La Internet de las cosas

Un informe de la política pública de Internet Society (ISOC)

2 de agosto de 2016

Introducción

La Internet de las cosas es un término amplio que se utiliza para describir situaciones en las que la conectividad a Internet y las capacidades informáticas se extienden a dispositivos, sensores y artículos cotidianos que no se consideran habitualmente computadoras (por ejemplo: productos de consumo, autos y camiones, componentes industriales, monitores de salud portátiles y colecciones de dispositivos que funcionan juntos para crear conceptos tales como "ciudades inteligentes" y "casas inteligentes"). Estos objetos recolectan datos de sus alrededores que luego se transmiten y analizan de manera remota para crear nuevas perspectivas, entregar servicios y controlar otros dispositivos.

Las proyecciones de impacto de la IoT, tanto en Internet como en la economía, son impresionantes: algo así como 100 mil millones de dispositivos de IoT conectados[1] y un impacto económico global de más de $11 billones para el 2025[2]. La IoT promete proporcionar ventajas en la automatización industrial, la atención médica, la conservación de la energía, la agricultura, el transporte, la gestión urbana, así como también otros sectores y aplicaciones. El potencial para la innovación, aplicaciones y servicios de enorme crecimiento es una prueba para la naturaleza abierta de la arquitectura y diseño de Internet, que no limita a los tipos de dispositivos y servicios que pueden conectarse a ella.

No obstante, al mismo tiempo existen desafíos importantes asociados a la IoT que podrían obstaculizar la forma en que se vuelven realidad sus posibles beneficios. Algunos de los desafíos y preguntas más apremiantes incluyen asuntos de seguridad, privacidad, interoperabilidad y estándares, así como también asuntos regulatorios y legales, y la predisposición de las economías emergentes a adoptarla.

A menudo referida como *la Internet de las cosas (IoT),* se espera que miles de millones de dispositivos inteligentes se pongan en línea en la década que viene, acercando la promesa de oportunidades económicas globales y nuevas innovaciones que transformarán la manera en que trabajamos, vivimos y jugamos. Sin embargo, los desafíos que vendrán con la IoT incluirán la seguridad y privacidad que deberán tenerse en cuenta para que la tecnología alcance su máximo potencial.

1 "Índice de conectividad global". Huawei Technologies Co., Ltd., 2015. Web. 6 Sept. 2015. http://www.huawei.com/minisite/gci/en/index.html.
2 Manyika, J.; Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R.; Bughin, J.; and Aharon, D. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015.

Este informe es una descripción de los asuntos clave de la IoT. Estos mismos asuntos se tratan en más detalle en el informe de Internet Society (ISOC), *La Internet de las cosas- una breve reseña. Para entender mejor los asuntos y desafíos de un mundo más conectado*.

Consideraciones clave

Aunque el interés en los dispositivos conectados ha aparecido en los últimos años, el concepto de conectar los objetos y los artículos para redes de comunicaciones y la Internet no es nuevo. Los sistemas de comunicaciones entre máquinas (M2M), que utilizaron redes propias más que la Internet, se extendieron en entornos industriales hace más de 25 años. Los primeros artículos cotidianos en ser controlados por medio de la Internet aparecieron a comienzos de la década de 1990 y establecieron el escenario para lo que hoy conocemos como la Internet de las cosas.

En la actualidad, la IoT representa un aspecto cada vez más creciente de la manera en que la gente y las instituciones interactúan con la Internet en sus vidas personales, sociales y económicas. También puede representar un cambio en la manera en que los usuarios se involucran con la Internet y cómo se ven afectados por esta. Por ejemplo, la experiencia de Internet actual se caracteriza ampliamente por usuarios que activamente bajan y generan contenido a través de sus computadoras y teléfonos inteligentes. Sin embargo, muchos dispositivos de IoT están diseñados para operar en un segundo plano, enviando y recibiendo datos por parte del usuario con muy poca intervención humana, o aun ni siquiera conocimiento; y otros están diseñados para controlar objetos y recursos físicos, como por ejemplo vehículos y edificios, o para controlar el comportamiento humano.

Si las proyecciones y tendencias sobre la IoT se vuelven realidad, sería pertinente considerar las implicaciones de un mundo en el cual la interacción más frecuente con la Internet proviniera de un compromiso pasivo con objetos conectados, y no uno activo con el contenido. Los gobiernos, por ejemplo, querrán asegurarse de que sus políticas estén al día con el entorno en rápido cambio.

Las políticas que promueven la infraestructura de la Internet, el uso eficiente del espectro inalámbrico, el desarrollo de los centros de datos y el empoderamiento y elección del usuario son de vital importancia en la evolución de la IoT. Y, a medida que la cantidad y naturaleza de los datos recolectados sobre los usuarios y sus entornos cambian por la IoT, se deberían considerar políticas de seguridad de privacidad y datos que reflejen la tecnología en evolución y sus impactos potenciales sobre los usuarios.

Más allá de la infraestructura directa y de los aspectos de telecomunicaciones de la IoT, otras áreas de políticas se pueden beneficiar de una evaluación. Los dispositivos de la IoT tocarán probablemente la mayor parte de aspectos de nuestras vidas, incluidos los dispositivos en nuestros hogares, lugares de trabajo, hospitales y otros espacios públicos. Así, es posible que afecten las políticas sobre privacidad, seguridad de datos, la atención médica, el transporte y la tecnología. Esta clase de amplio alcance sugiere que quienes crean las políticas necesitarán considerar las amplias implicaciones sobre las políticas a lo largo de un gran campo de objetivos e iniciativas de políticas.

Aunque la IoT no es una idea particularmente nueva desde una perspectiva técnica, su crecimiento y madurez presentarán tanto nuevos beneficios como nuevos desafíos que requerirán cambios en los acercamientos y estrategias de las políticas.

Desafíos

Se necesita abordar una gran cantidad de desafíos para ser plenamente conscientes de los beneficios potenciales para los individuos, las sociedades y las economías.

- **Seguridad.** Aunque las consideraciones sobre seguridad no son nuevas en el contexto de la tecnología de la información, los atributos de muchas de las implementaciones de la IoT presentan desafíos de seguridad nuevos y únicos.

  Los fabricantes enfrentan a menudo desafíos económicos y técnicos cuando construyen y mantienen características de seguridad sólidas en los dispositivos de la IoT. Sin embargo, los dispositivos y servicios con seguridad débil son vulnerables a ataques cibernéticos y pueden exponer los datos del usuario a robo. Esto es un desafío clave en la IoT porque un número mayor de dispositivos de la IoT en línea aumenta la cantidad de posibles vulnerabilidades de seguridad.

  Garantizar la seguridad de los productos y servicios de la IoT de por vida debe ser una prioridad fundamental para mantener la confianza total del usuario en esta tecnología. Los usuarios necesitan confiar en que los dispositivos de la IoT y los servicios de datos relacionados son seguros, especialmente a medida que se vuelven más omnipresentes e integrados a nuestras vidas diarias.

  En principio, los desarrolladores y los usuarios de dispositivos y sistemas de la IoT tienen una obligación colectiva de asegurar que no exponen a sus usuarios ni la misma Internet a un posible daño. Las acciones de la industria, el gobierno, los usuarios y otros contribuirán a asegurar el desarrollo, el mantenimiento y el uso de los dispositivos de la IoT.

  Internet Society (ISOC) cree que se necesitará un acercamiento colaborativo a la seguridad de la IoT para desarrollar soluciones eficaces y apropiadas que se adapten adecuadamente a la escala y complejidad de estos asuntos.

- **Privacidad.** La capacidad de recolectar, analizar y transformar datos es lo que impulsa la mayor parte del valor de los dispositivos y servicios de la IoT, pero estos datos también se pueden utilizar para delinear perfiles detallados e invasivos de los usuarios. En realidad, la IoT está redefiniendo el debate sobre asuntos de privacidad, puesto que muchas implementaciones pueden cambiar drásticamente la manera en que se recolectan, analizan y utilizan los datos.

  Específicamente, la IoT amplía las preocupaciones sobre un aumento potencial de monitoreo y seguimiento y la cantidad de datos sensibles que pueden recolectarse a través de los dispositivos que operan en nuestros entornos hogareños, de negocios y públicos. Algunas veces, estos dispositivos recolectan datos sobre los individuos sin que estos lo sepan o sin su consentimiento. Además, aunque los datos de estos dispositivos benefician a sus dueños, también pueden beneficiar con frecuencia al fabricante o proveedor del dispositivo. Esto se convierte en un tema serio de privacidad cuando los

individuos observados por los dispositivos de la IoT tienen expectativas de privacidad distintas con respecto al alcance y utilización de esos datos que las que tienen quienes recolectan los datos.
Los dispositivos de la IoT que recolectan datos sobre la gente en una jurisdicción pueden transmitir esos datos a otra jurisdicción para almacenamiento o procesamiento. Pueden generarse complicaciones si los datos recolectados son personales o sensibles y están sujetos a leyes de protección de datos en varias jurisdicciones.

Permitir flujos de datos transfronterizos que protejan la privacidad y promuevan la seguridad legal para los usuarios y los proveedores de la IoT será clave para la promoción de un crecimiento global de la IoT.

Aunque los desafíos de privacidad son considerables, no son inconmensurables. Se necesita desarrollar estrategias que promuevan la transparencia, la justicia y la elección del usuario en la recolección y el tratamiento de datos que mejoren las expectativas y los derechos de privacidad del usuario a través de una variedad de preferencias que impulsen la innovación en la tecnología y servicios nuevos.

- **Interoperabilidad y estándares.** La interoperabilidad entre los dispositivos de la IoT y los flujos de datos pueden motivar la innovación y proveer eficiencias para los fabricantes y usuarios de dispositivos, aumentando así los beneficios finales y el valor económico. McKinsey Global Institute estima que la interoperabilidad de dispositivos conducirá al 40 % del valor potencial generado por la IoT. [3]

  Aunque la interoperabilidad completa a través de productos y servicios no siempre es posible ni necesaria, los compradores pueden dudar si comprar o no productos y servicios con la IoT si no hay una flexibilidad de la integración, alta complejidad de propiedad, espacios protegidos (plataformas o ecosistemas cerrados) y preocupación sobre la dependencia de un proveedor. Las consideraciones sobre la interoperabilidad y los estándares también se extienden a los datos recolectados y procesados por los servicios de la IoT, puesto que los formatos de datos propios o incompatibles pueden representar desafíos actuales para los usuarios que buscan integrar sistemas, tienen la flexibilidad para cambiar a servicios diferentes, o realizar un análisis adicional sobre los datos recolectados. En resumen, un entorno fragmentado de implementaciones técnicas propias y formatos de datos[4] inhibirá el valor y la flexibilidad de la IoT tanto para usuarios como para la industria.

  El mercado actual ofrece una variedad de aproximaciones técnicas a la IoT. Algunas empresas consideran que el desarrollo de ecosistemas propios presenta ventajas estratégicas, mientras que otras desarrollan sus propios enfoques debido a que aún no existen tecnologías comunes. Un amplio rango de empresas, grupos industriales e investigadores se encuentran desarrollando enfoques que generen mayor interoperabilidad y estándares para IoT.

3 ibid.
4 Para acceder a información sobre las actividades de la Internet Engineering Task Force (IETF) y la Internet Architecture Board (IAB) para promover la estandarización e interoperabilidad de IoT, consulte https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf y https://www.iab.org/activities/workshops/iotsi/.

Internet Society (ISOC) considera que la mayor interoperabilidad y el uso de estándares genéricos, abiertos, voluntarios y de amplia disponibilidad como soportes técnicos para dispositivos y servicios IoT (como el Protocolo de Internet, o IP) se traducirán en mayores beneficios para los usuarios, innovaciones y oportunidades económicas.

- **Asuntos jurídicos, de derechos y de regulación.** La IoT amplifica y vuelve a introducir muchas interrogantes jurídicas y de regulación. Existe el riesgo de que el ritmo acelerado de los cambios en la tecnología de IoT se adelante a la capacidad de adaptación de las estructuras reguladoras, jurídicas y de políticas.

  Una de estas cuestiones es el posible conflicto entre la vigilancia policial y los derechos civiles. Los dispositivos de IoT ofrecen posibles beneficios para el cumplimiento de la ley, la seguridad pública y la administración pública. Sin embargo, también presentan posibles inquietudes respecto a los posibles derechos humanos y civiles en lo relacionado con la penetrabilidad del monitoreo de la sociedad, los usos secundarios de la información por parte del gobierno, y el acceso a la información a partir de dispositivos de la IoT personales por parte de las autoridades policiales o como evidencia en acciones jurídicas, entre otras cuestiones desafiantes.

  Además, los dispositivos de la IoT presentan interrogantes de responsabilidad jurídica. Una pregunta fundamental es la siguiente: Si alguien resulta perjudicado como consecuencia de la acción o inacción de un dispositivo IoT, ¿quién es responsable? La respuesta suele ser complicada y, en muchos casos, no hay suficientes criterios jurisprudenciales para respaldar alguna postura. Como los dispositivos IoT operan de una manera más compleja que los productos independientes, se deben contemplar situaciones de responsabilidad más complejas.

  Dada la amplia naturaleza de los desafíos de políticas y regulaciones que presenta IoT, es necesario un enfoque de gobernanza colaborativa respecto al desarrollo de políticas que se base en los comentarios y la participación de una variedad de actores para obtener los mejores resultados.

- **Asuntos de desarrollo y economías emergentes.** La IoT es muy prometedora en cuanto a los beneficios sociales y económicos que puede brindar a las economías emergentes y en desarrollo en áreas como agricultura sostenible, calidad y uso del agua, atención médica, industrialización, monitoreo del clima y gestión ambiental.

  Por ejemplo, las redes de sensores están ayudando a los aldeanos e investigadores de Asia y África a mejorar la entrega de agua potable mediante el control de la calidad del agua en la fuente y el rendimiento de las bombas de suministro. Además, se han implementado monitores inalámbricos de suelo, clima y ganado y equipos de agricultura automatizados con IoT en regiones en

desarrollo para ayudar a los agricultores a aumentar la productividad.[3] Con estos ejemplos y más, IoT es una herramienta muy prometedora para cumplir los Objetivos de Desarrollo Sostenible de las Naciones Unidas.[4]

Las regiones en desarrollo también presentan desafíos particulares relacionados con la implementación, el crecimiento, la implementación y el uso de tecnología. Estos desafíos incluyen la implementación de infraestructura adecuada de Internet y comunicaciones básicas en áreas rurales y remotas, incentivos para la inversión y participación local en las soluciones de desarrollo con IoT. Para que los beneficios de IoT sean verdaderamente globales, se deberán tratar las necesidades y desafíos específicos de la implementación en regiones menos desarrolladas.

Principios orientativos

Dada la adopción anticipada de dispositivos IoT, sus posibles beneficios económicos y sociales y los desafíos relacionados aumentaron el conocimiento por parte del sector público sobre la tecnología IoT, y la importancia de los asuntos que la acompañan es esencial. Se insta a los Gobiernos a tomar las siguientes medidas para acomodar y fomentar la implementación de IoT.

- **Promover el crecimiento de Internet y de la infraestructura de datos.** Los Gobiernos deben promover la expansión de la infraestructura por cable e inalámbrica, incluidas las áreas rurales y remotas, y deben considerar las necesidades de IoT para el uso con licencia y sin licencia del espectro. Se deben eliminar las barreras al desarrollo de centros de datos y de sistemas basados en el usuario para el análisis de datos de IoT, tales como grandes impuestos a los equipos o requisitos de licencia. Los Gobiernos deben revisar la infraestructura existente de Internet que poseen en miras al potencial aumento de las necesidades de comunicación de datos de los dispositivos IoT.

- **Fomentar la implementación de IPv6.** IPv6 es una tecnología que habilita el crecimiento de Internet, y se volverá cada vez más crítica a medida que IoT incremente el número de dispositivos conectados. Los Gobiernos deben hacer de la adopción del IPv6 una prioridad nacional e involucrar a los actores de su comunidad para que fomenten la implementación del IPv6.[5]

- **Fomentar estándares IoT voluntarios y abiertos.** Al emplear mayor interoperabilidad y utilizar estándares abiertos, voluntarios y de amplia disponibilidad como soportes técnicos para los dispositivos IoT, se obtendrán mayores innovaciones, oportunidades económicas y beneficios para los usuarios. Los Gobiernos deben abstenerse de dirigir los alcances técnicos respecto a IoT y, en su lugar, alentar a la industria, los investigadores y otros actores a trabajar en

3 Para más ejemplos sobre el modo en que IoT respalda el desarrollo, consulte "Harnessing the Internet of Things for Global Development", https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf.
4 Encontrará información sobre los Objetivos de Desarrollo Sostenible de las Naciones Unidas en https://sustainabledevelopment.un.org/sdgs.
5 Encontrará más orientaciones sobre IPv6 en el informe de la política ISOC IPv6, http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-IPv6-20160419-en.pdf.

conjunto en la implementación de estándares abiertos y basados en el consenso que sean compatibles con la interoperabilidad.

- **Adoptar un enfoque colaborativo y de múltiples actores para los debates sobre políticas para IoT.** IoT es un área desafiante para los legisladores, ya que es un entorno en rápido desarrollo y su tecnología abarca muchas industrias y usos. Será necesario un enfoque de gobernanza colaborativa, que aproveche la experiencia y la participación de una amplia variedad de actores, para desarrollar soluciones eficaces y adecuadas.[6] Las políticas deberían apuntar a la promoción de la capacidad de los usuarios de conectar, hablar, innovar, compartir, elegir y confiar de una manera tal que promueva la innovación y valide los derechos de los usuarios.

- **Fomentar un enfoque colaborativo a la seguridad de IoT.** Internet Society (ISOC) considera que la seguridad de IoT es responsabilidad colectiva de todos los que desarrollan y utilizan dispositivos IoT. Los participantes del espacio de IoT deben adoptar un enfoque colaborativo a la seguridad dentro de su amplia comunidad de múltiples actores asumiendo responsabilidad, compartiendo las mejores prácticas y lecciones aprendidas, fomentando el diálogo sobre la seguridad, y enfatizando el desarrollo de soluciones flexibles y compartidas de seguridad que puedan adaptarse y evolucionar a medida que las amenazan cambian con el paso del tiempo. La política de seguridad de IoT debería centrarse en permitir a los participantes resolver los asuntos de seguridad cerca del lugar en donde ocurren, en lugar de centralizar la seguridad de IoT en unos pocos miembros, al tiempo que se preservan las propiedades fundamentales de Internet y los derechos de los usuarios.[7]

- **Fomentar prácticas de diseño responsable para los servicios de IoT.** Se deben alentar las prácticas de seguridad por diseño y privacidad por diseño para los dispositivos IoT. Ya sea mediante la regulación de protección de datos y privacidad, la autorregulación voluntaria de la industria, u otros incentivos o políticas, se debe alentar a los desarrolladores de dispositivos IoT a respetar los intereses del usuario final respecto a privacidad y seguridad de los datos y considerar esos intereses como elementos centrales para el proceso de desarrollo de productos. Los diseñadores del sistema IoT también deben considerar el ciclo de vida completo de este para asegurarse de que los dispositivos obsoletos no presenten riesgos de seguridad y sean compatibles con la gestión responsable del medioambiente.

6 Está disponible un resumen del modelo colaborativo de múltiples actores para la gobernanza de la Internet en http://www.internetsociety.org/doc/internet-governance-why-multistakeholder-approach-works.
7 Está disponible un enfoque sobre la seguridad colaborativa en el informe de Internet Society, *Collaborative Security: An approach to tackling Internet Security Issues,* 2015. http://www.internetsociety.org/collaborativesecurity.

Recursos adicionales

Internet Society (ISOC) ha publicado varios documentos y contenido adicional relacionados con este asunto. Se puede acceder gratuitamente a ellos en su sitio web.

- Página web de recursos de IoT, http://www.internetsociety.org/iot.
- *The Internet of Things (IoT): An Overview - Understanding the Issues and Challenges of a More Connected World.* (2015). http://www.internetsociety.org/doc/iot-overview.
- "Adopción de IPv6". (2016). http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-IPv6-20160419-en.pdf.
- Páginas web de recursos de IPv6, http://www.internetsociety.org/deploy360/ipv6/.
- *Collaborative Security: An approach to tackling Internet Security Issues.* (2015). http://www.internetsociety.org/collaborativesecurity.