Brasil. Os padrões mais populares produzidos pela ISO são ISO 9001, para Gestão da Qualidade, ISO 8601 para formato de data e hora, ISO 3166 para códigos de país, ISO 50001 para a gestão de energia, além de uma grande variedade de normas específicas por setor.

GSMA

A GSMA representa os interesses das operadoras móveis em todo o mundo, unindo operadoras com empresas do ecossistema móvel mais amplo, incluindo fabricantes de celulares e aparelhos, empresas de software, fornecedores de equipamentos e empresas de internet, bem como organizações em setores adjacentes da indústria. A GSMA fornece uma ampla gama de especificações e princípios relacionados à interoperabilidade entre operadoras móveis. Outras áreas relevantes de trabalho incluem a atribuição e banco de dados de IMEI, roaming, cobrança, testes, segurança, etc.



GSMALA.COM

