Ministerio de Modernización
Presidencia de la Nación

Internet de las Cosas

Secretaría de Tecnologías de la Información y las Comunicaciones

Introducción

Desde la Secretaría de Tecnologías de la Información y las Comunicaciones del Ministerio de Modernización analizamos las nuevas tendencias en materia de TIC y sus implicancias, con el objetivo último de ser facilitadores de su desarrollo, entendiendo que éstas puedan constituirse en beneficiosas para nuestro país y sus ciudadanos.

Consideramos que Internet se encuentra entre las expresiones más acabadas del nuevo paradigma de la sociedad de la información, influyendo en el desarrollo de nuevos procesos tecnológicos, económicos y de producción de bienes y servicios que han resultado en la denominada "Economía Digital".

Sostenemos asimismo que al involucrar directamente aspectos vinculados a la innovación , de carácter complejo y dinámico , es oportuno propiciar un espacio para el diálogo de todas las partes interesadas, promoviendo la participación de la comunidad técnica y académica, del sector privado y las organizaciones de la sociedad civil, en un marco institucional oficial, que facilite su participación y aportes con la finalidad de lograr una visión amplia y participativa sobre las cuestiones objeto de estudio.

En este sentido, mediante la Resolución 8/2016, esta Secretaría creó el Grupo de Trabajo de Servicios de Internet, cuyo objeto es analizar y proponer políticas públicas y regulaciones para la promoción y el desarrollo de servicios de Internet. Este grupo lleva adelante reuniones abiertas y consultas públicas para nutrirse de las experiencias, mejores prácticas y opiniones de todos los sectores del ecosistema de internet.

Por su parte, entendemos que Internet de las Cosas está llamada a transformar las dinámicas de consumo, los procesos productivos, las cadenas de valor en todas las industrias y, en definitiva, la forma de relacionarnos con lo que nos rodea. Por tal motivo generamos este documento de entendimiento inicial, que servirá de base para el trabajo posterior del Grupo de Trabajo de Servicios de Internet.

¿Qué entendemos por Internet de las cosas?

Definición

Internet de las cosas, "*Internet of Things"* o *IoT* (por sus siglas en inglés), es un concepto abstracto. De su nombre se desprende el concepto de cosas cotidianas que se conectan a Internet, pero en realidad se trata de mucho más que eso. IoT potencia objetos que antiguamente no estaban conectados a una red o que se conectaban mediante circuito cerrado, como comunicadores, cámaras, sensores, y demás, y les permite comunicarse globalmente mediante el uso de la red de redes.

Una posible definición de IoT es considerarla como una red que interconecta objetos físicos y virtuales valiéndose de Internet. Tales dispositivos utilizan software embebido, que le permite no solo la conectividad a Internet, sino que además brindan servicios en función de acciones dictadas remotamente las cuales pueden ser resultado de eventos específicos o del aprendizaje de la información recibida. En resumen, se trata de la interconexión digital de los objetos.

En tal sentido, la recomendación ITU Y.6060 de la Unión Internacional de Telecomunicaciones (UIT) establece que "...IoT puede ser considerada una infraestructura global para la sociedad de la información, permitiendo servicios avanzados para interconectar (física y virtualmente) cosas, basadas en tecnologías de la información y las comunicaciones interoperables. A través de la identificación, captura de datos, capacidades de comunicaciones y procesamiento, IoT hace un uso integral de las cosas para ofrecer servicios para todo tipo de aplicaciones mientras asegura que los requisitos de seguridad y privacidad sean cumplimentados".

Características

IoT consiste en desarrollos de software y hardware que cuentan con todas las herramientas necesarias para cumplir tareas muy específicas. Cada uno de los objetos conectados a Internet tiene un número de IP y mediante este puede ser accedido para recibir instrucciones. Asimismo, puede contactarse con un servidor externo y enviar los datos que recoja.

En este sentido, las principales características de IoT son:

- **Interconectividad:** Cualquier cosa se puede interconectar con la infraestructura global de TIC.
- **Servicios relacionados con las cosas:** IoT es capaz de proveer servicios relacionados con objetos sin los propios constreñimientos de las cosas, como la consistencia semántica entre las cosas *físicas* y las cosas asociadas a ellas virtualmente.
- **Heterogeneidad:** los dispositivos IoT son heterogéneos al estar basados en hardwares muy variados de plataformas y redes, y a su vez pueden interactuar con otros dispositivos o servicios en otras plataformas o redes.
- **Cambios dinámicos:** el estado de los dispositivos cambia muy dinámicamente, generalmente de acuerdo al

usuario. Por ejemplo, de dormir a despertarse, conectado o desconectado, y también de acuerdo al contexto y velocidad necesarias.

Estándares de IoT

La discusión relativa a los estándares de IoT tomó importancia a principios de 2013. La industria tecnológica, sin embargo, avanzaba en el desarrollo de IoT mucho más rápido de lo que lo hacía el desarrollo de estándares. Desde 2014, algunas organizaciones incluso empezaron a certificar sus productos, aunque de modo limitado. Sin perjuicio de ello, el estado actual de situación es muy lejano al establecimiento de un único estándar universal de IoT, y hay incluso quienes afirman que el establecimiento de un único estándar -tal como sucedió con el DVD o el Wi-Fi- es imposible.

La otra cuestión relativa al establecimiento de los estándares de IoT es si en verdad son necesarios o no. Algunos miembros de la industria siguen señalándolos como centrales, principalmente aquellos que se dedican a desarrollarlos.

Si resultara como las anteriores guerras de estándares, plataformas y formatos, los grandes players y se alinearán detrás de las distintas opciones, hasta que uno gane la delantera y de a poco la mayoría de los actores empiecen a alinearse detrás de aquél. Eventualmente, tal vez, los dispositivos de IoT puedan conectarse y hablar entre sí.

En tal sentido, es necesario tener en cuenta que IoT requiere diversa tecnología para funcionar: desde comunicaciones móviles, a seguridad de la información, a intercomunicaciones e interoperabilidad con otros dispositivos. Un único estándar muy probablemente no podrá cubrir esto, del mismo modo que el funcionamiento de una computadora portátil no es alcanzado por un único estándar.

Como consecuencia de lo anterior, se pueden considerar cuatro capas en las que se está trabajando en desarrollo de estándares de IoT: la primera es la capa de *aplicación*, en la que se mira los protocolos para desarrollar aplicaciones de IoT. Estas aplicaciones están siendo desarrolladas por organismos de normalización como el IETF, OASIS, OMA, W3C, entre otros. La segunda capa es la de *servicios*, donde se desarrollan marcos que permitan servicios de IoT. Estos marcos están siendo desarrollados por oneM2M, OIC, AllSeen, entre otros. La capa siguiente es la de *redes*, donde se presta atención a las optimizaciones que apoyan a IoT. Finalmente, la última capa es la de *tecnologías de acceso*, que busca optimizar las capas de aplicación y de servicios para el uso de servicios de IoT y optimizaciones específicas de acceso a redes. Estas optimizaciones de acceso están siendo desarrolladas por 3GPP, IEEE, Bluetooth SIG, Weightless SIG, entre otros.

A continuación se describen algunas de las entidades más relevantes que han desarrollado estándares de IoT de diverso tipo en el último año.

Tendencias de uso

El sector privado es aquel donde IoT se está haciendo cada vez más popular. Entre los sectores empresarios que están haciendo uso de este nuevo fenómeno, se pueden mencionar:

- **La industria de producción en masa:** la maquinaria que se encarga de controlar los procesos de fabricación, robots ensambladores, sensores de temperatura, control de producción, etc.
- **Control de infraestructura urbana:** control de semáforos, puentes, vías de tren, cámaras urbanas.
- **Control ambiental:** sensores atmosféricos, meteorológicos, sísmicos, etc.
- **Sector salud:** monitoreo activo de pacientes de manera ambulatoria y no invasiva.
- **Transporte:** seguimiento satelital, control del estado de los automotores, autos conectados, etc.
- **Industria energética:** Smart Grid, una solución para gestionar la demanda de electricidad e integrar fuentes de energía renovables, mejorar el servicio al cliente y reducir el consumo energético.

El gran pendiente al momento es el mercado de consumo, es decir, los hogares, pero poco a poco surgen dispositivos como lámparas, cerraduras, termostatos, etc.

Iniciativas en el mundo

La Unión Europea

La Comisión Europea, el órgano ejecutivo de la UE, ha creado la "Alianza para la Innovación de IoT". La Comisión Europea ha sugerido que las futuras regulaciones deben enfocarse en la seguridad, la privacidad, la protección al consumidor, el margen para la competitividad y elección de los usuarios.

La Comisión Europea realizó un informe, basado en consultas públicas sobre IoT. La consulta pública concluyó, entre otras cosas, lo siguiente:

Privacidad: Los representantes de la industria no querían ver cambios en las actuales normas de privacidad, a los fines de promover la innovación, mientras que la mayoría de las organizaciones de usuarios y consumidores consideraron a las actuales regulaciones de privacidad inadecuadas, y quieren que se elaboren guías de Evaluación de Impacto en Protección de Datos específicas para IoT.
Seguridad y protección: Representantes de la industria no quieren ver cambios en los actuales requerimientos de seguridad y no quieren que haya una "sobre-regulación". Los usuarios, en cambio, quieren ver que se creen estándares de seguridad para proteger la confidencialidad de los datos, su integridad y disponibilidad en un ecosistema de IoT.
Competencia: Los representantes de la industria respondieron que los dispositivos de IoT deberían ser interoperables para promover la competencia y la innovación de servicios. Sin embargo, señalaron que sistemas no interoperables que estén integrados verticalmente no deben ser obstaculizados por la legislación, principalmente en productos que no son destinados a usuarios finales.

Estados Unidos

En enero de 2015, la Federal Trade Commission (FTC) publicó un Informe sobre IoT. El informe fue preparado en conjunto con sobresalientes tecnólogos, académicos, representantes de la industria y de asociaciones de usuarios. El Informe se enfocó en asuntos de privacidad, seguridad y sobre si la legislación

requería que se regule o no IoT. Las conclusiones a las que llegaron fueron las siguientes:

Privacidad: El informe sugirió que las empresas incurran en una práctica de "minimización de datos", que implica que la recolección de los datos y el tiempo en que se lo retiene sea por el menor tiempo posible, teniendo en cuenta la necesidad para su uso.

Seguridad y Protección: El informe reconoció que la seguridad en un contexto de IoT ganó más importancia. Principalmente, el Informe señaló las múltiples maneras en que las violaciones a la seguridad pueden llevar hacia preocupaciones en la vida real. El Informe sugiere que las empresas prioricen embeber a los dispositivos de seguridad desde el inicio, entrenando adecuadamente a sus empleados, asegurando que los contratistas puedan mantener la seguridad, y que monitoreen los dispositivos e informen a los consumidores cuando se detecten violaciones a la seguridad.

El informe también sugiere que una legislación específica de IoT sería prematura. En cambio, recomienda que legislación amplia en temas de seguridad y privacidad deben ser aplicadas a estos asuntos, manteniendo una flexibilidad suficiente para adaptarse a las innovaciones tecnológicas.

Asia

Según RAND Europe, China dedica recursos considerables a la inversión en IoT. En 2012, destinó € 625 millones (USD 775 millones) a la inversión en IoT, en tanto que el Ministerio de Información y Tecnología de China estableció un fondo de USD 775 millones para respaldar el desarrollo de IoT durante los próximos cinco años. Estas inversiones se destinarán al desarrollo de diez parques industriales de IoT y más de 100 empresas clave en todo el país, para 2015.

En efecto, la inversión de China en infraestructura de IoT en los últimos años, mayor que la de cualquier otro país, ha superado a la competencia de Europa y Estados Unidos

Si bien China es, sin duda alguna, el protagonista más importante del mercado de IoT, toda la región de Asia-Pacífico sacará enormes ventajas de la tecnología reciente de IoT. La empresa de investigación IDC estima que el tamaño del mercado de Internet de objetos interconectados, sin incluir a Japón, crecerá de USD 250.000 millones en 2013 a USD 583.000 millones en 2020. Mientras tanto, la cantidad de cosas conectadas a Internet en el mercado de Asia-Pacífico crecerá de 259.000 millones en 2013 a 898.000 millones en 2020. Aunque IDC pronostica que para el año 2020, 1 de cada 5 objetos conectados a Internet estará en China.

América latina

A pesar de que tanto a nivel de inversión como de proyecciones América Latina está lejos de EEUU, Europa o Asia, en 2014 el aumento en gasto en iniciativas relacionadas con IoT para empresas, inteligencia de negocios y tecnología para empresas fue el segundo más alto, justo por debajo de EEUU, lo que indica que ya existe cierta conciencia sobre su importancia. Por su parte, Machina Research calculó que América Latina tendrá una tasa de crecimiento anual de 27 % durante el periodo 2014–2024 en desarrollo de IoT. Así mismo, la cantidad de conexiones a IoT pasará de 14,6 millones a 160 millones.

Machina Research señala que "los pronósticos para América Latina reflejan un universo dinámico de soluciones que utilizan un mix de diversas tecnologías de conexión incluyendo opciones fijas, celulares,

satelitales e inalámbricas de corto alcance. A pesar de las incertidumbres económicas actuales en mercados clave, nos mantenemos optimistas en la adopción a largo plazo de soluciones IoT en la región, en tanto las compañías continúan reconociendo el valor de los datos IoT en sus organizaciones". En general, los países que más destacan en desarrollo de IoT son Brasil, Argentina, México, Perú y Chile.

Por citar un ejemplo: en el caso particular de Chile, se estima que sólo en 2014 la inversión en IoT superó los 300 millones de dólares en las áreas de transporte, logística y retail. Para 2015 y 2016 esta cifra ha seguido aumentando, mientras que se han multiplicado las iniciativas para acercar el IoT a la sociedad y a las distintas áreas en donde se puede aplicar.

Desafíos

La interconexión digital de los objetos, representa una gran oportunidad que tendrá un impacto fundamental en la forma en que vivimos y trabajamos, reduciendo el desperdicio y las ineficiencias y proveyendo beneficios sociales y ambientales importantes en seguridad, cuidado de la salud, transporte y logística, educación y energía, entre muchos otros sectores de la economía.

Para alcanzar su potencial, se tendrán que superar una cantidad de desafíos significativos. Como por ejemplo la fragmentación y complejidad del mercado, falta de claridad regulatoria, protección de datos, seguridad y privacidad.

En los siguientes párrafos se describen algunos de los desafíos que se plantean para el desarrollo y adopción de sistemas de IoT a los fines de maximizar sus beneficios sociales.

Licencias y espectro

El otorgamiento de licencias y la gestión del espectro son temas de gran relevancia para asegurar la disponibilidad y capacidad de las comunicaciones de IoT. Los dispositivos de IoT se comunican utilizando un rango amplio de protocolos, basados en requerimientos de conectividad y limitaciones de recursos. Estos incluyen protocolos de radio de corto alcance como ZigBee, Bluetooth y Wi-Fi, redes de datos móviles y aplicaciones especializadas como infraestructura de datos y protocolos de radio de largo alcance como Ultra-Narrow Band.

Para comunicarse con redes remotas, los dispositivos de IoT podrán enviar datos por medio de un puerto con una conexión móvil o fija a la red telefónica o de Internet. Para los consumidores, dicho puerto será usualmente un router doméstico o un smartphone, mientras que para las empresas probablemente sea su red corporativa. Los dispositivos que se comunican a grandes distancias necesitan acceso al espectro dentro del rango 300 MHz a 3GHz, mientras que las conexiones cercanas pueden usar comunicaciones en la frecuencia de 13 MHz o bandas EHF. Algunas aplicaciones de IoT también pueden usar bandas AM/FM en el rango VHF.

Para todo ello, es necesario prestar atención continua a la disponibilidad de espectro para comunicaciones de corto alcance, y la capacidad de las redes que conectan puertos de IoT a Internet, así como estimular la puesta en marcha de la tecnología de células pequeñas como el 4G.

La FCC de Estados Unidos también está revisando el uso de espectro por arriba de los 25 GHz para redes de 5G y, posiblemente, para IoT. Por su parte, el gobierno de Corea del Sur planea asegurar frecuencias adicionales de al menos 1 GHz en 2024 y asegurar que el 5G sea comercializado a partir de 2020 en respuesta al crecimiento exponencial que se espera de tráfico de IoT.

En lo que refiere a licencias, estudios de la UE recomiendan que un modelo de exención de licencias es el más efectivo para el desarrollo de IoT, dado que evita la necesidad de negociaciones contractuales antes de que los dispositivos sean utilizados y manufacturados, permitiendo así la producción de numerosos dispositivos

a bajos costos. La mayoría de los sistemas utilizan la exención de licencias para frecuencias en las bandas Industrial, Científica y Médica, incluyendo la sub-kHz para videovigilancia y control de acceso. Por ejemplo, los Servicios de Comunicaciones de Implantes Médicos operan en la banda de 400 MHz y 900 MHz para el estándar RFID. Los estándares de Bluetooth, ZigBee y Wi-Fi operan también en espectro sin licencia.

Conmutación y roaming

Las empresas que operan grandes redes de dispositivos *machine-to-machine* vía redes de telefonía móvil, con una tarjeta SIM fija a cada dispositivo, pueden encontrar no muy sencillo el cambiar de operador al final de un contrato, o si un dispositivo itinera hacia una red local diferente por determinado período puede ser que obtenga un mejor servicio de otro operador. Esta capacidad de itinerar es importante para los dispositivos que se mueven entre países, y también para dispositivos con una localización fija que puedan ser usados en áreas con períodos de no disponibilidad de servicios.

Se han llevado a cabo tareas de estandarización técnica para permitir dichos servicios. Los primeros pasos en esa dirección fueron tomados en los Países Bajos, que en 2014 permitieron que las tarjetas SIMs fueran entregadas por entidades que no fueren operadores de redes móviles, tales como empresas de servicios públicos y de autos. Asimismo GSMA ha desarrollado estándares para la gestión de dispositivos *machine-to-machine*, que están siendo apoyados por operadores móviles tales como China Unicorn y Telefónica.

Por su lado, la Conferencia Europea de Administraciones Postales y de Telecomunicaciones, por medio de su Comité de Comunicaciones Electrónicas, ha recomendado que los SIMs cuyo IMSI puede ser actualizado remotamente deberían ser implementados lo más pronto posible, mientras que los Estados miembros consideran que hay mayor flexibilidad en la asignación de Códigos de Red Móvil para proveedores de servicios de IoT. En tal sentido, han solicitado al Sector de Normalización de la ITU que reconsidere actualizar la Recomendación E.212 para que explícitamente autorice esta flexibilidad, así como planificar el futuro uno de Códigos de Red Móvil para apoyar un mayor rango de servicios de IoT. Estos cambios están en este momento bajo consideración del Grupo de Estudio ITU-T 2.

Direcciones y numeración

Los dispositivos de IoT requieren una dirección de comunicaciones única y enrutable y una dirección asignada que permite conexión entre redes limitada; o requieren hacer uso de redes locales únicamente, para compartir datos con otros dispositivos y recibir instrucciones de un controlador cercano, como una computadora personal o un smartphone, en cuyo caso una dirección globalmente única no es requerida.

Permitir conexiones P2P entre dispositivos puede aumentar la fiabilidad de las comunicaciones, en relación a las comunicaciones necesarias con una red global grande y compleja, lo cual coincide con el caso de uso común de un descubrimiento individual y la interacción con dispositivos cercanos. Pero cuando los dispositivos deben ser globalmente accesibles -posiblemente, a través de Internet- se requiere espacio de direcciones de gran tamaño para identificar individualmente a cada uno.

El número de direcciones no asignadas para la versión actual del protocolo de Internet (IPv4) es limitado, pero la nueva versión (IPv6) que se está desplegando en todo el mundo tiene suficientes direcciones para casi cualquier número concebible de dispositivos. La transición de IPv4 a IPv6 ha tardado más de lo esperado, y son necesario programas para fomentar la transición en el mediano plazo. El gobierno de Estados Unidos, por ejemplo, llevó a cabo una puesta para mover todas las agencias federales de IPv4 a IPv6, con el único objetivo es alentar al sector privado a hacer lo mismo. Muchos otros países han puesto en marcha también Task Force IPv6 para estimular las transiciones nacionales.

Interoperabilidad

La interoperabilidad influye en el impacto económico de IoT. Entendemos que 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.

La estandarización de la interoperabilidad representa un desafío para los dispositivos de la IoT que deben relacionarse 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. Se debe lograr un compromiso entre un diseño que mantenga la compatibilidad con los sistemas que existen y la intención que existe, de lograr una mayor interoperabilidad con otros dispositivos mediante la utilización de estándares.

En términos generales, no se puede negar la importancia de la interoperabilidad, por este motivo, 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 IoT. Dentro de los organismos, mencionamos el IETF, la ITU y el IEEE, Industrial Internet Consortium, Open Interconnection Consortium, ZigBee Alliance y AllSeen Alliance, entre muchas otras.

Seguridad

Sin seguridad adecuada, hay quienes pueden acceder a información personal potencialmente sensible acerca de los usuarios, y hacer uso de las vulnerabilidades de dispositivos para atacar redes y dispositivos locales. Esto es de particular relevancia cuando los dispositivos se utilizan en espacios privados, como los hogares de los individuos, por ejemplo, los monitores de bebés. Los operadores de sistemas de IoT, y otros con acceso autorizado a los datos producidos, están también en condiciones de "recopilar, analizar y actuar sobre grandes cantidades de datos dentro de los espacios privados tradicionales”

Otra cuestión común de seguridad es el uso de contraseñas por defecto en los dispositivos, esto es, el

hecho de que los usuarios no están obligados a cambiar la configuración del dispositivo. Una página web anunció haber encontrado 73.000 webcams accesibles a través de Internet utilizando una contraseña por defecto y conocida. En este sentido, dispositivos IoT pueden ser más difíciles de asegurar que las computadoras personales. A menudo los dispositivos IoT son de bajo costo, lo que pone una fuerte presión sobre los costos de seguridad y hardware adicional o software para hacer frente a amenazas. En combinación con la conectividad a Internet limitada de algunos dispositivos, esto puede hacer que sea más difícil de desarrollar y aplicar los parches de seguridad cuando regularmente se descubren vulnerabilidades. La mayoría de los dispositivos IoT contienen equipos polivalentes y pueden ser reprogramados más allá del propósito previsto. Los dispositivos IoT con frecuencia comparten sistemas operativos, chips integrados y drivers, lo que significa que una sola vulnerabilidad puede ser utilizada para atacar una amplia variedad de dispositivos.

Las empresas que desarrollan y operan sistemas IoT necesitarán llevar a cabo pruebas de seguridad y considerar cómo las vulnerabilidades de seguridad descubiertas después de que los dispositivos son vendidos pueden solucionarse durante la probable vida útil del dispositivo. En caso de que las fallas de seguridad causen daño al consumidor, las agencias de protección del consumidor pueden ser capaces de tomar medidas para requerir remediar estos daños y mejorar los procesos de seguridad para reducir el riesgo en la ocurrencia nuevamente del hecho.

Las reglas de UE requieren que las organizaciones que traten datos personales en los sistemas IoT lleven a cabo evaluaciones de seguridad como así también hacer uso de las certificaciones de seguridad pertinentes y standards. Además, las compañías necesitan garantizarlo cuando utilicen proveedores de servicios externos para gestionar los dispositivos y los datos de IoT, en este sentido, aquellos proveedores también deben tomar razonables precauciones de seguridad.

Para hacer frente a estos retos de seguridad y privacidad, los reguladores han sugerido que las empresas desarrolladoras de dispositivos IoT deberían cumplir con la seguridad y privacidad desde el diseño “by design”, y así generar construir la seguridad y funcionalidad de privacidad en el dispositivo desde el principio del proceso de desarrollo, cuando es mucho más probable que sea efectivo.

Una cantidad significativa de trabajo ya se ha hecho en materia de seguridad y de privacidad por los políticos y los reguladores de la UE y EE.UU. Bajo el Reglamento General de Protección de Datos discutido en el Parlamento Europeo y el Consejo de Ministros, habrá fuertes incentivos regulatorios para las empresas desarrolladoras de sistemas que procesan datos personales para la protección de la seguridad y privacidad desde el diseño.

La Comisión Federal de Comercio de los Estados Unidos (FTC) también sugiere a compañías que sigan el enfoque de "defensa en profundidad" (*defence in depth*), considerando las medidas de seguridad en varios puntos distintos de sus sistemas, tales como el uso de medidas de control de acceso y la encriptación de los datos incluso cuando los usuarios están haciendo uso de enlaces cifrados en el Wi-fi router del hogar (lo cual no protegerá los datos entre el router y servidores de la compañía o si el router está mal configurado).

Privacidad

La privacidad es un tema regulatorio particularmente fuerte en los países europeos, en los que se incluye un amplio marco legal que incluye la Convención Europea sobre los Derechos Humanos del Consejo de Europa y el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos personales y la Carta de los Derechos Fundamentales de la UE. Este Marco ha sido influyente en el desarrollo de las leyes de privacidad en más de 100 países de todo el mundo.

El alto volumen de flujos de datos personales podría presentar desafíos para la regulación tradicional de protección de datos - por ejemplo, desde que los individuos no serán conscientes necesariamente cuando se comparten datos o capaces de revisar esa información antes de ser enviada a otras partes, creando un riesgo de auto-exposición y falta de control.

Otra cuestión en privacidad es la cantidad de información personal que se puede derivar de los sensores, especialmente cuando se combina con perfiles de usuario y datos de otras fuentes. Los reguladores de privacidad de Europa señalan que el desarrollo pleno de IoT puede provocar una tensión en las posibilidades actuales del uso anónimo de los servicios y en general, limitar la posibilidad de pasar desapercibido.

Investigadores han encontrado que los datos obtenidos por los sensores de teléfonos inteligentes pueden utilizarse para inferir información acerca de los usuarios, tal como, tipos de personalidad, la demografía y factores de salud (estados de ánimo, los niveles de estrés, tabaquismo, niveles de ejercicio y actividad física) e incluso la aparición de enfermedades como la enfermedad de Parkinson y desorden bipolar. Este tipo de información tiene aplicaciones obvias, tales como, en cuanto al seguro de salud respecto a la fijación de precios como así también para otras decisiones relacionadas con el empleo, el crédito y la vivienda.

Para la protección de la privacidad individual, la Comisión Federal de Comercio de los Estados Unidos (FTC) ha sugerido el requerimiento de la notificación y consentimiento cuando datos personales son recolectados por aplicaciones IoT por fuera de la expectativa razonable de los consumidores, basado en el contexto de las transacciones y las empresas.

Del mismo modo, las autoridades de protección de datos de la Unión Europea han señalado que los datos recogidos por medio de dispositivos IoT para una determinada finalidad pueden ser analizados y combinados con otros datos, lo que lleva a una serie de efectos secundarios que debería ser compatible con el propósito original de la recolección y conocimiento para el usuario.

La recolección y análisis de datos por dispositivos IoT podría afectar la privacidad cuando se incluyen datos de los espacios privados como casas y automóviles, e incluso hacer que sea difícil para las personas manejarse en su vida diaria en forma anónima.

Cuando las aplicaciones de IoT procesan información personal que a la fecha puede revelar datos "sensibles" con arreglo a la ley de protección de datos - origen étnico racial, las opiniones políticas, creencias religiosas o filosóficas, la pertenencia a sindicatos, salud o la vida sexual - se requiere el consentimiento explícito del individuo.

Bajo la ley de la Unión Europea, los individuos deben ser capaces, en cualquier momento, de retirar su consentimiento a la totalidad o parte de los datos procesados, sin "ningún impedimento o restricción técnico u organizativo", utilizando herramientas que sean "accesibles, visibles y eficaces."

La Comisión Federal de Comercio de EEUU (FTC) prevé una mayor flexibilidad para los servicios IoT en la recolección de datos no requeridos inicialmente para proporcionar el servicio, mientras que bajo la normativa europea más estricta, las autoridades de protección de datos de la UE "no pueden compartir este análisis".

Tratamiento de datos

La captura masiva de información personal en tiempos de IoT tendrá diferencias a lo que actualmente se realiza. En este sentido, se puede mencionar: se capturará información en muchos lugares más; el acopio será invisible; los datos serán más íntimos –qué, dónde, cuándo, cómo, con quién, por cuánto tiempo, por qué– y por último, las facilidades de interconexión conllevarán a que nuestros datos sean compartidos en niveles nunca antes vistos. Asociada a la invasión de la privacidad –entendiéndose en un sentido que va más allá de la protección de un espacio íntimo–

Una de las cuestiones vinculadas con el tratamiento de datos resulta la acumulación masiva de información, lo que es más conocido como B*ig Data.* El complemento entre el Big Data y el internet de las cosas es ideal: "si tuviéramos computadores que supieran todo lo que hay que saber acerca de las cosas –usando datos que ellos mismos hayan recogido sin intervención humana– podríamos monitorear e inventariar todo y reducir significativamente las pérdidas, desperdicios y costos".[1]

A su vez, se ha indicado que a través del Big Data las empresas cuentan con una base racional que les permite identificar individuos para categorizarlos en grupos con otros similares.[2] Así, pueden hacer ofertas diferenciadas, productos para nichos específicos o seguimientos a compras previas. Los efectos benéficos no se quedarán solo en las empresas. Esta herramienta permitirá observar mejores correlaciones entre hábitos de consumo y efectos ambientales, lo que puede incentivar un consumo más consciente.[3]

Sin perjuicio de diferenciar *Big Data* de IoT, tales conceptos resultan complementarios al punto que potencian tanto las oportunidades que presentan a efectos de prevenir y planificar en base a datos certeros como así también mayores riesgos en cuanto a cuestiones vinculadas a privacidad y tratamiento de datos.

[1] Ashton, K. `The Internet of Things 'Thing'. En RFID Journal, junio de 2009. Disponible en: http://www.rfidjournal.com/articles/view?4986 (consultado el 30 de noviembre de 2014) Citado por Cortes, Carlos. Ob. citado. Págs. 15 y 16.
[2] Cfr. Barocas, S.; Selbst, A. 'Big Data's Disparate Impact'. SSRN 2477899, 2014. Disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899 (consultado el 30 de noviembre de 2014). Citado por Cortés, Carlos. Ob. citado.Pág. 16.
[3] Anderson, J , Rainie, L. `The Future of Big Data' en Pew Research Center's Internet & American Life Project, julio de 2012. Disponible en: http://www.pewinternet.org/2012/07/20/the-future-of-big-data/ (consultado el 30 de noviembre de 2014). Cortés, Carlos. Ob. citado. Pág. 16.

Economías emergentes y en desarrollo

Entendemos que IoT, presenta innumerables oportunidades, 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.

Si consideramos el potencial de IoT, podemos ejemplificar con beneficios para control de agua, mejoras en la calidad de vida, con la aplicación de redes de sensores, control de desastres naturales, cambio climático, salud, monitoreo de los recursos naturales. Existirían una gran cantidad de datos de los distintos tipos de aplicación de IoT, que podrían llegar a ser utilizados en diversos casos. Para nuevos estudios, análisis, precedentes, investigar, y brindar información y conocimiento a distintos institutos, universidades, centros académicos que se dediquen a investigar.

Conocemos que la población mundial, continua aumentando de manera exponencial, y surgen nuevos desafíos relacionados con el acceso a alimentos de calidad, seguros y asequibles aumentarán con el tiempo. Es una herramienta fundamental para afrontar estas situaciones promoviendo a través del uso de IoT, una agricultura sostenible.

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 cada economía.

Modelo de negocios de IoT

Actualmente el IoT se está acelerando a medida que los costos disminuyen y las aplicaciones innovadoras emergen. A partir de 2020, el despliegue comercial de las redes de la tecnología 5G proporcionarán capacidades adicionales que serán indispensables para el IoT, tales como las segmentaciones de redes y la capacidad de conectar de manera exponencial más dispositivos de lo que es posible en la actualidad". Se prevé que 16 mil millones (de los 28 mil millones) de dispositivos conectados se unan a Internet de las Cosas para finales de 2021.

La cadena de valor es probablemente la parte más importante del modelo de negocio, dado que define cómo el servicio es proporcionado. IoT tiene una cadena de valor muy compleja debido a que impacta en un gran número de procesos. Esto implica una gran oportunidad para múltiples partes interesadas que necesitan trabajar en conjunto para proveer servicios sobre la base de IoT.

Claramente la formación de alianzas no es fácil cuando cada entidad se considera a sí misma más importante que las demás. En tal escenario, la cuestión más importante para cualquier empresa interesada en IoT es encontrar una posición en la cadena de valor. La posición en la cadena de valor definirá su relevancia, estrategia y oportunidades.

Módulos Inteligentes	Objetos Inteligentes	Conectividad	Plataformas	Customización de Software	Aplicaciones	Clientes
Tarjetas SIM Sensores Chips embebidos Agregadores	Expendedoras Autos Cámaras Termostatos	Redes Conectividad Disponibilidad Calidad	Capacidades de IoT Cobranzas Integración con otras aplicaciones Analítica	Interfases Hardware Manejo de Datos	Soluciones verticales CRM y Cobranzas Customer care	Compra servicios Vende servicios

Otra clasificación agrupa a los actores en cinco grupos claves, cada uno tiene fortalezas únicas que aportar a IoT, pero no todos con la misma fuerza ni en pie de igualdad:

- **Proveedores de dispositivos:** sin un modelo de servicios, se beneficiarán de la moda generada alrededor de IoT pero se mantendrán como un simple vendedor de aparatos. Su mejor apuesta es ingresar a alianzas no exclusivas con jugadores líderes de otras partes de la cadena de valor.
- **Operadores:** los operadores son crítico dado que proveen conectividad y han tenido un buen comienzo en IoT. Es natural para este grupo considerarse como líderes en la cadena de valor. Sin embargo, los operadores de red pueden conectar con la mayoría de los dispositivos, ganando no sólo valor en la red sino también estando mejor posicionados para capturar valor. En consecuencia, el riesgo de los operadores es el de convertirse en la simple tubería hacia la computación en la nube.
- **Proveedores de plataformas:** Las plataformas son el corazón de IoT y son los que unen el hardware, la

conectividad, a los operadores y a las aplicaciones verticales, para proveer soluciones específicas de IoT en la industria. La mayoría de los jugadores con intenciones fuertes dentro del mercado de IoT buscan convertirse en proveedores de plataformas de IoT, pero el éxito depende de su habilidad para forjar alianzas hacia un mismo fin. Hay distintos tipos de plataformas:

- de conectividad o *machine-to-machine*, principalmente enfocadas en conectar dispositivos vía redes de telecomunicaciones y/o tarjetas SIM, sin demasiado foco en *analytics* o procesamiento de datos;
- plataformas de hardware específico, que suelen ser las plataformas propietarias, diseñadas exclusivamente para ciertos dispositivos;
- plataformas puras de IoT, que han sido específicamente desarrolladas por IoT para mantener la escala, estándares y requerimientos en mente.

No todos los tipos de plataformas tendrán la habilidad de liderar el esfuerzo de IoT. Algunos afirman que la combinación ganadora será una plataforma que ofrezca gestión de dispositivos, almacenamiento en la nube, *analytics*, visualización de datos y la posibilidad de integrarse con sistemas de terceros vía API o SDK para poder tomar ventaja de la gran variedad de software y hardware de IoT.

- **Integradores de Sistema:** Tienen un rol muy importante en las IoT industriales. Los integradores de sistemas hacen que los componentes individuales de IoT trabajen juntos de la manera más óptima para el cliente. La mejor opción para los integradores de sistemas es identificar su nicho de mercado y asociarse con grandes jugadores proveedores de plataformas.
- **Proveedores de Aplicaciones:** Son un jugador muy pequeño en general, y hay muy pocos grandes proveedores de aplicaciones específicos de IoT que puedan operar independientemente.

A continuación, los posibles modelos de negocios que pueden adoptar las empresas de tecnología, para maximizar los flujos de ganancias, detallando de qué fuente proviene el retorno de inversión:

Modelo de Negocios	Centrado en Dispositivos	Venta de datos	Dispositivos y/o suscripción	Centrado en el volumen	Ganancias colaborativas
Descripción	El foco del negocio es la venta de dispositivos El servicio provisto posteriormente es gratuito o mínimo En ocasiones los usuarios pagan una tarifa por una única vez para obtener características o servicios más complejos	Se comercializan los *insights* generados por el uso de plataformas de *analytics* Los datos cedidos son anónimos y agregados Los *data-sets* cedidos suelen ser relativos a un segmento específico de usuarios a los fines de ser utilizados para estrategias de marketing	Pago por adelantado por el hardware Suscripción mensual para acceder a contenidos, o en relación al uso o un software que es provisto como servicio Suele ser popular en las empresas que cuentan con una flota de vehículos	Apalancamiento de IoT para adquirir nuevos clientes Busca maximizar el número de unidades vendidas o aumentar la base de clientes Apunta al mercado masivo para aumentar la cuota de mercado y aprovechar las economías de escala	Uno de los mayores conductores en la presentación de nuevos modelos de negocios Ligado a la idea de "economía colaborativa" que crea y trae más salarios a gente que participa del negocio pero desde afuera de la industria Contribuye más eficientemente a bajar la estructura de costos en relación al modelo tradicional

Proyecciones estimadas de los efectos de la implementación de IoT

Un pronóstico de Business Insider establece algunas claves sobre las tendencias que se vienen en base a la implementación de IoT. En este sentido, surgen los siguientes ítems:

- Habrá 34 mil millones de dispositivos estarán conectados a internet para el 2020;
- Cerca de 6 trillones serán gastados en soluciones IoT en los próximos 5 años.
- Las empresas serán quienes más adoptarán las soluciones IoT. Ellos ven tres formas en que IoT puede mejorar resultados mediante:
    - la reducción de los costos de operación;
    - el aumento de la productividad; y
    - la expansión a nuevos mercados o el desarrollo de nuevas ofertas de productos;
- Los Gobiernos están enfocados en incrementar la productividad, reducir costos y mejorar la calidad de vida de los ciudadanos, por lo que se estima que serán los segundos en adoptar el ecosistema IoT;
- Los consumidores son los terceros en adoptar IoT. Aún así, ellos compraran dispositivos en números masivos e invertirán cantidades significativas de dinero en el ecosistema IoT.[4]

Conclusiones

Internet de las cosas promete abrir la puerta a un mundo revolucionario, más "inteligente", totalmente interconectado, en el cual las relaciones entre los objetos, las personas y su entorno se entrelazan cada vez más.

Esta omnipresencia de dispositivos conectados está dando lugar una nueva era para todo el mundo, transformando modelos económicos, procesos productivos, industrias y revolucionando aspectos de la vida diaria de cada individuo. Pero existen una serie de temáticas, que deben ser consideradas por los distintos actores involucrados, principalmente las mencionadas a lo largo del documento, seguridad, privacidad, interoperabilidad y estándares y las economías emergentes.

Por lo tanto Internet de las cosas implica un complejo conjunto de consideraciones tecnológicas, sociales y políticas en constante evolución y que atraviesa un periodo de constante evaluación, estudio y debate. 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.

Para definir las formas más eficaces de avanzar, se necesitará la participación informada, el diálogo y la colaboración de una variedad de partes interesadas por este motivo, desde la Secretaría de Regulación de Tecnologías de la Información y las Comunicaciones del Ministerio de Modernización analizamos las nuevas tendencias en las TIC y sus implicancias, con el objetivo último de fomentar el desarrollo de Internet de las cosas siempre y cuando estas contribuyan a mejorar la situación para nuestro país, los ciudadanos y el entorno.

[4] Greenough, John. "*How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond."* Consultado el 26.08.26 en: http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10