LA INTERNET DE LAS COSAS— UNA BREVE RESEÑA

Para entender mejor los problemas y desafíos de un mundo más conectado

OCTUBRE DE 2015

Internet Society™

LA INTERNET DE LAS COSAS— UNA BREVE RESEÑA

Para entender mejor los problemas y desafíos de un mundo más conectado

Karen Rose, Scott Eldridge, Lyman Chapin

OCTUBRE DE 2015

Internet Society™

ÍNDICE

¿QUÉ ES LA INTERNET DE LAS COSAS? 12

¿QUÉ TEMAS SE ESTÁN PLANTEANDO EN TORNO A LA INTERNET DE LAS COSAS? 29

RESUMEN EJECUTIVO

La Internet de las cosas es un tema emergente de importancia técnica, social y económica. En este momento se están combinando productos de consumo, bienes duraderos, automóviles y camiones, componentes industriales y de servicios públicos, sensores y otros objetos de uso cotidiano con conectividad a Internet y potentes capacidades de análisis de datos que prometen transformar el modo en que trabajamos, vivimos y jugamos. Las proyecciones del impacto de la IoT sobre Internet y la economía son impresionantes: hay quienes anticipan que en el año 2025 habrá hasta cien mil millones de dispositivos conectados a la IoT y que su impacto será de US$ 11.000.000.000.000.

Sin embargo, la Internet de las Cosas también plantea importantes desafíos que podrían dificultar la realización de sus potenciales beneficios. Noticias sobre ataques a dispositivos conectados a Internet, el temor a la vigilancia y las preocupaciones relacionadas con la privacidad ya han captado la atención del público. Los desafíos técnicos siguen allí, pero además están surgiendo nuevos desafíos de políticas, jurídicos y de desarrollo.

Este documento informativo está diseñado para ayudar a la comunidad de la Internet Societys a navegar los diálogos que rodean a la Internet de las Cosas a la luz de las predicciones contradictorias sobre sus promesas y los peligros que implica. La Internet de las Cosas plantea un amplio conjunto de ideas complejas y que se entrelazan desde diferentes perspectivas.

Los conceptos clave que sirven como base para explorar las oportunidades y desafíos de la IoT incluyen:

DEFINICIONES DE LA INTERNET DE LAS COSAS

Por lo general, el término Internet de las Cosas se refiere a escenarios en los que la conectividad de red y la capacidad de cómputo se extienden a objetos, sensores y artículos de uso diario que habitualmente no se consideran computadoras, permitiendo que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana. Sin embargo, no existe ninguna definición única y universal.

TECNOLOGÍAS INSTRUMENTALES

El concepto de combinar computadoras, sensores y redes para monitorear y controlar diferentes dispositivos ha existido durante décadas. Sin embargo, la reciente confluencia de diferentes tendencias del mercado tecnológico está permitiendo que la Internet de las Cosas esté cada vez más cerca de ser una realidad generalizada. Estas tendencias incluyen la conectividad omnipresente, la adopción generalizada de redes basadas en el protocolo IP, la economía en la capacidad de cómputo, la miniaturización, los avances en el análisis de datos y el surgimiento de la computación en la nube.

MODELOS DE CONECTIVIDAD

Las implementaciones de la IoT utilizan diferentes modelos de conectividad, cada uno de los cuales tiene sus propias características. Los cuatro de los modelos de conectividad descritos por la Junta de Arquitectura de Internet incluyen: *Device-to-Device* (dispositivo a dispositivo), *Device-to-Cloud* (dispositivo a la nube), *Device-to-Gateway* (dispositivo a puerta de enlace) y *Back-End Data-Sharing* (intercambio de datos a través del *back-end*). Estos modelos destacan la flexibilidad en las formas en que los dispositivos de la IoT pueden conectarse y proporcionar un valor para el usuario.

POTENCIAL DE TRANSFORMACIÓN

Si las tendencias y proyecciones sobre el desarrollo de la IoT se convierten en realidad, esto podría obligar un cambio de mentalidad con respecto a las implicancias y problemas en un mundo donde la interacción más frecuente con Internet provendrá de la interacción pasiva con objetos conectados y no de una interacción activa con el contenido. La potencial realización de este resultado —un "mundo hiperconectado"— es una prueba de la naturaleza de propósito general de la propia arquitectura de Internet, que no impone limitaciones inherentes a las aplicaciones o servicios que pueden hacer uso de la tecnología.

Se analizan cinco áreas temáticas clave de la IoT para explorar algunos de los desafíos y cuestiones relacionadas con la tecnología más urgentes. Estos incluyen la seguridad; la privacidad; la interoperabilidad y los estándares; cuestiones legales, reglamentarias y relacionadas con los derechos; y economías emergentes y cuestiones relacionadas con el desarrollo.

SEGURIDAD

Si bien en el contexto de la tecnología de la información las consideraciones de seguridad no son nuevas, los atributos de muchas implementaciones de la IoT presentan desafíos de seguridad nuevos y únicos. Hacer frente a estos desafíos y garantizar la seguridad en los productos y servicios de la IoT debe ser una prioridad fundamental. Los usuarios deben poder confiar en que los dispositivos de la IoT y los servicios de datos relacionados serán seguros y estarán libres de vulnerabilidades, especialmente a medida que esta tecnología sea más difundida y se integre a nuestra vida diaria. Los dispositivos y servicios de la IoT poco seguros pueden servir como potenciales puntos de entrada de ataques cibernéticos y exponer los datos de los usuario al robo al dejar flujos de datos con una protección inadecuada.

La naturaleza interconectada de los dispositivos de la IoT significa que cada dispositivo mal asegurado conectado a Internet podría afectar la seguridad y la resistencia de Internet a nivel global. Este desafío se ve amplificado por otras consideraciones, como el despliegue a gran escala de dispositivos homogéneos, la capacidad de algunos dispositivos de conectarse automáticamente a otros y la posibilidad de que estos dispositivos sean desplegados en entornos no seguros.

Por principio, los desarrolladores y usuarios de dispositivos y sistemas de la IoT tienen la obligación colectiva de asegurar que no estén exponiendo a los usuarios y la propia Internet a daños potenciales. Por lo tanto, se necesitará un enfoque colaborativo para desarrollar soluciones eficaces y adecuadas ante los desafíos de seguridad de la IoT, soluciones que se adapten bien a la escala y complejidad de los problemas.

PRIVACIDAD

El potencial de la Internet de las Cosas depende de estrategias que respeten las opciones de privacidad individuales correspondientes a un amplio espectro de expectativas. Los flujos de datos y la especificidad que permiten los dispositivos de la IoT puede liberar un valor único e increíble para los usuarios, pero las preocupaciones con respecto a la privacidad y los potenciales daños podrían dificultar la adopción plena de la Internet de las Cosas. Esto significa que los derechos de privacidad y las expectativas con respeto a la privacidad de los usuarios son esenciales para asegurar la confianza de los usuarios en Internet, en los dispositivos conectados y en los servicios relacionados.

De hecho, la Internet de las Cosas está redefiniendo el debate sobre las cuestiones de privacidad, ya que muchas implementaciones pueden cambiar drásticamente las formas en que se recogen, analizan, emplean y protegen los datos personales. Por ejemplo, la IoT amplifica las preocupaciones sobre el potencial de una mayor vigilancia y seguimiento, la dificultad de poder optar por no ser incluidos en ciertas recolecciones de datos y la potencia que tiene la agregación de los flujos de datos de la IoT para obtener retratos digitales detallados de los usuarios. Si bien estos desafíos son importantes, no son imposibles de superar. Para aprovechar las oportunidades, se deberán desarrollar estrategias para respetar las opciones de privacidad individuales considerando un amplio espectro de expectativas, sin dejar de fomentar la innovación en nuevas tecnologías y servicios.

INTEROPERABILIDAD / ESTÁNDARES

Un entorno fragmentado de implementaciones técnicas propietarias de IoT podría inhibir su valor para los usuarios y la industria. Si bien la interoperabilidad plena entre productos y servicios no siempre es posible o necesaria, los compradores podrían ser reacios a adquirir productos y servicios de la IoT si hay falta de flexibilidad en su integración, gran complejidad en cuanto a su propiedad y preocupación con respecto a posibles dificultades para cambiar de proveedores de tecnología (*lock-in*).

Además, los dispositivos de la IoT mal diseñados y configurados pueden tener consecuencias negativas para los recursos de red a los cuales se conectan y para Internet en un sentido más amplio. Contar con estándares apropiados, modelos de referencia y mejores prácticas también ayudará a frenar la proliferación de dispositivos que podrían alterar a Internet. El uso de estándares genéricos, abiertos y ampliamente disponibles (como el Protocolo de Internet) como componentes de los dispositivos y servicios de la IoT permitirá mayores ventajas para los usuarios, más innovación y más oportunidades económicas.

CUESTIONES LEGALES, REGLAMENTARIAS Y DE DERECHOS

El uso de dispositivos de la IoT plantea nuevas cuestiones reglamentarias y legales y también amplifica los problemas legales que ya existen en torno a Internet. Estas cuestiones son de amplio alcance y muchas veces el rápido ritmo con que cambia la tecnología de la IoT supera la capacidad de adaptación de las estructuras políticas, legales y reglamentarias asociadas.

Un conjunto de cuestiones tiene que ver con los flujos de datos transfronterizos, que se producen cuando los dispositivos de la IoT recogen datos personales en una jurisdicción y, para su procesamiento, los transmiten a otra jurisdicción donde las leyes de protección de datos son diferentes. Además, los datos recogidos por los dispositivos de la IoT podrían ser mal utilizados y potencialmente provocar resultados discriminatorios para ciertos usuarios. Otros problemas legales relacionados con los dispositivos de la IoT incluyen el conflicto entre la vigilancia por parte de las agencias de seguridad y los derechos civiles, las políticas de retención y destrucción de datos, y la responsabilidad legal por los usos accidentales, las violaciones de la seguridad y los fallos en la privacidad.

Aunque los desafíos legales y reglamentarios son de alcance amplio y complejo, la adopción de los principios rectores de la Internet Society para promover la capacidad del usuario para *conectarse, hablar, innovar, compartir, elegir,* y *confiar* es una consideración fundamental para la evolución de leyes y reglamentos sobre la IoT que propicien los derechos de los usuarios.

CUESTIONES RELACIONADAS CON LAS ECONOMÍAS EMERGENTES Y EL DESARROLLO:

La Internet de las Cosas encierra la promesa de aportar beneficios sociales y económicos a las economías emergentes y en desarrollo. Esto incluye, entre otras, áreas tales como la agricultura sostenible, la calidad y el uso del agua, el cuidado de la salud, la industrialización y la gestión del medio ambiente. Como tal, la IoT promete ser una herramienta para lograr los Objetivos de Desarrollo Sostenible de las Naciones Unidas.

El alcance de los desafíos de la IoT no se limitará a los países industrializados. Las regiones en desarrollo también deberán responder para hacer realidad los potenciales beneficios de la IoT. Además, se deberán abordar las singulares necesidades y desafíos de la implementación en las regiones menos desarrolladas, entre ellos el grado de preparación de la infraestructura, los incentivos para el mercado y la inversión, los requerimientos en cuanto a las habilidades técnicas y los recursos de políticas.

La Internet de las Cosas está ocurriendo ahora. Promete ofrecer un mundo revolucionario, "inteligente" y totalmente conectado a medida que las relaciones entre los objetos, su entorno y las personas estén cada vez más entrelazadas. Sin embargo, para que la IoT realice sus potenciales beneficios para las personas, la sociedad y la economía, es necesario considerar y abordar los problemas y desafíos asociados con la IoT.

En definitiva, un debate polarizado que enfrente a las promesas de la IoT contra sus posibles peligros no permitirá encontrar soluciones que maximicen los beneficios de la Internet de las Cosas y minimicen sus riesgos. Por el contrario, para definir las formas más eficaces de avanzar, se necesitará la participación informada, el diálogo y la colaboración de una variedad de partes interesadas.

INTRODUCCIÓN

La Internet de las Cosas (IoT) es un tema importante en la industria de la tecnología, las políticas y los círculos de ingeniería y se ha convertido en noticia de primera plana, tanto en la prensa especializada como en los medios populares. Esta tecnología se encarna en una amplia gama de productos, sistemas y sensores en red, que aprovechan los avances en la potencia de cálculo, la miniaturización de los componentes electrónicos y las interconexiones de red para ofrecer nuevas capacidades que antes no eran posibles. Una gran cantidad de conferencias, informes y artículos de noticias están discutiendo y debatiendo el potencial impacto de la "revolución de la IoT", desde nuevas oportunidades de mercado y modelos de negocio hasta las preocupaciones con respecto a la seguridad, la privacidad y la interoperabilidad técnica.

La implementación a gran escala de dispositivos de la IoT promete transformar muchos aspectos de la forma en que vivimos. Para los consumidores, los nuevos productos de la IoT —electrodomésticos, componentes de automatización del hogar y dispositivos de gestión de energía con conexión a Internet— nos están llevando hacia una visión de la "casa inteligente" que ofrece mayor seguridad y eficiencia energética. Otros dispositivos personales de la IoT —entre ellos los dispositivos portátiles para monitorear y gestionar la actividad física y los dispositivos médicos con conexión a Internet— están transformando la forma en que se ofrecen los servicios de salud. Esta tecnología promete ser beneficiosa para las personas mayores o con discapacidad, mejorando sus niveles de independencia y calidad de vida a un costo razonable.[1] Los sistemas de la IoT como los vehículos conectados en red, los sistemas de tráfico inteligentes y los sensores integrados en carreteras y puentes nos acercan más a la idea de "ciudades inteligentes", que ayudan a minimizar la congestión y el consumo de energía. La tecnología de la IoT ofrece la posibilidad de transformar la agricultura, la industria y la producción y distribución de energía mediante el aumento de la disponibilidad de información a lo largo de la cadena de valor de la producción por medio de sensores conectados en red. Sin embargo, la IoT plantea muchas preguntas y desafíos que se deben tener en cuenta y abordar para que se puedan realizar sus potenciales beneficios.

Diferentes empresas y organizaciones dedicadas a la investigación han publicado una amplia gama de proyecciones sobre el potencial impacto que tendrá la IoT sobre Internet y sobre la economía en los próximos cinco a diez años. Por ejemplo, Cisco ha proyectado que para el año 2019 habrá más de 24 mil millones de objetos conectados

a Internet,[2] aunque Morgan Stanley anticipa que para el año 2020 habrá 75 mil millones de dispositivos conectados en red.[3] Considerando un período de tiempo más largo, Huawei sube la apuesta y anticipa que en 2025 habrá 100 mil millones de conexiones a la IoT.[4] El McKinsey Global Institute sugiere que el impacto financiero de la IoT sobre la economía global puede llegar a ser de $3.9 a $11.1 mil millones en 2025.[5] Aunque la variabilidad de las predicciones las vuelve cuestionables, en conjunto permiten entrever una influencia y un crecimiento significativos.

Algunos observadores ven a la IoT como un mundo "inteligente", revolucionario y totalmente interconectado; un mundo de progreso, eficiencia y oportunidades, con el potencial de añadir un valor equivalente a miles de millones para la industria y la economía global.[6] Otros advierten que la IoT representa un mundo más oscuro, un mundo de vigilancia y violaciones a la privacidad en el cual los consumidores estarán atrapados. Los titulares sobre ataques cibernéticos a automóviles conectados a Internet,[7] las preocupaciones con respecto a la vigilancia que surgen de las funciones de reconocimiento de voz de los televisores "inteligentes"[8] y los temores con respecto a la privacidad que se derivan del posible uso indebido de los datos de la IoT[9] han captado la atención del público. Sumado a la gran cantidad de información que publican los medios populares y el marketing, este debate sobre "promesas contra peligros" puede hacer que la IoT sea un tema complejo y difícil de entender.

En síntesis, la Internet Society se preocupa por la IoT porque representa un componente cada vez mayor de la forma en que las personas y las instituciones probablemente interactuarán con Internet en sus vidas personales, sociales y económicas. Incluso si resultan ser correctas las proyecciones más modestas, una explosión de aplicaciones de la IoT podría provocar un cambio fundamental en la forma en que los usuarios interactúan con —y se ven afectados por— Internet, plantseando nuevas cuestiones y diferentes dimensiones de los desafíos existentes que atravesarán a todos los usuarios/consumidores, la tecnología, las políticas y el derecho. Probablemente la IoT también tendrá diferentes consecuencias en diferentes economías y regiones, por lo que llevará un variado conjunto de oportunidades y desafíos a todo el mundo.

Este documento informativo está diseñado para ayudar a la comunidad de la Internet Society a comprender los diálogos que rodean a la Internet de las Cosas a la luz de las predicciones contradictorias sobre sus promesas y los peligros que implica. Presenta una descripción de alto nivel de los conceptos básicos de la IoT y algunas de las principales cuestiones y preguntas que esta tecnología plantea desde la perspectiva de la Internet Society y los valores fundamentales que nuestra organización promueve.[10, 11] También reconoce algunos de los aspectos únicos de la Internet de las Cosas que la convierten en una tecnología transformacional para Internet.

Dado que el presente pretende ser un documento de naturaleza general, en este momento no proponemos para ISOC ningún curso de acción específico sobre la IoT. Más bien consideramos que este documento es una fuente de información y un punto de partida para el debate sobre cuestiones relacionadas con la IoT dentro de la comunidad de ISOC.

NOTAS DE LA SECCIÓN

Introducción

1. Para obtener más información sobre la IoT y su relación con las personas con discapacidad véase, por ejemplo: Valerio, Pablo. "Google: IoT Can Help The Disabled." *InformationWeek*, 10 de marzo, 2015. http://www.informationweek.com/mobile/mobile-devices/google-iot-can-help-the-disabled/a/d-id/1319404; y Domingo, Mari Carmen. "An Overview of the Internet of Things for People with Disabilities." *Journal of Network and Computer Applications* 35, no. 2 (marzo de 2012): 584–96. doi:10.1016/j.jnca.2011.10.015.

2. "Cloud and Mobile Network Traffic Forecast - Visual Networking Index (VNI)." *Cisco, 2015*. http://cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

3. Danova, Tony. "Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020." *Business Insider*, October 2, 2013. http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10

4. "Global Connectivity Index." Huawei Technologies Co., Ltd., 2015. Web. 6 de septiembre de 2015. http://www.huawei.com/minisite/gci/en/index.html

5. Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, junio de 2015.

6. Thierer, Adam, and Andrea Castillo. "Projecting the Growth and Economic Impact of The Internet of Things." George Mason University, Mercatus Center, 15 de junio de 2015. http://mercatus.org/sites/default/files/IoT-EP-v3.pdf

7. Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway—With Me in It." *WIRED*, 21 de julio de 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

8. "Samsung Smart TV's Voice Recognition Creates Privacy Concerns." *CBS This Morning*. CBS News, 10 de febrero de 2015. http://www.cbsnews.com/videos/samsung-smart-tvs-voice-recognition-creates-privacy-concerns/

9. Bradbury, Danny. "How Can Privacy Survive in the Era of the Internet of Things?" *The Guardian*, 7 de abril de 2015, sección sobre. Tecnología. http://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things

10. "Values and Principles." *Principles*. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles

11. Se ha escrito una gran cantidad de papers y artículos sobre la IoT. Los lectores interesados en profundizar más allá del alcance de este documento pueden investigar la literatura indicada en las notas al pie y en la sección Referencias incluida al final de este documento.

¿QUÉ ES LA INTERNET DE LAS COSAS?

ORÍGENES, IMPULSORES Y APLICACIONES

El término "Internet de las Cosas" (IoT) fue empleado por primera vez en 1999 por el pionero británico Kevin Ashton para describir un sistema en el cual los objetos del mundo físico se podían conectar a Internet por medio de sensores.[12] Ashton acuñó este término para ilustrar el poder de conectar a Internet las etiquetas de identificación por radiofrecuencia (RFID)[13] que se utilizaban en las cadenas de suministro corporativas para contar y realizar un seguimiento de las mercancías sin necesidad de intervención humana. Hoy en día, el término Internet de las Cosas se ha popularizado para describir escenarios en los que la conectividad a Internet y la capacidad de cómputo se extienden a una variedad de objetos, dispositivos, sensores y artículos de uso diario.

Aunque el término "Internet de las Cosas" es relativamente nuevo, el concepto de combinar computadoras y redes para monitorear y controlar diferentes dispositivos ha existido durante décadas. Por ejemplo, a fines de la década de 1970 ya había en el mercado sistemas disponibles para monitorear los medidores conectados a la red eléctrica de forma remota a través de las líneas telefónicas.[14] En la década de 1990, los avances en la tecnología inalámbrica permitieron la difusión de soluciones corporativas e industriales "máquina a máquina" (M2M) para monitorear y operar diferentes equipos. Sin embargo, muchas de estas primeras soluciones M2M se basaban en redes dedicadas especialmente construidas para este propósito y en estándares propietarios o específicos de la industria,[15] no en redes basadas en el Protocolo de Internet (IP) y los estándares de Internet.

El uso del protocolo IP para conectar a Internet dispositivos que no son computadoras no es una idea nueva. El primer "dispositivo" para Internet —una tostadora conectada vía IP que se podía encender y apagar a través de Internet— se presentó en una conferencia sobre Internet realizada en 1990.[16] Durante los años siguientes se fueron conectando otras "cosas" vía IP, entre ellas una máquina de refrescos[17] en la Universidad Carnegie Mellon en Estados Unidos y una cafetera[18] en el *Trojan Room* de la Universidad de Cambridge en el Reino Unido (que permaneció conectada a Internet hasta 2001). Luego de estos coloridos inicios, una robusta área de investigación y desarrollo dedicada a las "redes de objetos inteligentes"[19] ayudó a sentar las bases de la Internet de las Cosas como la conocemos hoy.

Si la idea de conectar objetos entre sí y a Internet no es nuevo, es razonable preguntar por qué la Internet de las Cosas es un tema que hoy en día está ganando popularidad.

Desde una perspectiva amplia, la confluencia de diferentes tendencias tecnológicas y de mercado[20] está permitiendo interconectar dispositivos más pequeños de forma económica y sencilla:

CASILLA 1

TENDENCIAS TECNOLÓGICAS Y DE MERCADO QUE ESTÁN IMPULSANDO LA IOT

CONECTIVIDAD UBICUA

La conectividad generalizada, de bajo costo y alta velocidad, sobre todo a través de servicios y tecnología inalámbricos con y sin licencia, hace que casi todo sea "conectable".

ADOPCIÓN GENERALIZADA DE REDES BASADAS EN EL PROTOCOLO IP

El protocolo IP se ha convertido en el estándar dominante para la creación de redes y ofrece una plataforma bien definida y ampliamente implementada en software y herramientas que se pueden incorporar en una variedad de dispositivos de forma fácil y económica.

ECONOMÍAS EN LA CAPACIDAD DE CÓMPUTO

Impulsada por las inversiones de la industria en las áreas de investigación, desarrollo y fabricación, la Ley de Moore[21] continúa ofreciendo mayor potencia de cálculo a precios más bajos y con menor consumo de energía.[22]

MINIATURIZACIÓN

Los avances logrados en la fabricación permiten incorporar tecnología de cómputo y comunicaciones de vanguardia en objetos muy pequeños.[23] Junto con una mayor economía en la capacidad de cómputo, esto ha impulsado el desarrollo de sensores pequeños y de bajo costo que a su vez impulsan muchas aplicaciones de la IoT.

AVANCES EN EL ANÁLISIS DE DATOS

La existencia de nuevos algoritmos y el rápido aumento de la potencia de cálculo, el almacenamiento de datos y los servicios en la nube permiten agregar, correlacionar y analizar grandes cantidades de datos. Estos conjuntos de datos grandes y dinámicos ofrecen nuevas oportunidades para extraer información y conocimiento.

SURGIMIENTO DE LA COMPUTACIÓN EN LA NUBE

La computación en la nube aprovecha recursos informáticos remotos conectados en red para procesar, gestionar y almacenar datos. Este paradigma permite que dispositivos pequeños y distribuidos interactúen con potentes sistemas de soporte que brindan capacidades analíticas y de control.

Desde este punto de vista, la IoT representa la convergencia de una variedad de tendencias en las áreas de la computación y la conectividad que se vienen dando desde hace muchas décadas. En la actualidad, una amplia gama de sectores de la industria —entre ellos el sector automotriz, la salud, la manufactura, la electrónica de consumo y para el hogar— están analizando el potencial de incorporar la tecnología de la IoT en sus productos, servicios y operaciones.

En su informe titulado "Unlocking the Potential of the Internet of Things", el McKinsey Global Institute[24] describe la amplia variedad de potenciales aplicaciones en términos de "entornos" donde se espera que la IoT creará valor para la industria y también para los usuarios.

Muchas organizaciones han desarrollado sus propias taxonomías y clasificaciones de las aplicaciones de la IoT y sus casos de uso. Por ejemplo, "IoT industrial" es un término ampliamente utilizado por empresas y asociaciones para describir aplicaciones de la IoT que se relacionan con la producción de bienes y servicios, por ejemplo, en la industria manufacturera y los servicios públicos.[26] Otros discuten la IoT según el tipo de dispositivo, por ejemplo, dispositivos para vestir[27] y electrodomésticos.[28] Aún otros abordan la IoT en el contexto de implementaciones integradas basadas en su ubicación, por ejemplo "hogares inteligentes" o "ciudades inteligentes".[29] Sea cual fuera la aplicación, es evidente que los casos de uso de la IoT se podrían extender a casi todos los aspectos de nuestras vidas.

A medida que crece el número de dispositivos conectados a Internet, se espera que la cantidad de tráfico que generan aumentará significativamente. Por ejemplo, Cisco estima que el tráfico generado por dispositivos que no son computadoras personales aumentará del 40% en 2014 a casi el 70% en 2019.[30] Cisco también pronostica que el número de conexiones "máquina a máquina" ("M2M ") (incluyendo las aplicaciones industriales, residenciales, para el cuidado de la salud, automotrices y otros mercados verticales de la IoT) aumentará del 24% de todos los dispositivos conectados en 2014 al 43% en 2019.

Una consecuencia de estas tendencias es que en los próximos diez años podría producirse un cambio en la noción popular de lo que significa estar "en Internet". Como señaló Neil Gershenfied,

70%

Cisco estima que el tráfico generado por dispositivos que no son computadoras personales aumentará del 40% en 2014 a casi el 70% en 2019.

Profesor del MIT, "...[E]l rápido crecimiento de la World Wide Web puede haber sido la carga que ahora está disparando la verdadera explosión a medida que las cosas empiezan a utilizar la Red".[31]

En el pensamiento popular, la World Wide Web se ha convertido prácticamente en sinónimo de la propia Internet. Las tecnologías web facilitan la mayoría de las interacciones entre las personas y el contenido, lo que las convierte en una característica definitoria de la experiencia de Internet actual. La experiencia web se caracteriza en gran medida por la participación activa de los usuarios que descargan y generan contenidos a través de sus computadoras y teléfonos inteligentes. Si las proyecciones de crecimiento para la IoT se convierten en realidad, podríamos ser testigos de un cambio hacia una interacción más pasiva en Internet, una interacción entre usuarios y objetos tales como componentes de automóviles, electrodomésticos y dispositivos de monitoreo personal; estos dispositivos envían y reciben datos en nombre del usuario, con poca intervención humana e incluso sin que nadie tenga conciencia de lo que está ocurriendo.

Si la interacción más frecuente con Internet —y la información derivada e intercambiada a través de dicha interacción— proviene de la participación pasiva con objetos conectados en el entorno más amplio, la IoT podría forzar un cambio en esta forma de pensar. La potencial realización de este resultado —un "mundo hiperconectado"— es una prueba de la naturaleza de propósito general de la arquitectura de Internet, que no impone limitaciones inherentes a las aplicaciones o servicios que pueden hacer uso de la tecnología.[32]

CASILLA 2

"ENTORNOS" PARA APLICACIONES DE LA IOT

ENTORNO	EJEMPLOS
CUERPO HUMANO Dispositivos unidos al cuerpo humano o colocados dentro del mismo.	Dispositivos (para vestir e ingeribles) para monitorear y mantener la salud y el bienestar de las personas, manejar enfermedades, aumentar la aptitud física y la productividad
HOGAR Edificios de vivienda	Controladores y sistemas de seguridad para el hogar
PUNTOS DE VENTA Espacios comerciales	Tiendas, bancos, restaurantes, estadios, cualquier lugar donde los consumidores consideren y compren; sistemas de autopago, ofertas en compras presenciales, optimización del inventario
OFICINAS Espacios donde trabajan trabajadores del conocimiento	Gestión de la energía y la seguridad en los edificios de oficinas; mejora de la productividad, incluso para los empleados móviles
FÁBRICAS Entornos de producción estandarizados	Lugares con rutinas de trabajo repetitivas, como hospitales y granjas; eficiencia operativa, optimización del uso de los equipos y el inventario
OBRAS Entornos de producción a medida	Minería, petróleo y gas, construcción; eficiencia operativa, mantenimiento predictivo, salud y seguridad
VEHÍCULOS Sistemas dentro de vehículos en movimiento	Vehículos, incluyendo automóviles, camiones, barcos, aviones y trenes; mantenimiento basado en la condición, diseño, basado en el uso, análisis de preventa
CIUDADES Entornos urbanos	Espacios públicos e infraestructura en entornos urbanos; sistemas de control adaptativo de tráfico, contadores inteligentes, monitoreo ambiental, gestión de recursos
EXTERIORES Entre entornos urbanos (y fuera de otros entornos)	Los usos exteriores incluyen las vías de ferrocarril, los vehículos autónomos (fuera de los centros urbanos) y la navegación aérea; el enrutamiento en tiempo real, la navegación conectada, el seguimiento de envíos

FUENTE: McKinsey Global Institute[25]

DEFINICIONES DIFERENTES, CONCEPTOS SIMILARES

A pesar del entusiasmo generalizado en torno a la Internet de las Cosas, no existe una definición única y universalmente aceptada para el término. Diferentes grupos utilizan diferentes definiciones para describir o promover una visión particular de lo que significa la IoT y sus atributos más importantes. Algunas definiciones especifican el concepto de Internet o del Protocolo de Internet (IP), mientras que otras —quizás sorprendentemente— no lo hacen. Por ejemplo, veamos las siguientes definiciones.

El Consejo de Arquitectura de Internet (IAB) comienza la RFC 7452,[33] "Architectural Considerations in Smart Object Networking", con esta definición:

> El término "Internet de las Cosas" (IoT) denota una tendencia en que un gran número de dispositivos embebidos utilizan los servicios de comunicación que ofrecen los protocolos de Internet. A estos dispositivos suelen llamarles "objetos inteligentes" y no son operados directamente por un ser humano, sino que existen como componentes en edificios o vehículos o están distribuidos en el entorno.

Dentro del Grupo de Trabajo en Ingeniería de Internet (IETF), el término "redes de objetos inteligentes" se utiliza habitualmente para referirse a la Internet de las Cosas. En este contexto, los "objetos inteligentes" son dispositivos que típicamente tienen limitaciones significativas, como por ejemplo limitaciones en cuanto a la energía, la memoria y los recursos de procesamiento, o el ancho de banda.[34] El trabajo en el IETF se organiza en torno a requisitos específicos para lograr la interoperabilidad entre varios tipos de objetos inteligentes.[35]

La Recomendación ITU–T Y.2060 que publicó la Unión Internacional de Telecomunicaciones (UIT) en 2012, *Overview of the Internet of things*[36] , discute el concepto de interconectividad, pero no vincula a la IoT específicamente con Internet:

> 3.2.2 Internet de las Cosas (IoT): Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras.
>
> Nota 1 — Gracias a la identificación, la adquisición y el procesamiento de datos y a las capacidades de comunicación, la IoT hace pleno uso de los objetos para ofrecer servicios a todo tipo de aplicaciones, garantizando a su vez el cumplimiento íntegro de los requisitos de seguridad y privacidad.
>
> Nota 2 — Desde una perspectiva más amplia, la IoT puede considerarse una noción con repercusiones tecnológicas y sociales.

Esta definición incluida en una convocatoria de trabajos para una edición de la IEEE Communications Magazine[37] vincula a la IoT con los servicios en la nube:

> La Internet de las Cosas (IoT) es un marco en el que todas las cosas tienen una representación y una presencia en Internet. Más específicamente, la Internet de las Cosas tiene como objetivo ofrecer nuevas aplicaciones y servicios que sirvan de puente entre el mundo físico y el virtual, en que las comunicaciones 'máquina a máquina' (M2M) representan la comunicación básica que permite las interacciones entre las cosas y las aplicaciones en la nube.

Oxford Dictionaries[38] ofrece una definición concisa que invoca a Internet como un elemento de la IoT:

> Internet de las Cosas (sustantivo): Interconexión a través de Internet de dispositivos de computación integrados en objetos cotidianos, que les permite enviar y recibir datos.

Todas las definiciones describen escenarios en los que la conectividad de red y la capacidad de cómputo se extiende a una constelación de objetos, dispositivos, sensores y artículos de uso diario que habitualmente no se consideran "computadoras". Las diferentes definiciones de la IoT no necesariamente son contradictorias, sino que más bien enfatizan diferentes aspectos del fenómeno de la IoT desde diferentes puntos de vista y casos de uso.

Sin embargo, la variedad de definiciones podría ser una fuente de confusión en el diálogo sobre cuestiones de la IoT, sobre todo en las discusiones entre grupos de partes interesadas o segmentos de la industria. En años recientes se produjo una confusión similar con respecto a la neutralidad de la red y la computación en la nube, ya que las diferentes interpretaciones de los términos a veces obstaculizan el diálogo. Si bien probablemente sea necesario desarrollar una definición única de la IoT, se debe reconocer que en las discusiones se deben tener en cuenta los diferentes puntos de vista existentes.

Para los propósitos de este trabajo, los términos "Internet de las cosas" e "IoT" en líneas generales se refieren a la ampliación de la conectividad de red y la capacidad de cómputo a objetos, dispositivos, sensores y elementos que habitualmente no se consideran computadoras. Estos "objetos inteligentes" requieren una mínima intervención humana para generar, intercambiar y consumir datos; muchas veces tienen conectividad con capacidad de recolección remota, análisis y gestión de datos.

Los modelos de redes y comunicaciones para objetos inteligentes incluyen algunos en que los datos intercambiados no atraviesan Internet ni una red basada en el protocolo IP. Incluimos estos modelos en nuestra descripción amplia de la "Internet de las cosas" utilizada para este trabajo. Lo hacemos porque probablemente los datos generados o procesados por estos objetos inteligentes finalmente atravesarán puertas de enlace con conectividad a redes basadas en IP o se incorporarán de alguna otra forma a características de productos accesibles a través de Internet. Por otra parte, los usuarios de los dispositivos de la IoT probablemente estarán más preocupados por los servicios prestados y por las implicancias de la utilización de estos servicios que por cuándo o dónde los datos atraviesan una red basada en IP.

Para los propósitos de este trabajo, los términos "Internet de las cosas" e "IoT" en líneas generales se refieren a la ampliación de la conectividad de red y la capacidad de cómputo a objetos, dispositivos, sensores y elementos que habitualmente no se consideran computadoras.

MODELOS DE COMUNICACIÓN DE LA INTERNET DE LAS COSAS

Desde el punto de vista operativo, es útil pensar en cómo se conectan y comunican los dispositivos de la IoT en términos de sus modelos de comunicación. En marzo de 2015, el Comité de Arquitectura de Internet (IAB) dio a conocer un documento para guiar la creación de redes de objetos inteligentes (RFC 7452),[39] que describe un marco de cuatro modelos de comunicación comunes que utilizan los dispositivos de la IoT. En la discusión siguiente se presenta este marco y se explican las principales características de cada modelo.

Comunicaciones 'dispositivo a dispositivo'

El modelo de comunicación dispositivo a dispositivo representa dos o más dispositivos que se conectan y se comunican directamente entre sí y no a través de un servidor de aplicaciones intermediario. Estos dispositivos se comunican sobre muchos tipos de redes, entre ellas las redes IP o la Internet. Sin embargo, para establecer comunicaciones directas de dispositivo a dispositivo, muchas veces se utilizan protocolos como Bluetooth,[40] Z-Wave[41] o ZigBee[42], como se muestra en la Figura 1.

Estas redes dispositivo a dispositivo permiten que los dispositivos que, para comunicarse e intercambiar mensajes, se adhieren a un determinado protocolo de comunicación logren su función. Por lo general, este modelo de comunicación se utiliza en aplicaciones como sistemas de automatización del hogar, que habitualmente utilizan pequeños paquetes de datos para la comunicación entre dispositivos con requisitos relativamente bajos en términos de la tasa de transmisión. Los dispositivos para la IoT residenciales —bombillas de luz, interruptores, termostatos y cerraduras— normalmente se envían pequeñas cantidades de información (por ejemplo, un mensaje del estado de bloqueo de una puerta o un comando para encender una luz) en un escenario de automatización del hogar.

Este enfoque de comunicación dispositivo a dispositivo ilustra muchos de los desafíos de interoperabilidad que se discuten más adelante en este trabajo. Según lo describe un artículo del *IETF Journal*, "muchas veces estos dispositivos se relacionan en forma directa, en general tienen [mecanismos de] seguridad y confianza integrados; además, utilizan modelos de datos específicos para cada dispositivo que requieren esfuerzos de desarrollo redundantes [por parte los fabricantes de dispositivos]".[43] Esto significa que los fabricantes deben invertir en desarrollar la forma de implementar formatos de datos específicos de diferentes dispositivos antes que métodos abiertos que permitan el uso de formatos de datos estándares.

Desde el punto de vista de los usuarios, esto significa que los protocolos de comunicación dispositivo a dispositivo subyacentes no son compatibles, lo que los obliga a seleccionar una

familia de dispositivos que emplean un protocolo común. Por ejemplo, la familia de dispositivos que utilizan el protocolo Z-Wave no es compatible de forma nativa con la familia de dispositivos ZigBee. Si bien estas incompatibilidades limitan la capacidad de elección de los usuarios a los dispositivos de una determinada familia de protocolos, los usuarios también saben que los productos de una familia determinada tienden a comunicarse bien.

FIGURA 1

Ejemplo de un modelo de comunicación dispositivo a dispositivo

Bombina del Fabricante A

Bluetooth, Z-Wave, Zigbee

Interruptor del Fabricante B

FUENTE: Tschofenig, H., et.al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. IAB, marzo de 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt.

Comunicaciones 'dispositivo a la nube'

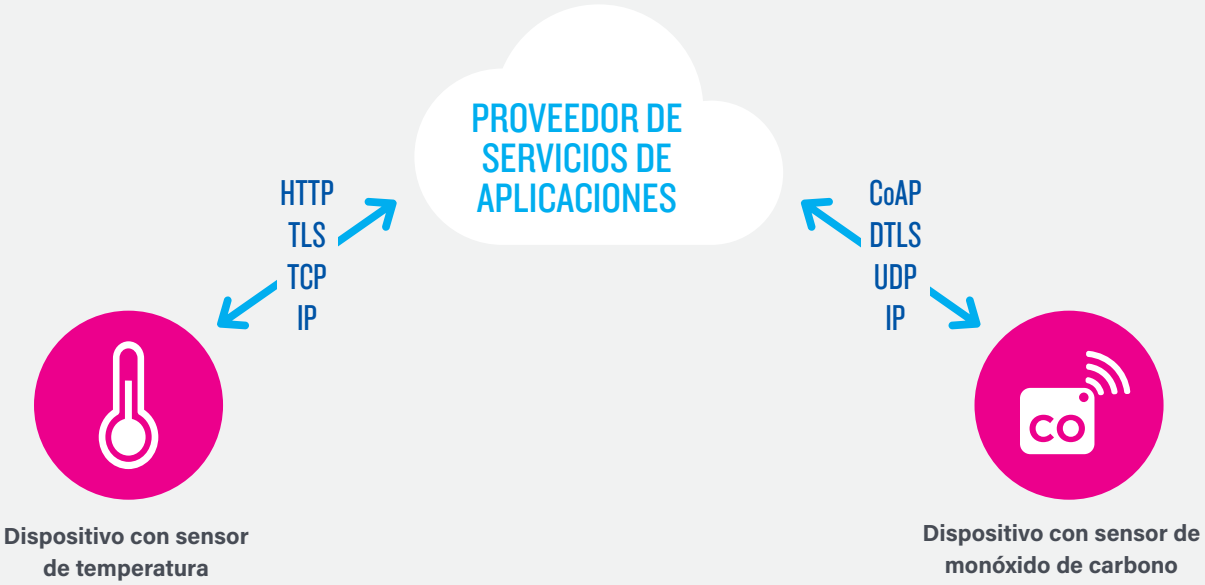
En un modelo de comunicación de dispositivo a la nube, el dispositivo de la IoT se conecta directamente a un servicio en la nube, como por ejemplo un proveedor de servicios de aplicaciones para intercambiar datos y controlar el tráfico de mensajes. Este enfoque suele aprovechar los mecanismos de comunicación existentes (por ejemplo, las conexiones Wi-Fi o Ethernet cableadas tradicionales) para establecer una conexión entre el dispositivo y la red IP, que luego se conecta con el servicio en la nube. Esto se ilustra en la Figura 2.

Este modelo de comunicación es empleado por algunos dispositivos electrónicos de consumo para la IoT, entre ellos el *Learning Thermostat*[44] de *Nest Labs* y el *SmartTV* de Samsung.[45] En el caso del *Learning Thermostat*, el dispositivo transmite los datos a una base de datos en la nube donde se pueden usar para analizar el consumo de energía en el hogar. Además, esta conexión a la nube permite que el usuario acceda a su termostato en forma remota, a través de un teléfono inteligente o una interfaz web, y también soporta las actualizaciones del software del termostato. Algo similar ocurre con la tecnología *SmartTV* de Samsung — el televisor utiliza una conexión a Internet para transmitir información a Samsung para su análisis y para activar las funciones interactivas de reconocimiento de voz de la televisión. En estos casos, el modelo dispositivo a la nube agrega valor para el usuario final, ya que amplía las capacidades del dispositivo más allá de sus características nativas.

No obstante, al intentar integrar dispositivos de diferentes fabricantes pueden surgir problemas de interoperabilidad. Muchas veces el dispositivo y el servicio en la nube son del mismo proveedor de tecnología.[46] Si entre el dispositivo y el servicio en la nube se utilizan protocolos de datos propietarios, el dueño del dispositivo o el usuario podrían quedar atados a un servicio en la nube específico, lo que limitaría o impediría el uso de proveedores de servicios alternativos. Esto generalmente se conoce como "dependencia de un proveedor" (*vendor lock-in*), un término que abarca otras facetas de la relación con el proveedor, como por ejemplo la propiedad y el acceso a los datos. A la vez, los usuarios generalmente pueden confiar en que los dispositivos diseñados para su plataforma específica se podrán integrar.

FIGURA 2

Diagrama del modelo de comunicación dispositivo a la nube



FUENTE: Tschofenig, H., et.al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. IAB, marzo de 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt.

Modelo 'dispositivo a puerta de enlace'

En el modelo dispositivo a puerta de enlace, o más generalmente el modelo dispositivo a puerta de enlace de capa de aplicación (ALG), el dispositivo de la IoT se conecta a través de un servicio ALG como una forma de llegar a un servicio en la nube. Dicho de otra manera, esto significa que hay un software de aplicación corriendo en un dispositivo de puerta de enlace local, que actúa como intermediario entre el dispositivo y el servicio en la nube y provee seguridad y otras funcionalidades tales como traducción de protocolos o datos. Este modelo se ilustra en la Figura 3.

En los dispositivos de consumo se utilizan diferentes formas de este modelo. En muchos casos, el dispositivo de puerta de enlace local es un teléfono inteligente con una aplicación para comunicarse con un dispositivo y transmitir datos a un servicio en la nube. Esto suele ser el modelo empleado con los artículos de consumo populares como los dispositivos utilizados para llevar registro de la actividad física. Estos dispositivos no tienen capacidad nativa para conectarse directamente a un servicio en la nube, por lo que muchas veces utilizan una aplicación para teléfono inteligente como puerta de enlace intermedia.

Otra forma de este modelo tipo dispositivo a puerta de enlace es la aparición de dispositivos "hub" en las aplicaciones de automatización del hogar. Se trata de dispositivos que sirven de puerta de enlace local entre los dispositivos individuales de la IoT y un servicio en la nube, pero que también pueden reducir los problemas de interoperabilidad entre los propios dispositivos. Por ejemplo, el hub *SmartThings* es un dispositivo de puerta de enlace independiente que tiene instalados transceptores Z-Wave y *Zigbee* para comunicarse con ambas familias de dispositivos.[47] Luego se conecta al servicio en la nube *SmartThings* y permite que el usuario acceda a los dispositivos usando una aplicación

para teléfono inteligente y una conexión a Internet.

Desde una perspectiva técnica más amplia, el artículo del IETF Journal explica las ventajas del enfoque dispositivo a puerta de enlace:

> Este modelo de comunicación se usa en situaciones donde los objetos pequeños deben interoperar con dispositivos que no utilizan el protocolo de Internet. A veces se adopta este enfoque para integrar dispositivos que solo soportan IPv6, lo que significa que se necesita una puerta de enlace para los dispositivos y servicios existentes que solo soportan IPv4.[48]

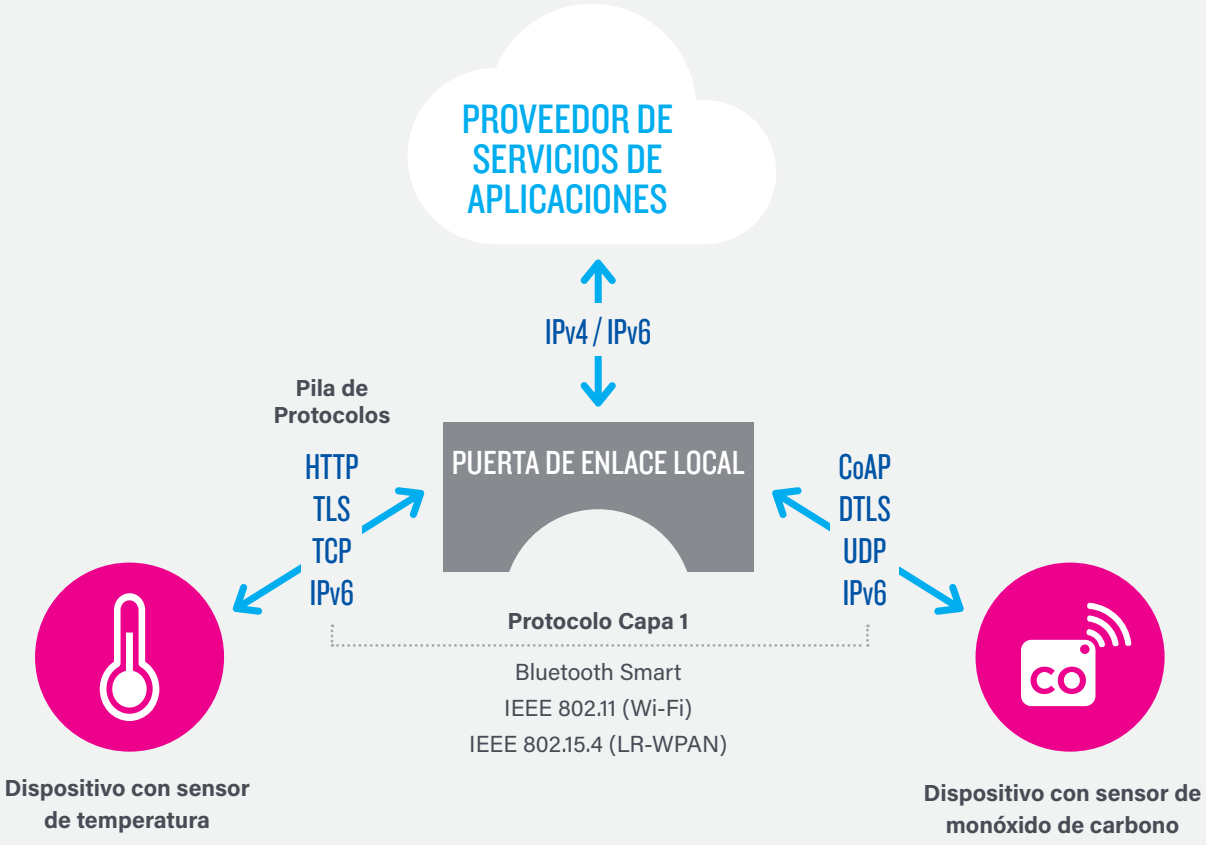
En otras palabras, este modelo de comunicación se suele utilizar para integrar nuevos dispositivos inteligentes en un sistema heredado con dispositivos que no son interoperables de forma nativa. Una desventaja de este enfoque es el costo y la complejidad que implican el desarrollo del software y el sistema para la puerta de enlace de capa de aplicación.

La RFC7452 del IAB sugiere una perspectiva para este modelo:

> Se anticipa que en el futuro se desplegarán más puertas de enlace genéricas con menores costos e infraestructura menos compleja para los consumidores finales, las empresas y los entornos industriales. La existencia de tales puertas de enlace será más probable si el diseño de los dispositivos de la IoT utiliza protocolos de Internet genéricos y no requiere puertas de enlace de capa de aplicación para traducir un protocolo

FIGURA 3

Ejemplo del modelo de comunicación de 'dispositivo a puerta de enlace'



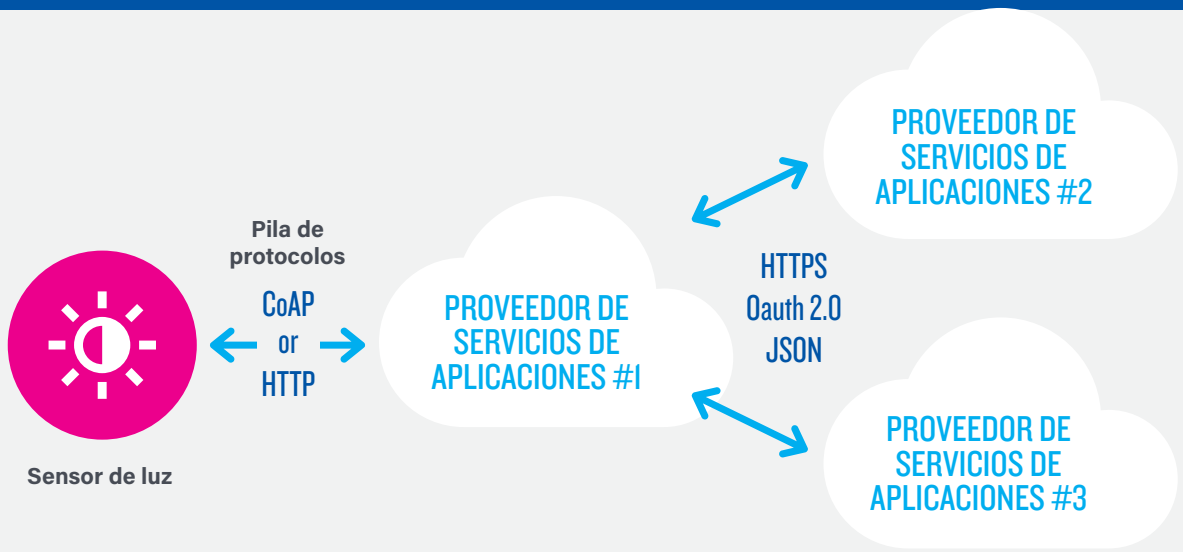
FUENTE: Tschofenig, H., et.al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. IAB, marzo de 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt.

> de capa de aplicación a otro. En general, el uso de puertas de enlace de capa de aplicación llevará a un despliegue más frágil, como ya se ha observado en el pasado...[49]

Los sistemas que utilizan el modelo de comunicación dispositivo a puerta de enlace y su papel más amplio en el abordaje de los problemas de interoperabilidad entre dispositivos de la IoT todavía están evolucionando.

FIGURA 4

Diagrama del modelo de intercambio de datos a través del back-end.



FUENTE: Tschofenig, H., et.al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. IAB, marzo de 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt.

Modelo de intercambio de datos a través del back-end

El modelo de intercambio de datos a través del *back-end* se refiere a una arquitectura de comunicación que permite que los usuarios exporten y analicen datos de objetos inteligentes de un servicio en la nube en combinación con datos de otras fuentes. Esta arquitectura soporta "el deseo del usuario de permitir que terceros accedan a los datos subidos por sus sensores".[50] Este enfoque es una extensión del modelo de comunicación tipo 'dispositivo único a la nube', que puede llevar a la existencia de silos de datos donde "los dispositivos de la IoT suben datos a un único proveedor de servicios de aplicaciones".[51] Una arquitectura de intercambio de datos a través del *back-end* permite agregar y analizar los datos recogidos de flujos obtenidos de un solo dispositivo de la IoT.

Por ejemplo, a un usuario corporativo a cargo de un complejo de oficinas le interesaría consolidar y analizar los datos de consumo de energía y otros servicios que producen todos los sensores de la IoT y los correspondientes sistemas habilitados para Internet disponibles en las instalaciones. En el modelo 'dispositivo único a la nube', muchas veces los datos que produce cada sensor o sistema de la IoT queda en un silo de datos independiente. Una arquitectura eficaz de intercambio de datos a través del *back-end* permitiría que la empresa acceda y analice fácilmente, en la nube, los datos producidos por

toda la gama de dispositivos instalados en el edificio. Además, este tipo de arquitectura facilita la portabilidad de los datos. Las arquitecturas eficaces de intercambio de datos a través del *back-end* permiten que los usuarios muevan sus datos al cambiar de servicio de IoT, rompiendo así las barreras tradicionales de los silos de datos.

El modelo de intercambio de datos a través del *back-end* sugiere que, para lograr la interoperabilidad de los datos de dispositivos inteligentes alojados en la nube, se requiere un enfoque de servicios federados[52] o interfaces de programación de aplicaciones (APIs) en la nube.[53] La Figura 4 muestra una representación de este diseño.

Este modelo de arquitectura es un enfoque para lograr interoperabilidad entre estos sistemas de *back-end*. Como sugiere el *IETF Journal*, "los protocolos estándares pueden ayudar, pero no son suficientes para eliminar los silos de datos dado que entre proveedores son necesarios modelos de información comunes."[54] En otras palabras, este modelo de comunicación es apenas tan eficaz como los diseños de los sistemas subyacentes de la IoT. Las arquitecturas de intercambio de datos a través del *back-end* no pueden superar completamente los diseños de los sistemas cerrados.

Modelos de comunicación de la Internet de las Cosas: resumen

Los cuatro modelos básicos de comunicación muestran las estrategias de diseño subyacentes utilizadas para permitir que los dispositivos de la IO se comuniquen. Además de ciertas consideraciones técnicas, el uso de estos modelos está influenciada en gran parte por la naturaleza abierta versus propietaria de los dispositivos de la IoT que se conectan en red. En el caso del modelo 'dispositivo a puerta de enlace', su principal característica es la capacidad de superar las restricciones que implica la conexión de dispositivos propietarios a la IoT. Esto significa que la interoperabilidad de los dispositivos y los estándares abiertos son consideraciones clave para el diseño y el desarrollo de sistemas de la Internet de las Cosas interconectados.

Desde el punto de vista del usuario en general, estos modelos de comunicación sirven para ilustrar la capacidad de agregar valor que tienen los dispositivos conectados en red. Al permitir que el usuario logre un mejor acceso a un dispositivo de la IoT y a sus datos, el valor global del dispositivo aumenta. Por ejemplo, en tres de los cuatro modelos de comunicación descritos, en última instancia los dispositivos se conectan a servicios de análisis de datos en un entorno de cómputo en la nube. Al crear conductos para comunicar datos a la nube, los usuarios y los proveedores de servicios pueden agregar los datos, analizar grandes volúmenes de datos y visualizar datos más fácilmente; además, las tecnologías de análisis predictivo obtienen más valor de los datos de la IoT del que pueden obtener las aplicaciones de silos de datos tradicionales. En otras palabras, las arquitecturas de comunicación eficaces son un importante generador de valor para el usuario final, ya que abren la posibilidad de utilizar la información de formas nuevas. Sin embargo, cabe señalar que estos beneficios no vienen sin desventajas. Al considerar una arquitectura determinada, es necesario considerar cuidadosamente los costos que deben incurrir los usuarios para conectarse a recursos en la nube, especialmente en las regiones donde los costos de conectividad del usuario son elevados.

Los modelos de comunicación efectivos benefician al usuario final, pero también cabe mencionar que los modelos eficaces de comunicación de la IoT también mejoran la innovación técnica y las oportunidades para el crecimiento comercial. Se pueden diseñar nuevos productos y servicios que aprovechen los flujos de datos de la IoT que antes no existían, y estos podrían catalizar la innovación.

CASILLA 3

IPv6 Y LA INTERNET DE LAS COSAS

Aunque difieren en cuanto a las cifras exactas, la mayoría de los observadores coincide en que, de aquí al año 2025, se conectarán a Internet miles de millones de nuevos dispositivos —desde sensores industriales hasta electrodomésticos y vehículos—. La Internet de las Cosas continúa creciendo y los dispositivos que requieren conectividad a Internet verdaderamente de extremo a extremo ya no podrán confiar en IPv4, el protocolo que hoy en día utiliza la mayor parte de los servicios de Internet. Estos dispositivos necesitarán una nueva tecnología: IPv6.

IPv6 es una actualización largamente esperada del protocolo original de Internet —el Protocolo de Internet o Protocolo IP—, que soporta todas las comunicaciones a través de Internet. IPv6 es necesario debido a que Internet se está quedando sin direcciones IPv4 originales. Mientras que IPv4 puede soportar 4300 millones de dispositivos conectados a Internet, IPv6 soporta 2128 direcciones, por lo que, a efectos prácticos, es inagotable. Esto representa alrededor de 3.4 × 1038 direcciones, que satisfacen sobradamente la demanda de los 100 mil millones de dispositivos de la IoT que se estima entrarán en servicio en las próximas décadas.

Dada la longevidad que se estima tendrán algunos de los sensores y otros dispositivos pensados para la Internet de las Cosas, las decisiones de diseño afectarán la utilidad de las soluciones por varias décadas. Los principales desafíos para los desarrolladores de la IoT son que IPv6 no es interoperable con IPv4 en forma nativa y que la mayor parte del software de bajo costo fácilmente disponible para embeber dispositivos de la IoT solo implementa IPv4. Sin embargo, muchos expertos creen que IPv6 es la mejor opción de conectividad y permitirá que la IoT realice su potencial.

Para obtener más información sobre IPv6, visite las páginas de recursos de la Internet Society disponibles en http://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6 y http://www.internetsociety.org/deploy360/ipv6/

NOTAS DE LA SECCIÓN

¿Qué es la Internet de las Cosas?

12. Ashton estaba trabajando en dispositivos RFID (identificación por radiofrecuencia) y la estrecha asociación entre estos sistemas y otras redes de sensores con el desarrollo del concepto de la IoT se refleja en el nombre de la compañía de dispositivos RFID a la que Ashton se unió más adelante: "ThingMagic."

13. "Radio-Frequency Identification." *Wikipedia, the Free Encyclopedia*, 6 de septiembre de 2015. https://en.wikipedia.org/wiki/Radio-frequency_identification

14. "Machine to Machine." *Wikipedia, the Free Encyclopedia*, 20 de agosto de 2015. https://en.wikipedia.org/wiki/Machine_to_machine

15. Polsonetti, Chantal. "Know the Difference Between IoT and M2M." *Automation World*, 15 de julio de 2014. http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m

16. "The Internet Toaster." Living Internet, 7 de enero de 2000. Web. 6 de septiembre 2015. http://www.livinginternet.com/i/ia_myths_toast.htm

17. "The "Only" Coke Machine on the Internet." Carnegie Mellon University Computer Science Department, n.d. Web. 6 de septiembre de 2015. https://www.cs.cmu.edu/~coke/history_long.txt

18. Stafford-Fraser, Quentin. "The Trojan Room Coffee Pot." N.p., mayo de 1995. Web. 6 de septiembre 2015. http://www.cl.cam.ac.uk/coffee/qsf/coffee.html

19. RFC 7452, "Architectural Considerations in Smart Object Networking" (marzo de 2015), https://tools.ietf.org/html/rfc7452

20. Otros puntos de vista sobre las tendencias de mercado convergentes que están impulsando el crecimiento de la IoT' incluyen el artículo "The IoT will be as fundamental as the Internet itself" de Susan Conant, disponible en http://radar.oreilly.com/2015/06/the-iot-will-be-as-fundamental-as-the-internet-itself.html y la declaración de Intel Corporation durante la audiencia de Cámara de Representantes sobre la IoT, disponible en http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-Wstate-SchoolerR-20150324.pdf.

21. La Ley de Moore tomó su nombre de Gordon Moore, pionero en el estudio de los semiconductores, quien observó que en los circuitos integrados el número de transistores por pulgada cuadrada se duplica aproximadamente cada dos años, lo que permite colocar mayor potencia de cálculo en chips cada vez más pequeños.

22. El lector encontrará una discusión sobre el uso de energía de los dispositivo para Internet y la computación de baja potencia en la conferencia presentada por Jon Koomey durante la cumbre "How green is the Internet?", disponible en https://www.youtube.com/embed/O8-LDLyKaBM

23. Además de otros avances técnicos, la miniaturización de los dispositivos electrónicos también es impulsada por la ley de Moore.

24. Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015. p.3. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

25. *Ibid*.

26. Cicciari, Matt. "What's Missing from the Industrial Internet of Things Conversation? Software." *Wired*. http://www.wired.com/insights/2014/11/industrial-internet-of-things-software/

27. "Internet of Things: Wearables." Application Developers Alliance. http://www.appdevelopersalliance.org/internet-of-things/wearables/

28. Baguley, Richard, and Colin McDonald. "Appliance Science: The Internet of Toasters (and Other Things)." CNET, 2 de marzo

de 2015. http://www.cnet.com/news/appliance-science-the-internet-of-toasters-and-other-things/

29. "IEEE Smart Cities." IEEE, 2015. Web. 6 de septiembre de 2015. http://smartcities.ieee.org/

30. "Cisco Visual Networking Index: Forecast and Methodology, 2014-2019." Cisco, 27 de mayo de 2015. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf

31. "History of the Internet of Things-Postscapes." Postscapes, n.d. Web. 6 de septiembre de 2015. http://postscapes.com/internet-of-things-history

32. Si desea leer una discusión más detallada sobre las características fundamentales de Internet y su arquitectura, consulte el trabajo de la Internet Society titulado "Internet Invariants: What Really Matters," disponible en http://www.internetsociety.org/internet-invariants-what-really-matters

33. RFC 7452, "Architectural Considerations in Smart Object Networking" (marzo de 2015), https://tools.ietf.org/html/rfc7452

34. Thaler, Dave, Hannes Tschofenig, and Mary Barnes. "Architectural Considerations in Smart Object Networking." IETF 92 Technical Plenary - IAB RFC 7452. 6 de septiembre de 2015. Web. https://www.ietf.org/proceedings/92/slides/slides-92-iab-techplenary-2.pdf

35. "Int Area Wiki - Internet-of-Things Directorate." *IOTDirWiki*. IETF, n.d. Web. 6 de septiembre de 2015. http://trac.tools.ietf.org/area/int/trac/wiki/IOTDirWiki

36. "Overview of the Internet of Things." ITU, 15 de junio de 2012. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060

37. http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standards-next-steps

38. "Internet of Things." Oxford Dictionaries, n.d. Web. 6 de septiembre de 2015. http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things

39. Tschofenig, H., et. al., *Architectural Considerations in Smart Object Networking*. Tech. no. RFC 7452. Internet Architecture Board, marzo de 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt

40. Ver http://www.bluetooth.com and http://www.bluetooth.org

41. Ver http://www.z-wave.com

42. Ver http://www.zigbee.org

43. Duffy Marsan, Carolyn. "IAB Releases Guidelines for Internet-of-Things Developers." *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, julio de 2015. Web. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

44. "Meet the Nest Thermostat | Nest." Nest Labs. Web. 31 de agosto de 2015. https://nest.com/thermostat/meet-nest-thermostat/

45. "Samsung Privacy Policy--SmartTV Supplement." Samsung Corp. Web. 29 de septiembre de 2015. http://www.samsung.com/sg/info/privacy/smarttv.html

46. Duffy Marsan, Carolyn. "IAB Releases Guidelines for Internet-of-Things Developers." *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, julio de 2015. Web. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

47. "How It Works." *SmartThings*, 2015. http://www.smartthings.com/how-it-works

48. Duffy Marsan, Carolyn. "IAB Releases Guidelines for Internet-of-Things Developers." *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, julio de 2015. Web. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

49. *Tschofenig, H., et. al.,* p. 6.

50. *Tschofenig, H., et. al.,* p. 9.

51. *Ibid.*

52. Un enfoque de servicios federados en la nube es aquel que combina los recursos de diferentes proveedores de servicios de nube para satisfacer una necesidad de negocio más amplia.

53. Producida por ownCloud.org, OwnCloud es un ejemplo de una herramienta de nube federada lista para usar. https://owncloud.org/blog/faster-easier-file-sync-and-share-with-federated-self-hosted-owncloud-8-0/

54. *Duffy Marsan, Carolyn.* p.7

¿QUÉ TEMAS SE ESTÁN PLANTEANDO EN TORNO A LA INTERNET DE LAS COSAS?

Sería imposible abarcar el amplio espectro de temas relacionados con la Internet de las Cosas en un solo trabajo. No obstante, a continuación ofrecemos un resumen de cinco temas que surgen muy frecuentemente en relación con la IoT. Estos incluyen: la seguridad; la privacidad; la interoperabilidad y los estándares; aspectos legales, reglamentarios y de derechos; y las economías emergentes y el desarrollo.

SEGURIDAD PÁGINA 33

PRIVACIDAD PÁGINA 41

INTEROPERABILIDAD / ESTÁNDARES PÁGINA 48

CUESTIONES LEGALES, REGLAMENTARIAS Y DE DERECHOS PÁGINA 56

CUESTIONES RELACIONADAS CON LAS ECONOMÍAS EMERGENTES Y EL DESARROLLO PÁGINA 66

Comenzamos nuestro análisis de estos temas a través del lente de las "Capacidades", la declaración de principios fundamentales que guían el trabajo de ISOC en términos de las habilidades que creemos que todos los usuarios de Internet deben disfrutar y que se deben proteger. Estas incluyen la capacidad de ***conectarse***, ***hablar***, ***innovar***, ***compartir***, ***escoger*** y ***confiar***.[55] Con estos principios como guía, presentamos aspectos importantes de cada tema y planteamos diferentes temas para su debate.

55. "Values and Principles." Principles. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles

CUESTIONES RELACIONADAS CON LA SEGURIDAD

El desafío de seguridad de la IoT

Tal como se observa en los principios que guían nuestro trabajo, garantizar la seguridad, la confiabilidad, la resiliencia y la estabilidad de las aplicaciones y servicios de Internet es fundamental para fomentar la ***confianza*** y el uso de Internet.[56] Como usuarios de Internet, tenemos que tener un alto grado de confianza en que Internet, sus aplicaciones y los dispositivos conectados a la red son lo suficientemente seguros como para realizar en línea toda la gama de actividades que deseamos en relación con la tolerancia al riesgo asociado con tales actividades. En este sentido, la Internet de las cosas no es diferente y la seguridad de la IoT está fundamentalmente relacionada con la capacidad de los usuarios de confiar en su entorno. Si los usuarios no creen que los dispositivos que tienen conectados y su información están razonablemente seguros contra el mal uso o los daños, la erosión de la confianza resultante provoca una renuencia a usar Internet. Esto tiene consecuencias globales para el comercio electrónico, la innovación técnica, la libertad de expresión y prácticamente para todos los demás aspectos de las actividades en línea. En efecto, para garantizar la seguridad en los productos y servicios de la IoT, el sector debe considerar la seguridad como una de sus máximas prioridades.

A medida que conectamos cada vez más dispositivos a Internet, surgen nuevas oportunidades para explotar potenciales vulnerabilidades de seguridad. Los dispositivos de la IoT mal asegurados servir como puntos de entrada para ciberataques, permitiendo que personas malintencionadas reprogramaran un dispositivo o perjudicaran su funcionamiento. Los dispositivos de la IoT mal diseñados pueden exponer los datos de los usuarios a robos, dejando los flujos de usuarios sin una protección adecuada. Los dispositivos defectuosos o que no funcionan bien también pueden crear vulnerabilidades. Estos problemas son tanto o más graves en el caso de los dispositivos inteligentes pequeños, baratos y ubicuos en la Internet de las Cosas que en el caso de los equipos que tradicionalmente han sido los puntos extremos de la conectividad a Internet. Los desafíos que imponen la competitividad de los costos y las limitaciones técnicas de la IoT hacen que para los fabricantes de dispositivos no sea fácil diseñar funciones de seguridad adecuadas, potencialmente generando, a largo plazo, vulnerabilidades en la seguridad y dificultades en el mantenimiento superiores a las computadoras tradicionales.

Junto con posibles deficiencias en el diseño de la seguridad, el enorme aumento del número y la variedad de los dispositivos de la IoT podría aumentar las oportunidades de ataque. Sumado a la naturaleza altamente interconectada de los dispositivos de la IoT, cada dispositivo mal asegurado conectado en línea potencialmente afecta la seguridad y la resistencia de Internet a nivel global, no solo a nivel local. Por ejemplo, un refrigerador o un televisor sin protección infectado con malware que se encuentra en Estados Unidos pueden enviar miles de correos electrónicos no deseados dañinos a destinatarios de todo el mundo usando la conexión Wi-Fi de la casa.[57]

Para complicar todavía más las cosas, en un mundo hiperconectado, nuestra capacidad de funcionar diariamente sin dispositivos o sistemas conectados a Internet probablemente disminuirá. De hecho, es cada vez más difícil comprar ciertos dispositivos sin conexión a Internet, ya que algunos fabricantes solo ofrecen productos conectados. Cada vez estamos más conectados y dependemos más de los dispositivos de la IoT para muchos servicios esenciales, por lo que necesitamos que los dispositivos sean seguros. Pero también reconocemos que ningún dispositivo puede ser absolutamente seguro. Este creciente nivel de dependencia de los dispositivos de la IoT y de los servicios de Internet con los cuales interactúan también aumenta las formas que tienen los delincuentes para acceder a los dispositivos. Si se ven comprometidas en un ataque cibernético, quizá podríamos desenchufar nuestros televisores conectados a Internet, pero no es tan fácil apagar un medidor inteligente de energía eléctrica, un sistema de control de tráfico o un marcapasos si estos dispositivos son víctimas de un ataque malicioso.

Esta es la razón por la cual la seguridad de los dispositivos y servicios de la IoT debe ser un importante punto de discusión y un tema crítico. Dependemos cada vez más de estos dispositivos para servicios esenciales, por lo que su comportamiento puede tener un alcance y un impacto globales.

Cada dispositivo mal asegurado conectado en línea potencialmente afecta la seguridad y la resistencia de Internet a nivel global, no solo a nivel local.

Un espectro de consideraciones de seguridad

Al pensar en los dispositivos de la Internet de las Cosas, es importante entender que la seguridad de estos dispositivos no es absoluta. La seguridad de los dispositivos de la IoT no es una proposición binaria de tipo seguro/inseguro. Por el contrario, resulta útil conceptualizar la seguridad de la IoT como un espectro de vulnerabilidad los dispositivos. El espectro va desde dispositivos totalmente desprotegidos sin ninguna función de seguridad hasta sistemas muy seguros con múltiples capas de elementos de seguridad. En un constante juego de gato y ratón, a medida que las nuevas amenazas de seguridad evolucionan, los fabricantes de dispositivos y los operadores de redes responden para hacer frente a las nuevas amenazas.

La seguridad general y la resiliencia de la Internet de las Cosas dependen de cómo se evalúen y gestionen los riesgos de seguridad. La seguridad de un dispositivo es función del riesgo de que un dispositivo se vea comprometido, del daño que tal compromiso provocaría y del tiempo y los recursos necesarios para lograr cierto nivel de protección. Si un usuario no puede tolerar un alto grado de riesgo (por ejemplo, un operador de un sistema de control de tráfico o una persona a quien se le ha implantado un dispositivo médico que está conectado a Internet implantado), puede que para dicho usuario sienta que se justifica gastar una cantidad considerable de recursos para proteger el sistema o el dispositivo contra un ataque. Del mismo modo, si a la persona no le preocupa que su refrigerador pueda ser hackeado y utilizado para enviar spam, puede que no se sienta obligada a pagar por un modelo que tenga un diseño de seguridad más sofisticado si esto hace que el dispositivo sea más costoso o complicado.

En esta evaluación y cálculo de la mitigación de los riesgos influyen diferentes factores. Estos factores incluyen una comprensión clara de los riesgos de seguridad actuales y posibles riesgos futuros, la estimación de los costos económicos y otros tipos de daño si los riesgos se hacen realidad, y el costo estimado de la mitigación de los riesgos.[58] Si bien este tipo de concesiones de seguridad muchas veces se realizan desde la perspectiva de los usuarios individuales y las organizaciones, también es importante tener en cuenta la interrelación de los dispositivos de la IoT como parte de un ecosistema mayor. La conectividad en red de los dispositivos de la IoT significa que las decisiones de seguridad que se toman a nivel local con respecto a un dispositivo pueden tener impactos globales sobre otros dispositivos.

Como cuestión de principio, quienes desarrollan objetos inteligentes para la Internet de las Cosas tienen la obligación de garantizar que estos dispositivos no expongan los bienes de sus propios usuarios ni de otras personas a potenciales daños. Como cuestión de negocios y de economía, a los fabricantes desean reducir sus costos, su complejidad y su tiempo de comercialización. Por ejemplo, son cada vez más comunes los dispositivos de la IoT de alto volumen y bajo margen de ganancia y que ya representan un costo adicional para los productos en los que están embebidos; añadir más memoria y un procesador más rápido para implementar medidas de seguridad podría hacer que el producto ya no fuera competitivo.

En términos económicos, el resultado de la falta de seguridad en los dispositivos de la IoT es una externalidad negativa, donde una o más partes imponen un costo sobre otras. Un ejemplo clásico es la contaminación del medio ambiente, donde los costos de los daños y la limpieza (externalidades negativas) resultantes de las acciones de quien contamina son asumidos por otras partes. El hecho es que el costo de la externalidad impuesto a los demás normalmente no se considera en el proceso de toma de decisiones, a menos que, como es el caso de la contaminación, se aplique un impuesto que sirva de aliciente para reducir la contaminación. De acuerdo con Bruce Schneier,[59] en el caso de la seguridad de la información surge una externalidad cuando el proveedor que crea el producto no corre con los costos que ocasionan las potenciales inseguridades; en este caso, una ley de responsabilidad puede convencer a los vendedores para que tomen en cuenta la externalidad y desarrollen más productos de seguridad.

Estas consideraciones de seguridad no son nuevas en el contexto de la tecnología de la información, pero la magnitud de los desafíos que pueden surgir en las implementaciones de la IoT las vuelve extremadamente significativas. Estos desafíos se describen a continuación.

Desafíos de seguridad que son exclusivos de los dispositivos de la IoT

Las diferencias entre los dispositivos de la IoT y las computadoras y los dispositivos informáticos tradicionales suelen desafiar la seguridad:

Muchos dispositivos de la Internet de las Cosas (por ejemplo, los sensores y los artículos de consumo) están diseñados para ser desplegados a una escala masiva que es varios órdenes de magnitud superior a la de los dispositivos tradicionalmente conectados a Internet. Por consiguiente, la potencial cantidad de enlaces interconectados entre estos dispositivos no tiene precedentes. Además, muchos de estos dispositivos podrán establecer enlaces y comunicarse con otros dispositivos por sí mismos, de manera impredecible y dinámica. Por lo tanto, puede ser necesario considerar nuevamente las herramientas, métodos y estrategias existentes asociadas con la seguridad de la IoT.

Muchos despliegues de la IoT consistirán en colecciones de dispositivos idénticos o prácticamente idénticos. Esta homogeneidad amplifica el potencial impacto de cualquier vulnerabilidad de seguridad simplemente por la gran cantidad de dispositivos que tienen las mismas características. Por ejemplo, una vulnerabilidad en el protocolo de comunicación de una marca de bombillas de luz conectadas a Internet se podría extender a todas las marcas y modelos de dispositivos que utilizan el mismo protocolo o que comparten características clave de diseño o fabricación.

Muchos de los dispositivos de la Internet las Cosas que se van a desplegar tendrán una vida útil anticipada muy superior a la que típicamente se espera para los equipos de alta tecnología. Además, estos dispositivos se podrían desplegar en circunstancias que los harían difíciles o imposibles de reconfigurar o actualizar; o bien estos dispositivos podrían sobrevivir a la empresa que los creó, lo que los dejaría huérfanos y sin apoyo a largo plazo. Estos escenarios ilustran que los mecanismos de seguridad que son adecuados en el momento del despliegue podrían no ser adecuados durante toda la vida útil del dispositivo y a medida que las amenazas a la seguridad evolucionen. Esta situación podría crear vulnerabilidades que podrían persistir por mucho tiempo. Esto contrasta con el paradigma de los sistemas de computadoras tradicionales en los cuales normalmente se aplican actualizaciones al sistema operativo durante toda la vida de servicio de los equipos para hacer frente a las amenazas de seguridad. El apoyo y la gestión a largo plazo de los dispositivos de la IoT representa un importante reto de seguridad.

Muchos dispositivos de la IoT estén diseñados intencionadamente sin ninguna posibilidad de actualización; en otros, el proceso de actualización es engorroso o poco práctico. Por ejemplo, consideremos el retiro de 1.4 millones de automóviles Fiat Chrysler 2015 para arreglar una vulnerabilidad que potencialmente permitiría hackear el vehículo en forma inalámbrica. Estos vehículos se deben llevar a un concesionario Fiat Chrysler para que les realicen una actualización manual del software, o bien los propietarios deben actualizar el software por sí mismos usando una memoria USB. La realidad es que un alto porcentaje de estos automóviles probablemente no se actualizará porque el proceso de actualización representa un inconveniente para los propietarios, y esto los deja permanentemente vulnerables a las amenazas de seguridad cibernética, sobre todo porque el automóvil parece estar funcionando muy bien.

Muchos dispositivos de la IoT funcionan de modo que es escasa o nula la visibilidad que tiene el usuario de su funcionamiento interno o de los flujos de datos que producen. Si un usuario cree que un dispositivo está ejecutando ciertas funciones pero en realidad está ejecutando funciones no deseadas o recogiendo más información que lo que el usuario desea, se crea una vulnerabilidad. Las funciones del dispositivo también podrían cambiar sin previo aviso cuando el fabricante ofrece una actualización, lo que deja al usuario vulnerable a cualquier cambio que realice el fabricante.

Algunos dispositivos de la IoT probablemente serán ser desplegados en lugares donde sea difícil o imposible lograr la seguridad física. Los

atacantes pueden tener acceso físico directo a los dispositivos. Para garantizar la seguridad será necesario considerar el uso de protección contra manipulaciones y otras innovaciones de diseño.

Al igual que muchos sensores ambientales, algunos dispositivos de la IoT han sido diseñados para ser integrados discretamente en su entorno, donde los usuarios apenas se den cuenta de su presencia o monitoreen su funcionamiento. Además, los dispositivos pueden no tener una forma clara de alertar al usuario cuando surge un problema de seguridad, por lo que es difícil para un usuario saber que la seguridad de un dispositivo de la IoT ha sido vulnerada. Esta situación podría persistir por mucho tiempo antes de ser detectada y corregida; incluso podría darse el caso de que no fuera posible o práctico implementar una corrección o mitigación. Del mismo modo, el usuario podría no ser consciente de que existe un sensor en su entorno, por lo que potencialmente un fallo de seguridad podría persistir por mucho tiempo sin ser detectado.

Los primeros modelos de la Internet de las Cosas asumen que la IoT será producto de grandes empresas de tecnología privadas y/o públicas. Sin embargo, en el futuro "construir su propia Internet de las Cosas" (*Build Your own Internet of Things, BYIoT*) podría convertirse en algo habitual, como lo demuestra el crecimiento de las comunidades de desarrolladores de *Arduino y Raspberry Pi*.[60] Estos despliegues podrán o no aplicar los estándares de mejores prácticas de seguridad de la industria.

Preguntas relacionadas con la seguridad de la IoT

Se ha planteado una serie de preguntas con respecto a los problemas de seguridad que plantea la Internet de las Cosas. Muchas de estas preguntas ya existían antes del crecimiento de la IoT, pero su importancia ha aumentado debido a la magnitud del despliegue de los dispositivos utilizados. Entre las preguntas más importantes podemos mencionar las siguientes:

BUENAS PRÁCTICAS DE DISEÑO

¿Cuáles son las mejores prácticas que los ingenieros y desarrolladores deben utilizar al diseñar dispositivos de la IoT para que sean más seguros? ¿Cómo se recogen y transmiten las lecciones aprendidas a partir de los problemas de seguridad de la Internet de las Cosas a las comunidades de desarrolladores para mejorar las futuras generaciones de dispositivos? ¿Qué formación y recursos educativos se pueden utilizar para enseñar a los ingenieros y desarrolladores cómo diseñar una IoT más segura?

EQUILIBRIO ENTRE COSTO Y SEGURIDAD

¿De qué manera las partes interesadas toman decisiones informadas con respecto a los dispositivos de la Internet de las Cosas considerando la relación costo-beneficio? ¿Cómo se pueden cuantificar y evaluar con precisión los riesgos de seguridad? ¿Qué motivará a los diseñadores y fabricantes de dispositivos para que acepten el costo adicional que implica el diseño de dispositivos más seguros, y, en particular, para que asuman la responsabilidad por el impacto de cualquier externalidad negativa derivada de sus decisiones de seguridad? ¿Cómo se van a conciliar las incompatibilidades entre la funcionalidad y la facilidad de uso y la seguridad? ¿Cómo nos aseguramos de que las soluciones de seguridad para la IoT soporten oportunidades para la innovación, sociales y de crecimiento económico?

ESTÁNDARES E INDICADORES

¿Qué papel desempeñan los estándares técnicos y operativos en el desarrollo y despliegue de dispositivos de la IoT seguros y de buen funcionamiento? ¿Cómo se pueden identificar y medir las características de seguridad de los dispositivos de la IoT? ¿Cómo se puede medir la efectividad de las iniciativas y medidas de seguridad en la Internet de las Cosas? ¿Cómo se puede asegurar la implementación de las mejores prácticas de seguridad?

CONFIDENCIALIDAD DE LOS DATOS, AUTENTICACIÓN Y CONTROL DE ACCESO

Cuál es el papel óptimo del cifrado de los datos con respecto a los dispositivos de la IoT? ¿Utilizar tecnologías de cifrado, autenticación y control de acceso en los dispositivos de la IoT es una solución adecuada para evitar intentos de espionaje y secuestro de los flujos de datos que producen estos dispositivos? ¿Qué tecnologías de cifrado y autenticación se podrían adaptar para la Internet de las Cosas y cómo se podrían aplicar considerando las limitaciones de costo, tamaño y velocidad de procesamiento de los dispositivos de la IoT? ¿Cuáles son los problemas de gestión que se espera deberán ser abordados como resultado del cifrado a una escala de la magnitud de la IoT? ¿Se están abordando las preocupaciones con respecto a cómo gestionar el ciclo de vida de las claves criptográficas y el período durante el cual se espera que un algoritmo dado permanezca seguro? ¿Los procesos de extremo a extremo son lo suficientemente seguros y simples como para que los utilicen los usuarios típicos?

CAPACIDAD DE ACTUALIZACIÓN EN CAMPO

Dado que se espera que muchos de los dispositivos de la IoT tendrán una vida útil prolongada, ¿estos dispositivos deben diseñarse considerando su mantenimiento y su capacidad de actualización in situ de modo que puedan adaptarse a las nuevas amenazas a la seguridad? Si cada dispositivo tiene integrado un agente de gestión de dispositivos, en los dispositivos de la IoT se podría instalar y configurar nuevos software. Pero los sistemas de gestión aumentan los costos y la complejidad; ¿habrá otros enfoques para actualizar el software de los dispositivos que sean más compatibles con el uso masivo de los dispositivos de la IoT? ¿Existe alguna clase de dispositivos de bajo riesgo y que por lo tanto no justifique este tipo de características? En general, ¿las interfaces de usuario de los dispositivos de la IoT (por lo general mínimas) se están analizando adecuadamente, tomando en cuenta la gestión de los dispositivos (por parte de cualquier persona, incluso por el usuario)?

RESPONSABILIDAD COMPARTIDA

¿Cómo se puede fomentar la responsabilidad compartida y la colaboración entre todas las partes interesadas en pos de la seguridad de la IoT?

REGULACIÓN

¿Se debe sancionar a los fabricantes de dispositivos por la venta de software o hardware con fallos de seguridad conocidas o desconocidas? ¿Cómo se podrían adaptar o ampliar las leyes de responsabilidad de producto y protección del consumidor para que abarquen las externalidades negativas relacionadas con la Internet de las Cosas? ¿Sería posible hacerlo en un entorno transfronterizo? ¿La regulación podrá seguir el ritmo y mantener su eficacia en vista de evolución de la tecnología de la IoT y la evolución de las amenazas a la seguridad? ¿Cómo se debe equilibrar la regulación con las necesidades de la innovación sin pedir permiso, la libertad en Internet y la libertad de expresión?

OBSOLESCENCIA DE LOS DISPOSITIVOS

¿Qué enfoque se debe adoptar con respecto a los dispositivos de la IoT obsoletos a medida que Internet evoluciona y cambian las amenazas a la seguridad? ¿Se debe exigir que los dispositivos de la IoT tengan una funcionalidad de "final de vida" integrada que los inactive? En el futuro, este tipo de requisito podría obligar a sacar de servicio a los dispositivos más antiguos que no son interoperables y a reemplazarlos por dispositivos más seguros e interoperables. Esto ciertamente sería muy difícil en un mercado abierto. ¿Qué implicancias tiene la inactivación automática de los dispositivos de la IoT?

La amplitud de estas preguntas es representativo de la variedad de las consideraciones de seguridad asociadas con los dispositivos de la Internet de las Cosas. Sin embargo, es importante recordar que, cuando un dispositivo está en Internet también es parte de Internet,[61] lo que significa que solo se pueden lograr soluciones de seguridad eficaces y apropiadas si todas las partes involucradas con estos dispositivos aplican un enfoque de seguridad colaborativo.[62]

Tanto entre la industria como entre los gobiernos y las autoridades públicas, el modelo colaborativo aparece como un enfoque eficaz para ayudar a asegurar a Internet y al ciberespacio, incluso a la Internet de las Cosas. Este modelo incluye una serie de prácticas y herramientas que incluyen el intercambio de información bidireccional y voluntario, herramientas de aplicación eficaces, preparación para incidentes y ejercicios cibernéticos, creación de conciencia y capacitación, acuerdo sobre las normas de comportamiento internacionales, y desarrollo y reconocimiento de prácticas y estándares internacionales. Es necesario continuar trabajando para que sigan evolucionando los enfoques colaborativos y basados en la gestión de riesgos, de manera de lograr que se adapten bien a la escala y la complejidad de los desafíos de seguridad de los dispositivo de la Internet de las Cosas del futuro.

NOTAS DE LA SECCIÓN

Cuestiones relacionadas con la seguridad

56. *Ibid.*

57. Starr, Michelle. "Fridge Caught Sending Spam Emails in Botnet Attack - CNET." CNET, 19 de enero de 2014. http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

58. Varias organizaciones han desarrollado guías para la evaluación de riesgos. Por ejemplo, en 2012 el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) emitió una serie de directrices, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091, mientras que la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) publicaron la norma ISO/IEC 31010:2009 "Gestión de riesgos – Técnicas de evaluación de riesgos". http://www.iso.org/iso/catalogue_detail?csnumber=51073

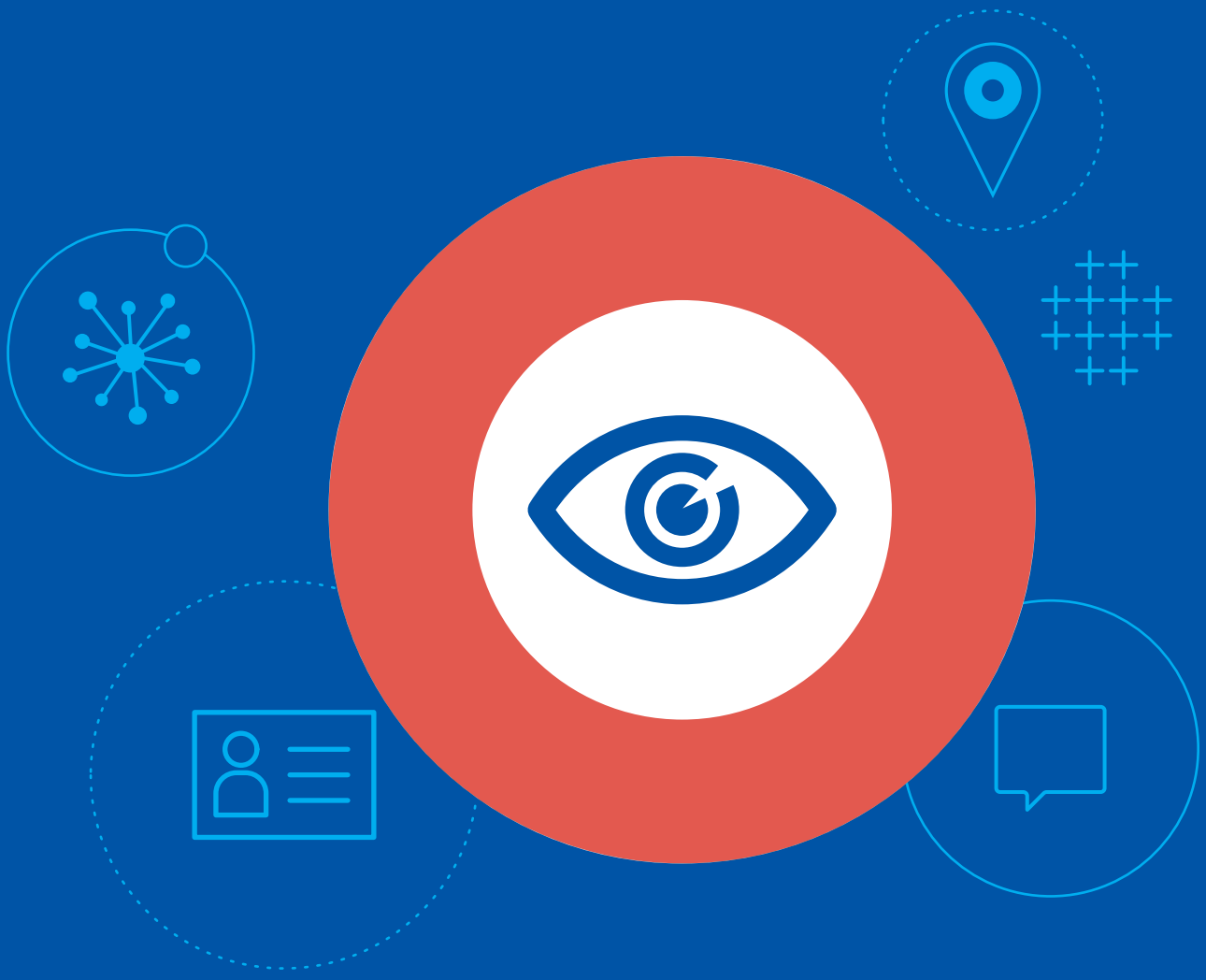
59. El artículo de Bruce Schneider está disponible el siguiente enlace: https://www.schneier.com/essays/archives/2007/01/information_security_1.html

60. Ver también la comunidad de código abierto Arduino http://www.arduino.cc y la Fundación Raspberry Pi http://www.raspberrypi.org/

61. Kolkman, Olaf. "Introducing Collaborative Security, Our Approach to Internet Security Issues." Web log post. Internet Society, 13 de abril de 2015. http://www.internetsociety.org/blog/public-policy/2015/04/introducing-collaborative-security-our-approach-internet-security-issues

62. *Collaborative Security: An Approach to Tackling Internet Security Issues*. Internet Society, abril de 2015. http://www.internetsociety.org/collaborativesecurity

CONSIDERACIONES SOBRE LA PRIVACIDAD



Antecedentes de la privacidad en la Internet de las Cosas

El respeto por las expectativas y los derechos de privacidad es fundamental para asegurar la ***confianza*** en Internet; además, también afecta la capacidad de las personas de ***hablar***, ***conectarse*** y ***escoger*** de formas significativas. Estos derechos y expectativas se suelen enmarcar en términos del manejo ético de los datos,[63] que hace hincapié en la importancia de respetar las expectativas de privacidad del individuo y el uso legítimo de sus datos. La Internet de las Cosas puede desafiar estas tradicionales expectativas de privacidad.

Es fundamental abordar estos tipos de problemas de privacidad, dado que tienen implicaciones sobre nuestros derechos básicos y nuestra capacidad colectiva de confiar en Internet.

La IoT suele referirse a una amplia red de dispositivos con sensores diseñados para recopilar datos acerca de su entorno, que muchas veces incluyen datos relacionados con las personas. Estos datos presumiblemente proporcionan un beneficio al propietario del dispositivo, pero muchas veces también benefician al fabricante o proveedor. La recopilación y el uso de los datos se convierte en una consideración de privacidad cuando las expectativas de privacidad de quienes son observados por los dispositivos de la IoT difieren de las de quienes recogerán y usarán estos datos.

También hay combinaciones de flujos de datos de la IoT aparentemente inocentes que también pueden poner en riesgo la privacidad. Cuando se combinan o correlacionan flujos de datos individuales, el retrato digital que se obtiene de las personas suele ser más invasivo que el que es puede obtener a partir de un flujo de datos individual. Por ejemplo, un cepillo de dientes con conexión a Internet puede recoger y transmitir información sobre los hábitos de cepillado de una persona, algo bastante inocuo. En cambio, si el refrigerador de este mismo usuario informa el listado de los alimentos que consume, y si además el dispositivo que el usuario utiliza para llevar cuenta de su actividad física también informa los datos correspondientes, la combinación de estos flujos de datos pinta una descripción mucho más detallada y privada de la salud general de la persona. Este efecto de agregación de los datos puede ser particularmente potente en el caso de los dispositivos de la IoT, dado que muchos producen otros metadatos como por ejemplo marcas de tiempo e información de geolocalización, lo que aumenta aún más la especificidad del usuario.

En otras situaciones, el usuario puede no ser consciente de que un dispositivo está recogiendo datos sobre su persona y potencialmente compartiéndolos con terceros. Este tipo de recolección de datos es cada vez más frecuente en los dispositivos de consumo, como por ejemplo en los televisores inteligentes y las consolas de videojuegos. Este tipo de productos tienen características de reconocimiento de voz o de visualización que permanentemente escuchan las conversaciones u observan la actividad en una habitación y selectivamente transmiten los datos recogidos a un servicio en la nube para su procesamiento, donde a veces participa un tercero. Una persona podría estar en presencia de este tipo de dispositivos sin saber que sus conversaciones o actividades están siendo monitoreadas o que sus datos están siendo registrados. Estos tipos de características pueden ser de beneficio para un usuario informado, pero pueden plantear un problema de privacidad para quienes no son conscientes de la presencia de estos dispositivos y no pueden influir significativamente sobre la forma en que se utiliza la información recogida.

Sin importar si el usuario está al tanto de que los dispositivos de la IoT recogen y analizan sus datos, estas situaciones ponen de relieve el valor que tienen estos flujos de datos personalizados para empresas y organizaciones que buscan recoger y sacar provecho de la información obtenida a través de la Internet de las Cosas. La demanda de esta información deja al descubierto los desafíos legales y regulatorios que enfrentan las leyes de protección de datos y privacidad.

Es fundamental abordar estos tipos de problemas de privacidad, dado que tienen implicaciones sobre nuestros derechos básicos y nuestra

capacidad colectiva de confiar en Internet. Desde una perspectiva más amplia, las personas reconocen que su privacidad es un valor intrínseco y tienen expectativas con respecto a los datos personales que se pueden recoger y cómo estos datos pueden ser utilizados por terceros. Esta noción general acerca de la privacidad también vale para los datos recogidos por los dispositivos de la Internet de las Cosas, pero estos dispositivos pueden socavar la capacidad del usuario de expresar y hacer cumplir sus preferencias de privacidad. Si el hecho de que sus preferencias de privacidad no sean respetadas por la Internet de las Cosas hace que los usuarios pierdan su confianza en Internet, entonces podría disminuir el mayor valor que tiene la Internet.

Aspectos relacionados con la privacidad que solo se aplican a la Internet de las Cosas

En general, la forma en que la Internet de las Cosas aumenta la viabilidad y el alcance de la vigilancia y el seguimiento amplifica las preocupaciones relativas a la privacidad. Las características de los dispositivos d la IoT y las formas en que se utilizan redefinen el debate sobre los temas de privacidad, ya que modifican drásticamente cómo se recogen, analizan, utilizan y protegen los datos personales. Por ejemplo:

El tradicional modelo de privacidad de "notificación y consentimiento" en que los usuarios hacen valer sus preferencias de privacidad interactuando directamente con información que aparece en la pantalla de una computadora o dispositivo móvil (por ejemplo, haciendo clic en "Acepto") deja de funcionar cuando los sistemas no le ofrecen al usuario ningún mecanismo de interacción. Muchas veces los dispositivos de la IoT no tienen una interfaz de usuario para configurar las preferencias de privacidad, y en muchas configuraciones los usuarios no tienen conocimiento ni controlan la forma en que se recogen y utilizan sus datos personales. Esto provoca una brecha entre las preferencias de privacidad del usuario y el comportamiento de recolección de datos del dispositivo. Si consideran que los datos recopilados no son datos personales, es posible que los proveedores de dispositivos de la IoT se sientan menos incentivados a ofrecer a los usuarios un mecanismo para que expresen sus preferencias de privacidad Sin embargo, la experiencia demuestra que, en realidad, los datos que tradicionalmente no se consideran personales podrían ser o convertirse en datos personales si se combinan con otros.

Suponiendo que se pudiera desarrollar un mecanismo eficaz que permitiera que un usuario expresara de manera informada sus preferencias de privacidad, este mecanismo debería poder manejar la gran cantidad de dispositivos de la IoT que debe controlar cada usuario. No es realista pensar que un usuario interactuará directamente con cada uno de los dispositivos con que se encuentre a lo largo del día para expresar sus preferencias de privacidad. Por el contrario, las interfaces de privacidad se deben poder escalar de acuerdo con el tamaño del problema, sin dejar de ser completas y prácticas desde la perspectiva del usuario.

La Internet de las Cosas puede poner en peligro las expectativas de los usuarios con respecto a la privacidad en situaciones comunes. Las normas sociales y expectativas de privacidad difieren en los espacios públicos

frente a los espacios privados; los dispositivos de la IoT desafían estas normas. Por ejemplo, las tecnologías de vigilancia que utiliza la IoT como las cámaras de vigilancia o los sistemas de trazabilidad de ubicación que normalmente funcionan en espacios públicos están migrando hacia espacios tradicionalmente privados como el hogar o los vehículos particulares, donde nuestras expectativas de privacidad son muy diferentes. Al hacerlo, desafían lo que muchas sociedades reconocen como el derecho a la privacidad en el hogar o los espacios privados. Además, las expectativas de las personas con respecto a su privacidad en los espacios que consideran públicos (parques, centros comerciales, estaciones de tren, etc.) también están siendo desafiadas por el aumento de la naturaleza y el alcance de la vigilancia en tales espacios.

Muchas veces los dispositivos de la IoT funcionan en contextos donde la proximidad expone a múltiples personas a una misma actividad de recolección de datos. Por ejemplo, el sensor de seguimiento por geolocalización de un automóvil podría registrar los datos de localización de todos los ocupantes del vehículo, sin importar si estas personas desean que lo haga o no. Incluso podría realizar un seguimiento de las personas que viajan en otros vehículos cercanos. En este tipo de situaciones podría ser difícil o imposible distinguir —mucho menos respetar— las preferencias de privacidad individuales.

El análisis de datos personales consolidados a gran escala de por sí representa un riesgo sustancial de invasión a la privacidad y potencial discriminación. Este riesgo se amplifica en la Internet de las Cosas debido a la escala y a la mayor intimidad de la recolección de datos personales. Los dispositivos de la IoT pueden recoger información personal con un grado de especificidad y penetración sin precedente; agregar y correlacionar estos datos permite crear perfiles personales detallados que general un potencial para la discriminación y otros daños. La sofisticación de esta tecnología puede crear situaciones que expongan al individuo a daños físicos, penales, financieros o de reputación.

La ubicuidad, familiaridad y aceptación social de muchos dispositivos de la IoT pueden crear una falsa sensación de seguridad y alentar a las personas a divulgar información confidencial o privada sin pleno conocimiento o apreciación de las posibles consecuencias.

Preguntas relacionadas con la privacidad de la Internet de las Cosas

Estas preguntas referidas a la privacidad serían un desafío incluso si estuvieran bien alineados los intereses y motivaciones de todas las partes involucradas en el ecosistema de la IoT. Sin embargo, sabemos que las relaciones y los intereses de quienes están expuestos a la recolección de sus datos personales y quienes agregan, analizan y utilizan los datos pueden ser desequilibrados o injustos. La fuente de datos puede ver una intrusión no deseada a su espacio privado, muchas veces sin consentimiento, control, elección o incluso conciencia. No obstante, quien recoge los datos podría considerarlos un

recurso beneficioso que puede añadir valor a sus productos y servicios y proporcionar nuevas fuentes de ingresos.

Dado que la Internet de las Cosas desafía nuestras nociones de privacidad de formas nunca antes vistas, al reevaluar los modelos de privacidad en línea en el contexto de la IoT es necesario responder ciertas preguntas clave. Algunas de las preguntas que se han planteado incluyen las siguientes:

LEGITIMIDAD EN LA RECOPILACIÓN Y EL USO DE LOS DATOS

En el contexto de la IoT, ¿cómo se resuelve la relación de mercado entre las fuentes de los datos y quienes los recogen? Los datos personales tienen un valor personal y comercial diferente según se consideren desde el punto de vista de las fuentes o de los recolectores, tanto individualmente como en su conjunto; por lo tanto, ambas partes tienen intereses legítimos que podrían estar en conflicto. ¿Cómo se pueden expresar estos diferentes intereses de una manera que conduzca a reglas en materia de acceso, control, transparencia y protección que sean justas y consistentes, tanto para las fuentes como para los recolectores?

TRANSPARENCIA, EXPRESIÓN Y CUMPLIMIENTO DE LAS PREFERENCIAS DE PRIVACIDAD

¿Cómo se puede hacer que las políticas y prácticas de privacidad sean de fácil acceso y comprensibles en el contexto de la IoT? ¿Cuáles son las alternativas al modelo tradicional de privacidad de "notificación y consentimiento" que podrían abordar los aspectos únicos de la Internet de las Cosas? ¿Cuál sería un modelo eficaz para expresar, aplicar y hacer cumplir las preferencias de privacidad individuales y las preferencias multipartitas? ¿Se podría construir un modelo multipartito de este tipo? De ser así, ¿qué aspecto tendría? ¿Cómo se podría aplicar a circunstancias concretas que impliquen las preferencias de privacidad individuales? ¿Existe un mercado para tercerizar la gestión de la configuración de la privacidad a servicios comerciales diseñados para implementar las preferencias de los usuarios? ¿Es necesario que exista un proxy de privacidad que exprese y haga cumplir las preferencias del usuario a través de una serie de dispositivos, al tiempo que elimine la necesidad de interacción directa con cada uno de ellos?

GRAN VARIEDAD DE EXPECTATIVAS DE PRIVACIDAD

Las normas y expectativas de privacidad están estrechamente relacionadas con el contexto social y cultural del usuario, que puede variar de una nación o de un grupo a otro. Muchos escenarios de la IoT implican el despliegue de dispositivos y actividades de recopilación de datos de alcance multinacional o global que atraviesan fronteras sociales y culturales. ¿Qué implicará esto para el desarrollo de un modelo de protección de la privacidad que se pueda aplicar ampliamente a la Internet de las Cosas? ¿Cómo se pueden adaptar los dispositivos y sistemas de la IoT para que reconozcan y respeten la variedad de expectativas de privacidad de los usuarios y las diferentes legislaciones?

PRIVACIDAD POR DISEÑO

¿Cómo se puede animar a los fabricantes de dispositivos de IoT para que incorporen los principios de la privacidad por diseño a sus valores fundamentales? ¿Cómo se puede fomentar la inclusión de consideraciones sobre la privacidad de los consumidores en todas las fases de desarrollo y operación de los productos? ¿Cómo se pueden conciliar los requisitos de funcionalidad y privacidad? En principio, los fabricantes deberían anticipar que, a largo plazo, los productos y las prácticas que respeten la privacidad se ganarán la confianza y la satisfacción de los cliente y generarán lealtad hacia la marca. ¿Es esta motivación suficiente para competir con los deseos de simplicidad en el diseño y velocidad al mercado? ¿Los dispositivos se deberían diseñar con una configuración predeterminada para el modo de recopilación de datos más conservador (es decir, no recopilación de datos por defecto)?

IDENTIFICACIÓN

¿Cómo debemos proteger los datos recogidos por la IoT que parecieran no ser personales donde se recogen o que han sido "desidentificados", pero que en algún momento futuro podrían llegar a ser datos personales (por ejemplo, porque podrían ser re-identificados o combinados con otros datos)?

La Internet de las cosas genera desafíos únicos para la privacidad que van más allá de los problemas que existen en la actualidad. Es necesario desarrollar estrategias para respetar las opciones de privacidad individuales considerando un amplio espectro de expectativas, sin dejar de fomentar la innovación en nuevas tecnologías para la IoT.

NOTAS DE LA SECCIÓN

Cuestiones relacionadas sobre la privacidad

63. Wilton, Robin. *CREDS 2014 - Position Paper: Four Ethical Issues in Online Trust*. Issue brief no. CREDS-PP-2.0. Internet Society, 2014. https://www.internetsociety.org/sites/default/files/Ethical Data-handling - v2.0.pdf

INTEROPERABILIDAD / CUESTIONES RELACIONADAS CON LAS NORMAS

Interoperabilidad / Estándares de la IoT–Antecedentes

En la Internet tradicional, la interoperabilidad es el valor central más básico; el primer requisito de la conectividad a Internet es que los sistemas "conectados" deben poder "hablar el mismo idioma" en cuanto a protocolos y codificaciones. La interoperabilidad es tan fundamental que los primeros talleres para fabricantes de equipos de Internet se denominaban "Interops";[64] además, es el objetivo explícito de todo el aparato de estandarización de Internet concentrado en el Grupo de Trabajo en Ingeniería de Internet (IETF).[65]

La interoperabilidad es también una de las piedras angulares de la Internet abierta.[66] Las barreras erigidas para obstruir el intercambio de información puede afectar la capacidad de los usuarios de Internet de ***conectarse***, ***hablar***, ***compartir*** e ***innovar***, que son los cuatro principios fundamentales de SOC.[67] También llamadas "jardines vallados", las plataformas cerradas en las que los usuarios solo pueden interactuar con un subconjunto seleccionado de sitios y servicios pueden disminuir considerablemente los beneficios sociales, políticos y económicos que permite el acceso a la totalidad de Internet.

La interoperabilidad eficaz y bien definida de los dispositivos puede fomentar la innovación y ofrecer eficiencias a quienes fabrican dispositivos, aumentando así el valor económico total del mercado.

En un entorno totalmente interoperable, cualquier dispositivo de la IoT se podría conectar a cualquier otro dispositivo o sistema e intercambiar información si así lo desean. En la práctica, la interoperabilidad es mucho más compleja. La interoperabilidad entre los dispositivos y sistemas de la IoT ocurre en diferentes grados en diferentes capas dentro de la pila de protocolos de comunicación entre los dispositivos. Además, no siempre es posible, necesario o deseable lograr la interoperabilidad plena en todos los aspectos de un producto técnico y, de ser impuesta artificialmente (por ejemplo, a través de un mandato gubernamental), podría desincentivar la inversión y la innovación. La estandarización y la adopción de protocolos que especifican estos detalles de la comunicación, en particular cuando resulta óptimo tener estándares, están en el centro de la discusión sobre la interoperabilidad para la IoT.

Más allá de los aspectos técnicos, la interoperabilidad tiene una importante influencia sobre el potencial impacto económico de la IoT. La interoperabilidad eficaz y bien definida de los dispositivos puede fomentar la innovación y ofrecer eficiencias a quienes fabrican dispositivos, aumentando así el valor económico total del mercado. Por otra parte, la implementación de los estándares existentes y el desarrollo de nuevos estándares abiertos cuando estos son necesarios ayudan a reducir las barreras de entrada, facilitan nuevos modelos de negocio y construyen economías de escala.[68]

Un informe del McKinsey Global Institute publicado en 2015 sostiene que "en promedio, la interoperabilidad es necesaria para crear un 40 por ciento del potencial valor que puede generar la Internet de las Cosas en diversos entornos."[69] El informe continúa diciendo que "La interoperabilidad es necesaria para desbloquear más de 4 billones de dólares al año de potencial impacto económico por el uso de la IoT en 2025, de un impacto total de $11.1 billones en los nueve entornos analizados por McKinsey".[70] Aunque para algunas empresas el hecho de construir sistemas propietarios pareciera tener ventajas competitivas e incentivos económicos, en un mercado de silos las oportunidades económicas pueden ser limitados.

Además, la interoperabilidad es valiosa tanto desde el punto de vista del consumidor individual como de las organizaciones que utilizan estos dispositivos. Facilita la capacidad de escoger los dispositivos con las mejores características y al mejor precio e integrarlos de manera que funcionen juntos. Los compradores podrían vacilar a la hora de adquirir productos y servicios de la IoT si no existe flexibilidad en cuanto a su integración, si su propiedad es compleja, si existe preocupación con respecto a una potencial dependencia del proveedor o en caso de temor a su obsolescencia debido al cambio de estándares.

Consideraciones clave y desafíos en la Interoperabilidad de la IoT / Estándares

La interoperabilidad, los estándares, los protocolos y las convenciones son temas fundamentales en el desarrollo y la adopción temprano de los dispositivos de la IoT. Sin ser exhaustiva, la lista de consideraciones y desafíos clave incluye:

LOS ECOSISTEMAS PROPIETARIOS Y LA ELECCIÓN DEL CONSUMIDOR

Algunos fabricantes de dispositivos ven una ventaja competitiva en la creación de un ecosistema de productos propietarios compatibles —a veces llamados "jardines vallados"— que limiten la interoperabilidad a los dispositivos y componentes de una misma marca. Estos fabricantes pueden generar dependencia (*lock-in*) en el ecosistema de sus dispositivos, aumentando los costos en que deben incurrir los consumidores para cambiar a otra marca o utilizar componentes de otros proveedores. Por ejemplo, en el mercado de la domótica, las bombillas de un proveedor podrían no ser interoperables con un sistema de interruptores de otro.

Los partidarios de la interoperabilidad consideran que estas prácticas impiden la elección del usuario, dado que evitan que los usuarios se cambien a productos alternativos. También consideran que estas prácticas representan una barrera para la innovación y la competencia, ya que limitan la capacidad de los competidores de crear nuevos productos basados en la infraestructura en la cual se sustenta el ecosistema. Sin embargo, algunos fabricantes de dispositivos consideran que el enfoque del ecosistema cerrado beneficia a los usuarios porque les proporciona un protocolo que se puede adaptar con mayor rapidez y facilidad cada vez que las exigencias técnicas o de mercado requieran un cambio.

Las consideraciones con respecto a interoperabilidad también se extienden a los datos que recogen y procesan los servicios de la IoT. Uno de los principales atractivos de los dispositivos conectados es su capacidad de transmitir y recibir datos de los servicios "en la nube", que a su vez proporcionan valiosos servicios o información sobre la base de esos datos. Si bien esto es extremadamente útil, también puede presentar desafíos en caso que un usuario desee pasar a un servicio competidor. Incluso si el acceso a los datos generados por los dispositivos se pone a disposición de los usuarios, obtener los datos no servirá de nada si están en un formato propietario. Un usuario solo podrá cambiarse a otro proveedor de servicios o analizar los datos por su cuenta si los datos fuente están libremente disponibles para los usuarios que los originan y en un formato abierto estándar.

LIMITACIONES TÉCNICAS Y DE COSTOS

A medida que los fabricantes desarrollan dispositivos de l IoT van surgiendo limitaciones técnicas, de tiempo al mercado y de costos que hay que tener en cuenta a la hora de decidir sobre su interoperabilidad y su diseño, Algunos dispositivos se ven limitadas por factores técnicos como los recursos de procesamiento disponibles, la memoria o las demandas de energía. Del mismo modo, los fabricantes se ven presionados para reducir el costo unitario de los dispositivos, reduciendo al mínimo los costos de diseño de los productos y las piezas. Los fabricantes realizan análisis de costo-beneficio para decidir si los mayores costos y las potenciales reducciones del rendimiento de los productos justifican los beneficios adicionales que tendría la implementación de los estándares. A corto plazo, puede ser más costoso diseñar e incluir características de interoperabilidad en un producto y probar su conformidad con la especificación de una norma. En ciertos contextos, el camino más económico al mercado podría ser el uso de protocolos y sistemas propietarios. Sin embargo, esto se debe comparar con las ganancias que se obtendrán durante el ciclo de vida a largo plazo gracias a la interoperabilidad del producto.

RIESGOS ASOCIADOS CON LOS TIEMPOS AL MERCADO

En un mercado competitivo y global, quien saca un producto y establece una cuota de mercado más rápidamente suele tener una ventaja. Esto ciertamente se aplica a los fabricantes de dispositivos de la IoT. El problema surge cuando el cronograma de diseño del fabricante se adelanta a la disponibilidad de los estándares de interoperabilidad. Un fabricante de dispositivos ansioso por sacar un producto al mercado puede considerar que la falta de certeza en cuanto a los tiempos y los procesos de desarrollo de los estándares constituye un riesgo comercial que se debe minimizar o evitar. Esto puede hacer que las alternativas de diseño que no contemplan estándares de interoperabilidad abiertos sean más atractivas, especialmente a corto plazo.

RIESGOS TÉCNICO

Como parte del proceso de desarrollo, quien fabrica o utiliza dispositivos para la Internet de las Cosas debe evaluar los riesgos técnicos de diseño de los protocolos. Incorporar estándares existentes y comprobados en el diseño de sistemas y productos puede implicar un riesgo técnico menor que desarrollar y utilizar protocolos propietarios. El uso de estándares genéricos, abiertos y ampliamente disponibles (como la familia de protocolos de Internet) como componentes de los dispositivos y servicios puede aportar otros beneficios, como el acceso a una mayor cantidad de talento técnico, software y una reducción de los costos de desarrollo. Estos factores se discuten en la RFC 7452, "*Architectural Considerations in Smart Object Networking*".[71]

DISPOSITIVOS MAL COMPORTADOS

El impacto de la falta de estándares y mejores prácticas documentadas va más allá de la limitación del potencial de los dispositivos de la IoT. De una manera pasiva, la ausencia de estas normas puede permitir el mal comportamiento de los dispositivos. En otras palabras, sin estándares que sirvan de guía para los fabricantes, quienes desarrollan estos dispositivos suelen diseñar productos cuyo funcionamiento perjudica a Internet sin prestar demasiada atención al impacto que pueden llegar a tener. Estos

dispositivos son peores que aquellos que simplemente no son interoperables. Si están mal diseñados y configurados, pueden afectar a los recursos de red que conectan a Internet e incluso a la propia Internet.

En un ensayo, Geoff Huston, experto en Internet, describe la proliferación de este tipo de dispositivos como la "Internet de las cosas estúpidas".[72] Huston describe el ejemplo de un cable módem de consumo producido por un fabricante que había configurado en el producto una dirección IP fija para el servidor de protocolo de tiempo de red (NTP) operado por la Universidad de Wisconsin, algo que constituye una violación de las prácticas de diseño habitualmente aceptadas. Tal como lo explica Huston, "Cuanto más unidades se vendían, mayor era el volumen total de tráfico que se enviaba al servidor de la universidad."[73] Estos dispositivos no solo se comportaban mal (canalizaban todas las solicitudes NTP a un único servidor), sino que el mal diseño del proveedor agravó la situación por no haber provisto un mecanismo eficaz para solucionar el problema.

Con el tiempo, la implementación de estándares y mejores prácticas para la Internet de las Cosas ofrece la oportunidad de disminuir significativamente estos problemas.

SISTEMAS HEREDADOS

La estandarización de la interoperabilidad representa un desafío para los nuevos dispositivos de la IoT que deben interactuar con los sistemas que ya están desplegados y en funcionamiento. Esto es relevante para muchos entornos específicos de ciertas industrias y aplicaciones que ya cuentan con redes de dispositivos establecidas.[74] Los ingenieros que trabajan en la IoT deben llegar a un compromiso entre un diseño que mantenga la compatibilidad con los sistemas heredados y su intención de lograr una mayor interoperabilidad con otros dispositivos mediante la utilización de estándares.

CONFIGURACIÓN

Los usuarios enfrentarán cada vez mayores desafíos a medida que aumente la cantidad de dispositivos de la IoT que deban manejar. Uno de estos desafíos es la necesidad de modificar rápida y fácilmente la configuración de múltiples dispositivos en una red. A la hora de enfrentar la configuración de cientos de dispositivos individuales, será fundamental que las herramientas, métodos e interfaces a utilizar hayan sido cuidadosamente diseñadas y estandarizadas.[75]

PROLIFERACIÓN DE LOS ESFUERZOS DE ESTANDARIZACIÓN

Además de los tradicionales organismos de normalización, han surgido múltiples coaliciones de la industria cuyo objetivo es ayudar a evaluar, desarrollar, modificar o armonizar los estándares y los protocolos relacionados con la IoT. Esto incluye, por ejemplo, organismos de normalización de larga data como el IETF, la ITU y el IEEE, además de iniciativas comparativamente nuevas como el Industrial Internet Consortium, el Open Interconnection Consortium, ZigBee Alliance y AllSeen Alliance, entre muchas otras.[76]

Es probable que la industria y las demás partes interesadas deban invertir mucho tiempo y recursos para participar en esta amplia gama de esfuerzos de normalización. Además, es probable que se produzcan solapamientos e incluso conflictos entre algunas de estas iniciativas.[77] Además de aumentar los costos de desarrollo de los estándares, la falta de coordinación entre los diferentes esfuerzos de normalización podría producir protocolos incompatibles, demorar el despliegue de los productos y generar fragmentación entre los diferentes productos, servicios y mercados verticales de la industria de la Internet de las Cosas.

Preguntas relacionadas con la interoperabilidad

La interoperabilidad y los estándares plantean desafíos y preguntas que será necesario responder para el futuro de los dispositivos de la IoT, entre ellas las siguientes:

¿En qué áreas son más necesarias y deseables las normas de interoperabilidad? ¿Son suficientemente similares o diferentes en toda la gama de posibles aplicaciones y casos de uso de la IoT (por ejemplo, bienes de consumo, aplicaciones industriales y aparatos médicos)? ¿Cuáles normas genéricas y ampliamente disponibles (como por ejemplo la familia de protocolos de Internet) se podrían utilizar como componentes de los dispositivos y servicios de la IoT? ¿Cómo afectaría la falta de interoperabilidad la capacidad de los usuarios de conectarse, hablar, compartir e innovar?

¿Qué funciones deben cumplir los organismos de normalización, los consorcios de la industria y los grupos de partes interesadas en el desarrollo de estándares para la IoT? ¿Qué potencial tendría reunir a la amplia gama de grupos que están trabajando en implementaciones técnicas de la IoT para una discusión más amplia sobre la interoperabilidad y la implementación de estándares? ¿Se pueden evitar la existencia de estándares que compitan entre sí, la duplicación de esfuerzos y los conflictos que surgen cuando diferentes organismos y consorcios de normalización abordan temas similares o coincidentes sin que los gastos de coordinación se vuelvan excesivos? En términos más prácticos, ¿cómo pueden los actores de la industria y otras partes interesadas mantenerse al tanto de todo lo que ocurre en este amplio espacio?

¿Cuál es el mejor enfoque para involucrar y educar a las comunidades de usuarios y desarrolladores sobre los problemas que generan los dispositivos de la IoT que no se comportan bien y la falta de implementación de los estándares? Dada la amplia variedad de aplicaciones y casos de uso de la IoT, ¿qué tipos de mejores prácticas o modelos de referencia de implementación serían eficaces?

¿Cómo afectará la Internet de las Cosas el consumo de ancho de banda y otros recursos? ¿En qué medida será necesario modificar los estándares para dar soporte a las necesidades cambiantes? Dada la importancia que tienen los servicios basados en la nube para la Internet de las Cosas, ¿qué desafíos plantea la interoperabilidad entre nubes?

En términos generales, no se puede negar la importancia de la interoperabilidad y los estándares de la IoT para el mercado y para los consumidores. En última instancia, es fundamental incorporar el desafío de desarrollar y emplear estándares de interoperabilidad en la discusión sobre la innovación, la competencia y la elección de los servicios por parte del usuario, todos temas que forman parte de los básicos de ISOC.

NOTAS DE LA SECCIÓN

Interoperabilidad / Cuestiones relacionadas con las normas

64. "A History of the Internet: 1988." Web log post. Computer Information, 12 de agosto de 2010. Web. 6 de septiembre de 2015. http://inthistory4u.blogspot.com/2010/08/1988.html

65. Ver http://www.ietf.org

66. "Open Internet: What is it, and how to avoid mistaking it for something else," Internet Society 3 de septiembre de 2014. https://www.internetsociety.org/doc/open-internet-what-it-and-how-avoid-mistaking-it-something-else

67. "Values and Principles." *Principles*. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles

68. La Sección 3.5.6, Internet de las Cosas, del Plan Progresivo de Normalización de las TIC de la Comisión Europea (2015) incluye un debate sobre los estándares para la IoT desde el punto de vista de la competitividad y las políticas. Ver https://ec.europa.eu/digital-agenda/en/rolling-plan-ict-standardisation

69. Manyika, James, et. al., *The Internet of Things: Mapping the Value beyond the Hype*. McKinsey Global Institute, junio de 2015. p. 2. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

70. *Ibid.* 4.

71. Tschofenig, H., et. al., *Architectural Considerations in Smart Object Networking*. Tech. no. RFC 7452. Internet Architecture Board, marzo de 2015. Web. https://tools.ietf.org/html/rfc7452

72. Huston, Geoff. "The Internet of Stupid Things." *APNIC Labs*., 28 de abril de 2015. https://labs.apnic.net/?p=620

73. *Ibid*.

74. Son ejemplos de protocolos de sistemas legados: el protocolo SCADA (Supervisory Control and Data Acquisition), que se utiliza para la comunicación de dispositivos industriales, y los protocolos CAN Bus (Control Area Network) para sensores vehiculares e industriales.

75. Vint Cerf, personal communications, 9 de septiembre de 2015.

76. En la sección "Más información" que se encuentra al final de este trabajo el lector encontrará un listado de organismos de normalización, consorcios y alianzas que están trabajando en la estandarización de la IoT.

77. Lawson, Stephen. "Why Internet of Things 'Standards' Got More Confusing in 2014." *PCWorld*, 24 de diciembre de 2014. http://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html

CUESTIONES REGLAMENTARIAS, LEGALES Y DE DERECHOS

La aplicación de los dispositivos de la IoT plantea una variedad de desafíos y preguntas sobre aspectos regulatorios y legales que deben ser considerados cuidadosamente. En algunos casos, los dispositivos de la IoT dan lugar a nuevas situaciones legales y regulatorias y generan preocupaciones con respecto a los derechos civiles que antes no existían. En otros casos, estos dispositivos magnifican cuestiones legales que ya existían. Además, la tecnología está avanzando a una velocidad mucho mayor que los entornos regulatorios y de políticas relacionados. A continuación se discuten algunos potenciales problemas regulatorios y legales que afectan a todo el espectro de aplicaciones de la IoT.

Protección de datos y flujos de datos transfronterizos

No se puede evitar que los datos que recogen los dispositivos de la IoT se envíen a través de los límites jurisdiccionales. Estos dispositivos utilizan Internet para comunicarse e Internet atraviesa límites jurisdiccionales a todo nivel. Los dispositivos de la IoT pueden recoger datos sobre las personas en una jurisdicción y transmitirlos a otra para su almacenamiento o procesamiento, muchas veces sin mayores obstáculos técnicos. Esto puede convertirse rápidamente en un problema legal, por ejemplo, si los datos recogidos se consideran datos personales o datos sensibles y están sujetos a las leyes de protección de datos de múltiples jurisdicciones. Para complicar aún más las cosas, las leyes de protección de datos en la jurisdicción donde residen el dispositivo y el titular de los datos podría ser inconsistente o incompatible con las leyes de la jurisdicción donde los datos se almacenan y procesan.

Estas situaciones se describen como flujos de datos transfronterizos y plantean preguntas con respecto al alcance jurídico de las normas que podrían ser aplicables. En otras palabras, ¿cuál régimen legal regula el dispositivo que recoge los datos y cuál regula el almacenamiento y el uso de los datos recogidos? Este escenario también

La Internet de las Cosas plantea nuevas preguntas regulatorias y legales y puede amplificar los desafíos legales que ya existen en torno a Internet. Promover la capacidad de los usuarios para conectarse, hablar, innovar, compartir, elegir y confiar es una consideración fundamental para la evolución de leyes y reglamentos.

plantea preguntas normativas. ¿Se pueden modificar estas leyes para reducir el grado de fragmentación de Internet que provocan y, a la vez, proteger los derechos de los usuarios? Si una jurisdicción tiene leyes de protección de datos más restrictivas en cuanto al manejo y la transmisión de determinados datos provenientes de la IoT, ¿estos requisitos legales se deberían poder proyectar a otras jurisdicciones?

Si bien muchas de estas preguntas sobre los flujos de datos transfronterizos ya se han

planteado y abordado en el marco del tráfico de datos de la Internet tradicional,[78] los dispositivos de la IoT plantean un nuevo desafío en este sentido. Cada vez más, estos dispositivos podrán conectarse automáticamente a otros dispositivos y sistemas y transmitir información a través de las fronteras sin el conocimiento del usuario. Esto podría crear situaciones en las que un usuario se podría convertir en responsable de cumplir con los requisitos aplicables a los flujos de datos transfronterizos, incluso sin saber que esto está ocurriendo. Estos son temas complejos y lo serán cada vez más, ya que la tecnología sigue avanzando más rápido que las políticas.

Discriminación de los datos de la IoT

Los datos recogidos por los dispositivos de la IoT permiten formar una imagen detallada de las personas con que interactúan y estos datos pueden ser utilizados tanto para fines beneficiosos como para fines discriminatorios. Consideremos el caso de los dispositivos que se utilizan para llevar registro de la actividad física. Muchas veces una persona lleva uno de estos dispositivos de forma permanente durante un período de días o semanas; durante todo este tiempo, el dispositivo recoge información muy detallada sobre los movimientos de la persona y otros datos biométricos. Una aplicación analiza estos datos para determinar el estado físico de la persona, estimar las calorías que quema, llevar un registro de las horas de sueño y caracterizar la calidad del sueño. Este análisis es claramente beneficioso para el usuario, ya que le ofrece una manera de cuantificar su actividad física mientras intenta alcanzar un objetivo de pérdida de peso o aptitud física.

Pero estos mismos datos se pueden utilizar en formas potencialmente discriminatorias. En Estados Unidos, algunos planes de seguro médico están incentivando a los participantes para que permitan que el asegurador acceda a los datos del dispositivo a cambio de primas de seguro más bajas.[79] Esta practica puede ser vista como positiva: ofrecer precios preferenciales a quienes estén dispuestos a entregar sus datos biométricos a cambio de un descuento. Por otra parte, potencialmente podría ser discriminatoria, en especial para quienes se encuentran en desventaja económica. En palabras de un comentarista:

> Imaginemos un esquema de precios [de pólizas de seguros] que castiga a los padres solteros privados de sueño o a los hábitos alimenticios de los trabajadores más pobres. Los incentivos financieros para permitir que las aseguradoras y otros interesados accedan a la información sobre su salud podrían llegar a ser tan convincentes que "escoger" participar sería la única opción viable.[80]

Los datos que recogen los dispositivos de la IoT permiten formar una imagen detallada de las personas con que interactúan. Estos datos pueden ser utilizados para propósitos y productos muy valiosos que benefician a los usuarios. Sin embargo, estos mismos datos podrían ser utilizados en forma discriminatoria.

Los escenarios como este son cada vez más frecuentes. Los vehículos más nuevos están equipados con transpondedores equipados con GPS y enlaces de datos que comunican información de geolocalización y hábitos de conducción (por ejemplo, excesos de velocidad y fuerza de frenado) a sistemas remotos, o que se utilizan para proporcionar asistencia o servicios de viaje al conductor. Si bien estas características le proporcionan ventajas al usuario, los datos podrían llegar a ser utilizados en formas potencialmente discriminatorias. Por ejemplo, los operadores de flotas pueden utilizar estos datos para monitorear el desempeño de sus conductores sin que los conductores puedan optar por no ser observados. Estos son ejemplos bastante directos de cómo se pueden utilizar los datos de la IoT de forma discriminatoria, pero no queda claro cómo se podrían utilizar las diferentes combinaciones de datos para discriminar en el futuro.

Además, la calidad, la especificidad y el volumen de los datos producidos por la IoT podría magnificar el potencial de que se generen prácticas de precios discriminatorias y servicios ilegítimos. Con frecuencia los datos de la IoT se pueden etiquetar con metadatos (marcas de fecha y de tiempo, etiquetas de geolocalización) que aumentan dramáticamente la calidad de los datos desde el punto de vista de su análisis. Además, los sensores de la IoT suelen realizar muy pocas funciones. Esto significa que los datos de los sensores suelen asociarse con una situación operativa específica, que permite un alto grado de especificidad a la hora de correlacionar los datos con una persona o con un grupo de personas. De hecho, el dispositivo se podría llegar a asociar con la persona en la que está implantado, como en el caso de un marcapasos o una bomba de insulina conectados a Internet. En otros casos, este nivel de especificidad no es deseable y accidentalmente puede provocar resultados discriminatorios. Los sensores de la IoT pertenecientes o gestionados por terceros pueden recoger datos identificables sobre las personas sin su conocimiento o consentimiento. Estos datos se podrían utilizar de formas que perjudicarían a la persona monitoreada.

Por último, estos dispositivos crean importantes flujos de datos continuos sin intervención humana. La combinación de estas cualidades hace que los análisis de los datos de la IoT sean muy descriptivos y útiles para la investigación, el desarrollo de productos y también en otras áreas. Los algoritmos de *Big Data* pueden examinar cantidades enormes de datos y buscar correlaciones estadísticas y semánticas para así determinar grupos de usuarios con características afines. A su vez, estos algoritmos podrían categorizar injustamente a los usuarios y explotar sus características.

Este tipo de usos de los datos de la IoT plantea cuestiones prácticas, legales y reglamentarios. En primer lugar, ¿cómo podemos detectar las prácticas discriminatorias o injustas contra los usuarios? ¿Existen prácticas discriminatorias virtualmente imposibles de detectar? ¿Existe alguna diferencias legal en caso que la decisión de discriminar sea tomada por una persona o por una máquina? El desarrollo de herramientas para detectar prácticas algorítmicas injustas es un desafío para la investigación académica, sobre todo porque la mayoría de los algoritmos de análisis de datos son secretos empresariales y no son del dominio público. ¿Cómo podemos equilibrar los enormes beneficios comerciales y sociales del análisis de datos de la IoT con la probabilidad de que se generen prácticas discriminatorias contra los usuarios? ¿Cómo podemos fomentar la adopción de los principios de la innovación sin pedir permiso (*permissionless innovation*) en el ámbito de la IoT y a la vez proteger a los usuarios contra las prácticas ilegítimas? ¿Cómo podemos mejorar la transparencia? ¿Las leyes de privacidad y de protección del consumidor existentes alcanzan para hacer frente a este escenario? ¿Qué recursos deberían estar disponibles en caso de discriminación? ¿Los dispositivos de la IoT se deberían categorizar y regular en función de la naturaleza de los datos que producen, especialmente cuando los datos son propensos a ser mal utilizados?

Los dispositivos de la IoT utilizados como ayudas para las agencias de aplicación de la ley y la seguridad pública

Los dispositivos de la IoT podrían servir como ayudas para las agencias de aplicación de la ley y la seguridad pública, pero en este caso es necesario considerar cuidadosamente las ramificaciones legales y sociales. Indudablemente, los dispositivos de la IoT y los datos que generan pueden ser utilizados como herramientas eficaces para luchar contra el crimen. Muchos comercios minoristas han instalado cámaras de seguridad para recoger imágenes de video y realizar un seguimiento de la actividad de los compradores, algo que ha resultado de gran valor como prueba en los procesos penales y como elemento de disuasión de la delincuencia.[81] Más recientemente, On-Star Corporation, una subsidiaria de General Motors, puede proporcionar datos de los sensores que se encuentran en el automóvil de la policía para ayudar en la recuperación de vehículos robados y puede desactivar de forma remota un vehículo robado.[82] El Departamento de Policía del Condado de Nassau (Nueva York) utiliza una red de sensores de sonido llamada *ShotSpotter* que permite detectar y localizar la fuente exacta de un disparo en los barrios donde han sido desplegados.[83] Todos estos son ejemplos de los beneficios que la tecnología de la Internet de las Cosas puede ofrecer a la policía para combatir la delincuencia y mejorar la seguridad pública.

Sin embargo, el despliegue y uso de este tipo de tecnologías provocan preocupación entre algunos defensores de los derechos civiles y otras personas. Entre las posibles causas de preocupación se incluyen la omnipresencia de las actividades de monitoreo de los datos, las políticas sobre su conservación y destrucción, los usos secundarios que los gobiernos pueden darles, así como la potencial exposición accidental de los datos a actores maliciosos. Además, se deben considerar cuidadosamente los efectos potencialmente negativos sobre las actividades beneficiosas de las comunidades y sociedades monitoreadas.

Otras situaciones de orden y seguridad públicos son más complejas. Por ejemplo, al lanzar el iPhone 6 y su sistema operativo iOS 8, Apple Corporation eliminó un método de acceso tipo "puerta trasera" que existía en versiones anteriores de su teléfono. La función de puerta trasera permitía a la policía acceder a los datos que se encontraban en el teléfono de un usuario. Apple eliminó esta característica en el nuevo iPhone y ahora encripta el contenido interno del teléfono de una manera difícil de vulnerar y para la cual Apple no tiene las claves, por lo cual no tiene forma de permitir el acceso.[84] Esto hace que solo el propietario del teléfono pueda acceder a su contenido. Las agencias federales de seguridad sostienen que esto hace que sea más difícil procesar los comportamientos criminales,[85] mientras que los partidarios de los derechos civiles ven en esto una victoria para la protección de la privacidad de los datos de los usuarios.[86] Esta controversia con respecto al cifrado de los dispositivos también se aplica a otros dispositivos de la IoT. ¿Qué papel debe desempeñar el cifrado de los dispositivos en la protección de los dispositivos de la IoT contra los ataques criminales? ¿Cómo se puede equilibrar esto con el legítimo acceso a los datos del usuario en interés de la aplicación de la ley y la seguridad pública?

Responsabilidad por los dispositivos de la IoT

Los dispositivos de la IoT plantean interrogantes con respecto a la responsabilidad desde el punto legal que invitan a la reflexión. Una de las preguntas fundamentales subyacentes en lo que respecta a los dispositivos de la IoT es la siguiente: Si alguien se ve perjudicado como consecuencia de la acción u omisión de un dispositivo de la IoT, ¿quién es el responsable? En muchos casos la respuesta es complicada y a veces todavía no existe demasiada jurisprudencia para sustentar una posición determinada. Los dispositivos de la IoT funcionan de forma más compleja que un producto independiente y esto sugiere que será necesario considerar escenarios de responsabilidad más complejos. Por ejemplo:

- Puede que los dispositivos de la IoT sean utilizados en formas nunca previstas por su fabricante. No es razonable suponer que un fabricante de dispositivos pueda realizar pruebas de control de calidad para todos los potenciales casos de uso de los dispositivos de la IoT.

- Quizás los dispositivos de la IoT se conecten e interactúen con otros de formas no anticipadas y para las cuales no se realizaron pruebas. A medida que aumente la interoperabilidad, estos dispositivos podrán formar entre sí conexiones de red *ad hoc*. Por lo tanto, antes de desplegar estos dispositivos, es difícil para un fabricante o usuario tener en cuenta todos los escenarios potencialmente perjudiciales que podrían llegar a surgir.

- Una vez instalados, estos dispositivos pueden tener una larga vida útil y serán susceptibles a futuras amenazas a la seguridad que hoy en día son desconocidas. Esto significa que estos dispositivos podrían verse comprometidos y ser reprogramados maliciosamente para dañarse a sí mismos o a otros dispositivos, o bien para revelar información sensible en forma no intencionada e inadvertida.

- Los dispositivos de la IoT se integrarán en sistemas autónomos (por ejemplo, automóviles sin conductor) que incorporan algoritmos de aprendizaje adaptativo para controlar su comportamiento sobre la base de la información aportada por los sensores de tales dispositivos. Es imposible conocer y probar con anticipación las acciones de estos sistemas.

Estos y otros escenarios plantean interrogantes. Si uno de uno de estos escenarios genera daños, ¿las leyes de responsabilidad existentes abordan adecuadamente la culpabilidad legal y aclaran la responsabilidad de las partes involucradas? ¿Es necesario repensar las leyes de responsabilidad para los dispositivos inteligentes de la IoT que aprenden de su entorno y se modifican a sí mismos a medida que pasa el tiempo? Si un sistema autónomo recibe instrucciones del usuario y no de sus algoritmos internos, ¿qué pasa en caso de error del usuario? ¿Los dispositivos de la IoT deberían ser lo suficientemente inteligentes como para tener una instrucción de tipo “haz lo que quise decir”? ¿En qué medida se pueden ampliar las leyes de responsabilidad que existen para los productos convencionales de manera que abarquen los productos que se van conectando a Internet? Como comunidad, ¿qué podemos hacer para informar mejor a los legisladores y a los formuladores de políticas de modo que no sean tan susceptibles frente a la enorme cantidad de información errónea y consejos sesgados que reciben? ¿Qué podemos hacer para informar mejor a los usuarios y compradores de estos dispositivos de modo que entiendan todos los factores que afectan su uso?

Proliferación de dispositivos de la IoT utilizados en acciones legales

Los datos que recogen los dispositivos de la IoT muchas veces pueden servir como prueba en una variedad de procedimientos legales. A medida que estos datos se vuelvan más frecuentes, es probable que se utilicen cada vez más en este tipo de procedimientos. Por ejemplo, algunos abogados en Estados Unidos han utilizado durante un juicio de divorcio los datos de hora y localización obtenidos de los dispositivos de peaje electrónico instalados en los automóviles para demostrar que un cónyuge engañaba al otro.[87] En 2014, una mujer canadiense utilizó los datos de su propio dispositivo de actividad física en apoyo de su reclamo en una demanda por lesiones personales.[88]

Los dispositivos de la IoT funcionan de forma más compleja que un producto independiente y esto sugiere que será necesario considerar escenarios de responsabilidad más complejos.

En cuanto a usos más deliberadas de los dispositivos de la IoT para procedimientos legales, en los automóviles se pueden instalar dispositivos conectados a Internet de manera que actúen como garantía en caso de incumplimiento de las obligaciones de pago. Si un conductor no para el *leasing* o el crédito de su automóvil, el arrendatario o prestamista puede inactivar el vehículo de forma remota usando el dispositivo instalado hasta que se realice el pago.[89] Estos dispositivos ya se han instalado en más de dos millones de automóviles en Estados Unidos.[90]

Este tipo de escenarios plantean nuevas preguntas legales y reglamentarias con respecto a los dispositivos de la IoT. ¿Deberían los fabricantes de dispositivos incluir en estos dispositivos tecnologías como el cifrado para restringir el acceso a los flujos de datos como lo ha hecho Apple en el iPhone? A la inversa, ¿deberían los fabricantes estar diseñando dispositivos de la IoT que faciliten el uso de los datos en un procedimiento judicial? ¿Es necesario desarrollar estándares que especifiquen requisitos de diseño para que los datos de la IoT soporten la cadena de custodia de los datos en los procesos judiciales? ¿Se deberían establecer regulaciones que protejan al consumidor de ciertos dispositivos de la IoT?

proceedings? Are standards needed to specify design requirements for IoT data to support legal chain of custody of data in legal proceedings? Should there be consumer protection regulations placed on certain IoT devices?

Resumen de las cuestiones reglamentarias, legales y de derechos

La gama de temas legales, reglamentarios y de derechos relacionados con la Internet de las Cosas es amplia y variada. Los dispositivos de la IoT crean nuevos desafíos legales y de políticas que no existían anteriormente y que amplifican muchos de los desafíos ya existentes. Por ejemplo, algunos tipos de dispositivos de la IoT pueden plantear nuevos desafíos en cuanto a la accesibilidad para personas con discapacidades, sin dejar de lado la compatibilidad con los estándares y directrices de accesibilidad existentes.[91] Por otra parte, la enorme cantidad de dispositivos inalámbricos de la IoT y el ruido de radiofrecuencia (RF) y las interferencias que producen son ejemplos de cómo los dispositivos de la IoT amplifican la dificultad que existe para regular el uso del espectro de RF.[92] Otros desafíos emergentes para los dispositivos de la IoT son las preocupaciones legales y reglamentarias con respecto a la propiedad intelectual, las cuestiones ambientales (por ejemplo, cómo desechar los dispositivos) y la propiedad legal de dispositivos (por ejemplo, ¿los dispositivos serán propiedad del usuario o serán alquilados?).

A las complejidades de decidir las estrategias apropiadas de regulación o de políticas para los problemas de la IoT se suma la complejidad de decidir qué lugar de la arquitectura de un sistema de la IoT es el mejor para conseguir los resultados deseados. ¿Dónde se deben colocar los controles regulatorios? ¿En el dispositivo, en el flujo de datos, en la puerta de enlace, en el usuario o en la nube en que se almacenan los datos? Las respuestas a estas y otras preguntas dependen de la perspectiva desde la cual se analice la situación. Cada vez más, los análisis regulatorios de los dispositivos de la IoT se realizan desde una perspectiva legal general y tecnológicamente neutra, como por ejemplo las leyes y reglamentos de protección al consumidor.[93] Entre otras cosas, evaluar las implicancias legales de los dispositivos de la IoT desde la perspectiva de la prevención de prácticas desleales o engañosas contra los consumidores[94] puede ayudar a informar las decisiones sobre privacidad y seguridad.[95]

Por último, tanto la resolución de los desafíos en este espacio como su impacto se deben tener en cuenta en relación con los principios rectores de la Internet Society que promueven la capacidad de ***conectarse***, ***hablar***, ***innovar***, ***compartir***, ***escoger*** y ***confiar***.

NOTAS DE LA SECCIÓN

Cuestiones reglamentarias, legales y de derechos

78. En general, los flujos de datos transfronterizos se abordan dentro de los marcos de privacidad regionales e internacionales (por ejemplo, las Directrices de la OCDE que regulan la protección de la privacidad, el Convenio No. 108 del Consejo de Europa, el Marco de Privacidad de APEC) y disposiciones especiales (por ejemplo, el sistema de Reglas de Privacidad Transfronteriza de APEC, las Normas Corporativas Vinculantes de la UE). Pero esta no es una solución que se pueda aplicar a escala global, sino un enfoque fragmentado.

79. "Big Doctor Is Watching". *Slate*, 27 de febrero de 2015. http://www.slate.com/articles/technology/future_tense/2015/02/how_data_from_fitness_trackers_medical_devices_could_affect_health_insurance.html

80. *Ibid*.

81. Goforth Gregory, Jennifer. "5 Ways Tech Is Stopping Theft." *Entrepreneur*, 7 de noviembre de 2013. http://www.entrepreneur.com/article/229674

82. Bond, Jr., Vince. "Lawyers Reaching for In-car Data." *Automotive News*, 14 de septiembre de 2014. http://www.autonews.com/article/20140914/OEM11/309159952/lawyers-reaching-for-in-car-data

83. Weis, Todd R. "Cool Cop Tech: 5 New Technologies Helping Police Fight Crime." *Computerworld*. N.p., 16 de febrero de 2012. Web. 03 Aug. 2015. http://www.computerworld.com/article/2501178/government-it/cool-cop-tech--5-new-technologies-helping-police-fight-crime.html?page=2

84. Timm, Trevor. "Your IPhone Is Now Encrypted. The FBI Says It'll Help Kidnappers. Who Do You Believe?" *The Guardian*, 30 de septiembre de 2014. http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default

85. *Ibid*.

86. Timberg, Craig. "Apple Will No Longer Unlock Most IPhones, IPads for Police, Even with Search Warrants." *Washington Post.* The Washington Post, 18 de septiembre de 2014. http://wapo.st/XGGwDi

87. Newmarker, Chris. "E-ZPass Records out Cheaters in Divorce Court." *Msnbc.com*. NBC News.com, 10 de agosto de 2007. http://www.nbcnews.com/id/20216302/ns/technology_and_science-tech_and_gadgets/t/e-zpass-records-out-cheaters-divorce-court/ - .Vbp9KnjfbFI

88. Olson, Parmy. "Fitbit Data Now Being Used In The Courtroom." *Forbes*. Forbes Magazine, 16 de noviembre 2014. http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/

89. Picchi, Aimee. "Why the Repo Man Can Remotely Shut off Your Car Engine." *CBS News*, 25 de septiembre de 2014. http://www.cbsnews.com/news/why-the-repo-man-can-remotely-shut-off-your-car-engine/

90. Corkery, Michael, and Jessica Silver-Greenberg. "Miss a Payment? Good Luck Moving That Car." *New York Times*, 24 de septiembre de 2014. http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/

91. Muchas de las normas que rigen los procesos de compras del sector público especifican requisitos de accesibilidad

mínimos para los productos de tecnología de la información y la comunicación (TIC) que debe ser considerados en el contexto de la compatibilidad de los dispositivos de la IoT. Ejemplos de estas normas incluyen la Sección 508 de la Junta de Accesibilidad de Estados Unidos y la Norma Europea EN 301 549 V1.1.1.

92. McHenry, Mark A., Dennis Roberson, and Robert J. Matheson. "Electronic Noise Is Drowning Out the Internet of Things." *IEEE Spectrum*, no. septiembre de 2015 (18 de agosto de 2015). http://spectrum.ieee.org/telecom/wireless/electronic-noise-is-drowning-out-the-internet-of-things

93. Botterman, Maarten. *Policy Paper on IoT Future Technologies: Opening towards a New Reality*. Issue brief no. D5.2. 39. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf

94. Ley de la Comisión Federal de Comercio de Estados Unidos, Código 15 § 45(a).

95. La Coalición Dinámica del Foro de Gobernanza de Internet sobre la Internet de las Cosas (DC IoT, por su sigla en inglés) DC ha propuesto un "enfoque ético" para enmarcar las soluciones a los desafíos de la IoT. Ver, por ejemplo: http://www.iot-dynamic-coalition.org/intersessional-meetings/dresden-meeting-2015/ y http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/

96. "Values and Principles." *Principles*. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles

CUESTIONES RELACIONADAS CON LAS ECONOMÍAS EMERGENTES Y EL DESARROLLO

Garantizar que las oportunidades de la IoT sean globales

La propagación y el impacto de Internet tienen un alcance global: ofrecen oportunidades y beneficios a las regiones desarrolladas y las regiones en desarrollo por igual. A la vez, muchas veces en las regiones en desarrollo se plantean desafíos únicos relacionadas con el despliegue, el crecimiento, la implementación y el uso de la tecnología, incluso de Internet. Es razonable esperar que esto también sea válido para los potenciales beneficios y desafíos asociados con la Internet de las Cosas.

Desde la perspectiva de los principios de la Internet Society, creemos que Internet debe ser una fuente de empoderamiento a nivel global, sin importar la ubicación, la región o el estado de desarrollo económico del usuario, y que toda la gama de habilidades y principios[97] que impulsan nuestro trabajo y el éxito de Internet se aplican a nivel global. Desde los primeros tiempos de Internet, la comunidad técnica, la sociedad civil, las organizaciones gubernamentales y la industria privada, entre otros actores, se han centrado en las oportunidades y los desafíos relacionados con Internet en las economías emergentes. De modo que esto también debería ser cierto con respecto a las oportunidades y desafíos relacionados con la Internet de las Cosas.[98]

La IoT encierra una gran promesa como habilitador del desarrollo social, incluyendo el logro de los Objetivos de las Naciones Unidas para el Desarrollo Sostenible.

Oportunidades económicas y de desarrollo

Con respecto a las oportunidades, el McKinsey Global Institute señala que la tecnología de la IoT tiene gran potencial en las economías en desarrollo. Se proyecta que en 2025 hasta un 38% del impacto económico anual de las aplicaciones de la IoT provendrá de las regiones menos desarrolladas.[99] Desde una perspectiva económica, se anticipa que las tendencias tanto demográficas como de mercado impulsarán las oportunidades. Por ejemplo, los países en desarrollo tienen un elevado número de potenciales usuarios de la IoT (especialmente China), el crecimiento económico mundial se está desplazando hacia las economías en desarrollo y se espera que las aplicaciones industriales de la IoT (por ejemplo, en las fábricas, los lugares de trabajo y el transporte) impulsaran la creación de valor económico.[100]

Si se materializan las expectativas con respecto a la innovación y la aplicación de la tecnología, las implementaciones de la IoT podrían encerrar una gran promesa como habilitadoras del desarrollo social, incluyendo el logro de los Objetivos de las Naciones Unidas para el Desarrollo Sostenible.[101] Los Objetivos de la ONU para el Desarrollo Sostenible son un conjunto de diecisiete objetivos que abarcan más de cien metas y que apuntan a guiar los esfuerzos para lograr dignidad, bienestar e igualdad para todas las personas del mundo —especialmente las personas pobres y marginadas—. Abarcan una amplia gama de desafíos de desarrollo fundamentales, entre ellos la agricultura sostenible, la energía, la disponibilidad de agua, la industrialización y la gestión de los recursos terrestres y marítimos.

Al considerar el potencial de que la tecnología de los objetos inteligentes y la Internet de las Cosas aborde los desafíos del desarrollo de manera significativa, las oportunidades parecen ser convincentes. Por ejemplo, la aplicación de redes de sensores a diferentes desafíos ambientales —la calidad y el uso del agua, el saneamiento, la salud y las enfermedades, el cambio climático y el monitoreo de los recursos naturales— podría tener un fuerte impacto más allá de la gestión de los recursos. Los datos obtenidos de este tipo de aplicaciones también se podrían utilizar en contextos de investigación y ayudar a los científicos y a las universidades locales a realizar contribuciones únicas al cuerpo de conocimiento científico global e incentivar a los talentos académicos locales de manera que permanezcan en el país y se dediquen a la investigación.

La creciente población mundial —especialmente en las economías emergentes— y se anticipa que los desafíos relacionados con el acceso a alimentos de calidad, seguros y asequibles aumentarán con el tiempo. El potencial uso de la IoT para combatir el hambre y promover una agricultura sostenible ha recibido especial atención, quizás más que cualquier otro problema relacionad con el desarrollo.[102] Desde la gestión de los ciclos de producción agrícola, las amenazas de enfermedades y el aumento de las materias primas gracias a la automatización de las cosechas, la logística aplicada a la distribución y el control de la calidad, se anticipa que las técnicas de "agricultura inteligente" basadas en la IoT se incorporarán a toda la cadena de valor para mejorar la sostenibilidad y la productividad de la oferta de alimentos.[103, 104]

CASILLA 4

CÓMO APROVECHAR LA IOT PARA EL DESARROLLO GLOBAL

La Internet de las Cosas (IoT) se está desplegando alrededor del mundo para resolver algunos de los problemas de desarrollo más urgentes a nivel global. Se están usando tecnologías conectadas para mejorar la prestación de servicios y los resultados del desarrollo en múltiples áreas, desde el alivio de la pobreza hasta la mejora de la gestión sostenible del agua y el saneamiento.

Impulsada por los costos cada vez menores de los sensores y microprocesadores y la creciente variedad de tecnologías de conectividad asequibles, la IoT representa la próxima frontera para las tecnologías de la información y la comunicación (TIC) para el desarrollo (ICT4D). Mientras que más del 90% de la población mundial tiene cobertura de las redes celulares móviles y dos tercios tienen acceso a señales 3G que permiten una comunicación de datos robusta, también hay otras tecnologías de corto y largo alcance que ofrecen una amplia gama de opciones de conectividad de datos. A medida que los dispositivos y servicios continúen volviéndose más asequibles, crecerán las intervenciones de la IoT en el desarrollo (IoT4D). Por ejemplo, hoy en día, si cuentan con sensores para monitorear la temperatura y la ubicación, las cadenas de frío —especialmente las que facilitan el transporte y la distribución de las vacunas esenciales— son más seguras y eficientes, por lo que un porcentaje mayor de los envíos llegan a destino sin echarse a perder. En África oriental, se están desplegando bombas de agua manuales equipadas con sensores de flujo con módulos SMS 2G que pueden informar a los municipios locales, a las oficinas gubernamentales y a las comunidades de donantes sobre la tasa de uso del agua y el tiempo de inactividad debido a un mal funcionamiento de las bombas.

El sector agrícola también se ha beneficiado de la IoT. Ahora es posible alimentar y monitorear el ganado de forma más específica por medio de etiquetas de nombre / número que contienen información en un chip de identificación por radiofrecuencia (RFID). Se pueden enterrar sensores electroquímicos para medir la exposición a la luz solar, así como los niveles de saturación de agua y la presencia de nutrientes esenciales como el fósforo y el nitrógeno. Además, las familias de bajos ingresos que viven en regiones remotas o en zonas urbanas sin acceso a la red eléctrica formal están utilizando tecnologías de la IoT junto con células solares para proveer de energía a sus hogares. Los costos del capital inicial de las unidades solares se amortizan y se pagan a través de servicios de dinero móvil; las células solares comunican el nivel y la utilización de las baterías en forma regular a través de comunicaciones de datos.

Estos son apenas algunos ejemplos que ponen de relieve el impacto de la IoT como herramienta para alcanzar los Objetivos de Desarrollo del Milenio de las Naciones Unidas (ODM) y los Objetivos de Desarrollo Sostenible (ODS) que pronto estarán disponibles. Sin embargo, todavía existen desafíos, especialmente en lo que respecta a la infraestructura, la capacidad técnica y la promoción de entornos regulatorios que le den la bienvenida a las intervenciones de la IoT. Una mayor atención al potencial de IoT4D ayudará a aumentar su impacto y su eficacia en la lucha contra algunos de los desafíos de desarrollo más importantes de nuestro tiempo.

Fuente: "Harnessing the Internet of Things for Global Development", por Cisco y la Comisión de la Banda Ancha para el Desarrollo Sostenible de la UIT/UNESCO (disponible pronto).

Preguntas sobre la IoT y su relación con las economías emergentes y el desarrollo

Para asegurar que las oportunidades y los beneficios relacionados con la IoT sean globales, es necesario considerar las necesidades específicas y los potenciales desafíos relacionados con las economías emergentes. Los asuntos discutidos en las secciones anteriores no son exclusivos de los países industrializados y se deben considerar aplicables a los mercados en desarrollo. Sin embargo, las circunstancias únicas que suelen encontrarse en las economías emergentes plantean algunas otras preguntas con respecto a la maximización de los beneficios y la gestión de los desafíos de la IoT. Aunque este listado no es en absoluto exhaustivo, algunas áreas a considerar incluyen las siguientes:

RECURSOS DE INFRAESTRUCTURA

La infraestructura de Internet y las comunicaciones se han propagado rápidamente por todo el mundo en desarrollo, aunque en muchos países todavía existen lugares donde no es posible asegurar un acceso confiable, de alta velocidad y asequible, incluso para uso comercial y de negocios. ¿En qué medida la Internet de las Cosas ejercerá presión sobre la infraestructura y los recursos de Internet y las telecomunicaciones? ¿Los desafíos actuales frenarán las oportunidades de la IoT en las regiones emergentes? ¿O será la IoT un generador de demanda que impulsará la construcción de más infraestructura? ¿Es necesario prestar especial atención a la gestión del espectro, teniendo en cuenta que muchas implementaciones de la IoT se sustentan en la tecnología inalámbrica? A medida que los servicios en la nube y los análisis de datos relacionados incorporen valor en muchos servicios de la IoT, ¿la relativa escasez de infraestructura de centros de datos en las economías emergentes representará un obstáculo para el despliegue?

INVERSIÓN

En los países industrializados, la inversión en investigación y desarrollo de productos para la IoT está siendo impulsado por las oportunidades de mercado para diferentes productos y servicios. ¿Hasta qué punto el mercado impulsará la inversión en implementaciones de la IoT en los países en desarrollo, sobre todo más allá de las aplicaciones en industrias y entornos con una clara perspectiva de retorno a corto plazo? Por el contrario, ¿los despliegues de la IoT en las economías emergentes serán más eficientes y rentables? Dada la menor cantidad de sistemas heredados que suelen existir en estas economías, ¿podrán saltearse la generación tecnológica que está en uso en el resto

del mundo? ¿Los gobiernos deberían incentivar el desarrollo de soluciones técnicas innovadoras por parte de los investigadores y las industrias locales?

DESARROLLO TÉCNICO Y DE LA INDUSTRIA

¿En qué medida están participando investigadores y emprendedores de los países emergentes en el desarrollo técnico y el despliegue de la IoT? ¿Qué se debe hacer para fomentar su participación en el desarrollo de soluciones técnicas y aplicaciones que satisfagan las necesidades y oportunidades de estos mercados, que a la vez sean respetuosas de las normas culturales y que construyan niveles adecuados de seguridad y protección de la privacidad? ¿Qué nuevas habilidades pueden ser necesarias en las economías emergentes para construir, desplegar y gestionar sistemas de la IoT? ¿Las industrias en las economías emergentes están listas para aprovechar la tecnología de la IoT? ¿Quedarán rezagadas o estarán en mejores condiciones de saltearse las tecnologías industriales más antiguas? ¿Cómo pueden los investigadores y las industrias de los países con economías emergentes posicionarse para desarrollar soluciones a los desafíos económicos y sociales locales que tienen un impacto directo en sus sociedades?

COORDINACIÓN REGULATORIA Y DE POLÍTICAS

En los últimos diez años, los formuladores de políticas y reguladores de las economías emergentes han logrado avances significativos en cuanto al desarrollo y la adaptación de las políticas y regulaciones existentes para fomentar el crecimiento de Internet y hacer frente a los desafíos relacionados. En las economías emergentes, los formuladores de políticas tecnológicas deben enfrentar importantes exigencias, especialmente en vista de la velocidad de los desarrollos y las limitaciones de los recursos. Aunque la IoT promete nuevas oportunidades, también agregará una nueva dimensión de complejidad. ¿Qué información y recursos necesitan ahora los formuladores de políticas de las economías emergentes para tener en cuenta las exigencias de políticas y otras preguntas que surgirán con el crecimiento de la IoT?

NOTAS DE LA SECCIÓN

Cuestiones relacionadas con las economías emergentes y el desarrollo

97. *Ibid.*

98. La Coalición Dinámica del Foro de Gobernanza de Internet sobre la Internet de las Cosas (DC IoT) ha dedicado mucho esfuerzo a la consideración del impacto y los desafíos de la IoT en las economías emergentes y en desarrollo. Ver el sitio web de la DC IoT http://www.iot-dynamic-coalition.org/ fpara ver discusiones relacionadas con este tema.

99. Manyika, James, et. al., *The Internet of Things: Mapping the Value beyond the Hype*. McKinsey Global Institute, junio de 2015. p. 4. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

100. Manyika, James, et. al., p. 4-5.

101. La lista de Objetivos y metas de Desarrollo Sostenible de las Naciones Unidas se puede consultar en https://sustainabledevelopment.un.org/topics.

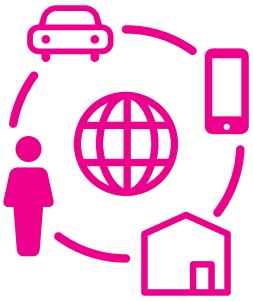
102. Los miembros de la Internet Society han formado un Grupo de Interés Especial para investigar específicamente los problemas que surgen en la intersección de la Internet, la IoT y el sector de los alimentos. Para obtener más información sobre el Grupo de Interés Especial de ISOC sobre Alimentos, diríjase a http://internet-of-food.org/

103. Botterman, Maarten. *Policy Paper on IoT Future Technologies: Opening towards a New Reality*. Issue brief no. D5.2. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf

104. "Digital Farm Set for Internet's next Wave." *The Guardian*, 20 de septiembre de 2015, sec. connecting the future. http://www.theguardian.com/connecting-the-future/2015/sep/21/digital-farm-set-for-internets-next-wave

CONCLUSIÓN

CONCLUSIÓN



Aunque el concepto de combinar computadoras, sensores y redes para monitorear y controlar diferentes dispositivos ha existido durante décadas, la reciente confluencia de tecnologías clave y tendencias de mercado está marcando el comienzo de una nueva realidad para la "Internet de las Cosas". La IoT promete abrir la puerta a un mundo revolucionario, un mundo "inteligente" totalmente interconectado en el cual las relaciones entre los objetos y su entorno y las personas se entrelazarán aún más. La perspectiva de la Internet de las Cosas como una matriz omnipresente de dispositivos conectados a Internet podría cambiar radicalmente la definición de lo que significa estar "en línea".

Aunque las potenciales ramificaciones son significativas, hay una serie de problemas que podrían interponerse en el camino de esta visión, particularmente en las áreas de la seguridad; la privacidad; la interoperabilidad y los estándares; temas legales, reglamentarios y de derechos; y la inclusión de las economías emergentes. La Internet de las Cosas implica un complejo conjunto de consideraciones tecnológicas, sociales y políticas en constante evolución y que atraviesa un conjunto diverso de partes interesadas. La Internet de las Cosas está sucediendo ahora mismo, por lo que es necesario hacer frente a sus desafíos, maximizar sus beneficios y simultáneamente reducir sus riesgos.

A la Internet Society le importa la IoT, ya que representa un componente cada vez mayor de la manera en que las personas y las instituciones probablemente interactuarán con Internet e incorporarán la conectividad en sus vidas personales, sociales y económicas. Un debate polarizado que enfrente a las promesas de la IoT contra sus posibles peligros no permitirá encontrar soluciones que maximicen los beneficios de la IoT y a la vez minimicen sus riesgos. Por el contrario, para definir las formas más eficaces de avanzar, se necesitará la participación informada, el diálogo y la colaboración de una variedad de partes interesadas.

MÁS INFORMACIÓN

Una amplia variedad de organizaciones, alianzas y esfuerzos gubernamentales de todo el mundo están abordando cuestiones relacionadas con la Internet de las Cosas. La siguiente lista de fuentes de información adicionales no es en absoluto exhaustiva, sino que más bien pretende ser un punto de partida para una mayor investigación.

Organizaciones y alianzas que están trabajando en Internet de las Cosas

AIOTI, Alliance for Internet of Things Innovation
Esta alianza fue lanzada por la Comisión Europea para apoyar el desarrollo de un ecosistema europeo para la IoT que también incluyera políticas de normalización. https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti

AllSeen Alliance
AllSeen Alliance es un grupo formado por 180 miembros de la industria que promueve la adopción generalizada de un marco de comunicación entre pares interoperable basado en AllJoyn para dispositivos y aplicaciones de la IoT. https://allseenalliance.org/

ETSI, European Telecommunications Standards Institute
La iniciativa del ETSI llamada *Connecting Things* está elaborando normas para la seguridad, la gestión, el transporte y el procesamiento de los datos relacionados con la potencial conexión de miles de millones de objetos inteligentes a una red de comunicaciones. http://www.etsi.org/technologies-clusters/clusters/connecting-things

IEC 62443/ISA99
El Comité de Seguridad para Sistemas de Automatización y Control Industrial elabora normas, informes técnicos y procedimientos para la implementación de sistemas seguros para la automatización y el control industrial. http://isa99.isa.org/ISA99%20Wiki/Home.aspx

IEEE (including P2413)
El IEEE tiene una iniciativa dedicada a la IoT y un centro de información para la comunidad técnica que participa en la investigación, la implementación, la aplicación y el uso de las tecnologías de la IoT. http://iot.ieee.org/

IERC, European Research Cluster
El Cluster Europeo para la Investigación de la Internet de las Cosas coordina las actividades relacionadas con la IoT en toda Europa. http://www.internet-of-things-research.eu/

Internet Engineering Task Force (IETF)
El principal órgano de estandarización de Internet tiene una Dirección dedicada a la IoT que coordina los esfuerzos de todos sus grupos de trabajo, revisando las especificaciones para verificar que sean coherentes y monitoreando las actividades relacionadas con la IoT que llevan a cabo otros grupos de normalización. https://trac.tools.ietf.org/area/int/trac/wiki/IOTDirWiki

IIC, Industrial Internet Consortium
El IIC se ha asociado con la OIC para acelerar la entrega de un marco arquitectónico de grado industrial para la IoT. En 2015, el IIC publicó una arquitectura de referencia para la IoT. http://www.industrialinternetconsortium.org/

IGF, Foro de Gobernanza de Internet
El FGI auspicia la Coalición Dinámica sobre la IoT, que organiza reuniones abiertas para discutir los desafíos globales que deben ser abordados en relación con el despliegue de la IoT. http://www.intgovforum.org/cms/component/content/article?id=1217:dynamic-coalition-on-the-internet-of-things

Internet of Things Consortium
Este grupo ofrece servicios de educación del consumidor e investigación de mercado con el objetivo de impulsar la adopción de productos y servicios de la IoT. http://iofthings.org/#home

IPSO, IP for Smart Objects Alliance
Dedicada a facilitar la IoT, IPSO busca establecer el protocolo IP como base para la conexión de objetos inteligentes a través de la educación, la investigación y la promoción. http://www.ipso-alliance.org/

ISO/IECJTC-1
EN 2014, ISO publicó un informe preliminar sobre la IoT, además de un informe sobre ciudades inteligentes. El grupo actualmente tiene subcomités en ambas áreas. http://www.iso.org/iso/internet_of_things_report-jtc1.pdf

Grupo de Interés Especial de ISOC sobre Alimentos
Este grupo de interés especial lidera la discusión sobre los estándares necesarios para la infraestructura técnica que requerirá la industria alimentaria en el futuro. http://internet-of-food.org/

UIT, Unión Internacional de Telecomunicaciones
La UIT organizó una Iniciativa de Estándares Globales para la IoT que concluyó sus actividades en julio de 2015, luego de lo cual se formó un nuevo Grupo de Estudio 20 cuyo foco son las aplicaciones de la IoT. http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx

Fundación MAPI, Manufacturers Alliance for Productivity and Innovation
Esta fundación está desarrollando Industrie 4.0 para aplicaciones industriales de la IoT. https://www.mapi.net/research/publications/industrie-4-0-vs-industrial-internet

OASIS
OASIS está desarrollando protocolos abiertos para garantizar la interoperabilidad de la IoT. El grupo escogió el protocolo MQTT (*Message Queuing Telemetry Transport*) como su protocolo para la IoT y ha optimizado MQTT-S-N para redes de sensores inalámbricos. OASIS tiene tres comités técnicos trabajando en la IoT supervisando MQTT y otros dos estándares, AMQP (*Advanced Message Queuing Protocol*) y oBIX (*OASIS Open Building Information Exchange*). https://www.oasis-open.org/committees/tc_cat.php?cat=iot

oneM2M
Dedicado al desarrollo de una arquitectura y estándares para las comunicaciones 'máquina a máquina', este grupo donde se congregan múltiples fabricantes trabaja en las áreas de la telemedicina, la automatización industrial y la automatización del hogar. Su objetivo es lograr una capa de servicio común para la comunicación M2M que se pueda embeber en el hardware y el software. http://www.onem2m.org/

Online Trust Alliance
Este grupo de proveedores de seguridad ha desarrollado un proyecto de marco de confianza para las aplicaciones de la IO que se centra en la seguridad, la privacidad y la sostenibilidad. https://otalliance.org/initiatives/internet-things

The Open Management Group
Este consorcio de normalización técnica está desarrollando varios estándares para la IoT, entre ellos el DDS (*Data Distribution Service*) y el IFML (*Interaction Flow Modeling Language*), junto con marcos de confiabilidad, modelado de amenazas y un modelo de componentes unificados para sistemas en tiempo real y embebidos. http://www.omg.org/hot-topics/iot-standards.htm

Open Web Application Security Project
OWASP patrocina un proyecto Top Ten de la IoT diseñado para ayudar a que los fabricantes, desarrolladores y consumidores comprendan los problemas de seguridad relacionados con su lista de las superficies de ataque más significativas para la IoT. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

Smart Grid Interoperability Panel
SGIP tiene una iniciativa llamada EnergyIoT que se dedica a buscar nuevas oportunidades para la IoT dentro de la industria de la energía. El OpenFMB del grupo es un proyecto liderado por las empresas de servicios públicos que está incorporando modelos de datos de uso habitual en el sector y protocolos de comunicación de la IoT para crear un bus de comunicaciones estándar (*Open Field Message Bus*). http://iofthings.org/#home

Thread Group
Este grupo de fabricantes de dispositivos para hogares inteligentes está desarrollando un protocolo de red común que soportará dispositivos que se comunican mediante IP en el hogar, entre ellos electrodomésticos, luces y sistemas de seguridad. http://threadgroup.org/About.aspx

Iniciativas gubernamentales de desarrollo de políticas, investigación y cooperación

Australia
CISRO (Australia Commonwealth Scientific and Industrial Research Organisation), la agencia nacional de ciencias de Australia, lidera los esfuerzos de investigación y desarrollo en materia de la IoT. http://www.csiro.au/en/Research/DPF/Areas/Autonomous-systems/IoT

China
El Gobierno Popular Central de la República Popular China ha publicado un documento programático titulado "Directrices para promover un desarrollo ordenado y saludable de la Internet de las Cosas" que describe la política nacional de China para la IoT. http://www.gov.cn/zwgk/2013-02/17/content_2333141.htm

China
El Ministerio de Industria y Tecnología de la Información de la República Popular China publicó el "12º Plan quinquenal", un documento donde se planifica el desarrollo de la IoT. http://kjs.miit.gov.cn/n11293472/n11295040/n11478867/14344522.html

Unión Europea
Agenda Digital de la Comisión Europea para Europa, Internet de las Cosas – La Comisión está trabajando con los estados miembros con vistas al futuro despliegue de la IoT. El grupo ha compilado listas de proyectos piloto y de investigación sobre la IoT en Europa. http://ec.europa.eu/digital-agenda/en/Internet-things

Unión Europea
Grupo de Trabajo de la Comisión Europea sobre la Internet de la Cosas (EO2514) – Este grupo de expertos asesora a la Comisión sobre los desafíos técnicos, legales y organizativos que presenta el despliegue de la IoT en toda Europa. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2514

India
El Ministerio de Comunicaciones y TIC del Gobierno de India centra su atención en el desarrollo de un ecosistema de la industria de la IoT como iniciativa prioritaria para transformar a India en una sociedad digital y una economía del conocimiento. http://deity.gov.in/content/internet-things

República de Corea
En 2014, el Ministerio de Ciencia, TIC y Planificación a Futuro de la República de Corea publicó un "Plan rector para la construcción de la Internet de las Cosas (IoT) que lidere la revolución digital hiperconectada" (disponible a través del sitio web de la Asociación Korea IOT en http://karus.or.kr/uploadFiles/board/KOREA-IoT%20Master%20Plan.pdf).

Singapur
SPRING Singapore, la autoridad encargada del desarrollo de las TIC en Singapur (IDA) y el Comité de Estándares para Tecnología de la Información (ITSC), bajo la jurisdicción del Comité de Normalización de Singapur (SSC), han redactado un Proyecto de Estándares para la Internet de las Cosas (IoT) en apoyo de la iniciativa llamada *Smart Nation*. http://www.spring.gov.sg/NewsEvents/PR/Pages/Internet-of-Things-(IoT)-Standards-Outline-to-Support-Smart-Nation-Initiative-Unveiled-20150812.aspx

https://www.ida.gov.sg/Tech-Scene-News/Tech-News/Tag?tag=internet+of+things

Reino Unido
En 2015, el Asesor Científico en Jefe del Gobierno del Reino Unido publicó un informe delineando los objetivos de la IoT titulado "La Internet de las Cosas: Cómo aprovechar al máximo la Segunda Revolución Digital". https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

Reino Unido
Ofcom, el regulador de comunicaciones del Reino Unido, ha identificado varias áreas prioritarias que promoverán el despliegue de la IoT, entre ellas la disponibilidad de espectro, la privacidad de los datos, la seguridad de las redes, la resiliencia y las direcciones de red. http://stakeholders.ofcom.org.uk/consultations/iot/next-steps/

Estados Unidos
La Comisión Federal de Comercio de los Estados Unidos creó la Oficina de Investigación en Tecnología (OTRI) para explorar, entre otros temas, la privacidad, la seguridad y los problemas de pago relacionados con la IoT. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

NOTAS Y AGRADECIMIENTOS

La Internet de las Cosas—Una breve reseña
Problemas y desafíos de un mundo más conectado

Este trabajo fue preparado por:

Karen Rose
Directora Senior de Estrategia y Análisis, Internet Society

Scott Eldridge
Director, Cam & Sprocket LLC y Miembro Individual de la Internet Society

Lyman Chapin
Director, Interisle Consulting Group y Miembro Individual de la Internet Society

Los autores desean agradecer a los miembros del grupo de trabajo de la Internet Society que perfeccionó el concepto para este trabajo y ofreció su orientación y aportes durante todo su desarrollo: Michael Kende, Graham Minton, Steve Olshansky, Robin Wilton, Greg Wood y Dan York. También desean agradecer al personal de la Internet Society que contribuyó a la revisión de este documento y aportó sus valiosas opiniones y puntos de vista: Joyce Dogniez, Olaf Kolkman, Megan Kruse, Ted Mooney, Christian O'Flaherty, Maarit Palovirta, Bastiaan Quast, Andrei Robachevsky, Phil Roberts, Christine Runnegar, Sally Wentworth, Fernando Zarur y Jan Žorž.

Ofrecemos un especial agradecimiento a la comunidad de miembros, capítulos y colaboradores de la Internet Society que generosamente donaron su tiempo y experiencia para revisar y comentar sobre borradores anteriores de este documento: Nicolas Antoniello, Grunela Astbrink, Hosein Badran, Maarten Botterman, Vint Cerf, Sri Chandra, Glenn Deen, Tim Denton, Patrik Fältström, John Garrity, Andrés Gomez, Richard Hill, Howard Lee, Mike O'Reirdan, Robert Pepper, Alejandro Pisanty, Chip Sharp, Bert Wijnen y Paul Wilson.

Edición: Carolyn Marsan
Diseño de la cubierta: Michelle Speckler

Para obtener más información, diríjase a
https://www.internetsociety.org/iot

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444 • Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tel: +1 703 439 2120 • Fax: +1 703 326 9881
Email: info@isoc.org

report-InternetofThings-20151015-en