



Internet de las Cosas: Evolución o Revolución?

Parte 1 de una serie

Forewords by:

Shawn DuBravac, Ph.D.

Economista principal, Consumer Technology Association (CEA); autor del libro de gran venta de New York Times, "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate"

Carlo Ratti, Ph.D.

profesor del MIT SENSEable City Lab y diseñador de la Future Food District en la 2015 Milan Expo



Consumer
Technology
Association™



Reconocimientos

El siguiente artículo ha sido posible gracias a la colaboración de la Consumer Technology Association y su economista principal, Shawn DuBravac.

También queremos agradecer a las siguientes personas de AIG por sus valiosos aportes para este informe:

Lex Baugh
Nicolas Berg
Julien Combeau
David Bassi
Erik Nikodem
Garin Pace
Joe Trotti
and
Jason Kelly



Tabla de Contenidos

FOREWORDS	2
RESUMEN EJECUTIVO	4
¿QUÉ ES LA “INTERNET DE OBJETOS INTERCONECTADOS”?	6
UNA NUEVA ERA ECONÓMICA	9
RIESGOS DE LA IOT	15
LA SITUACIÓN DE LA IOT EN EUROPA, EE. UU. Y ASIA	19
CONCLUSIÓN	21
CITATIONS	22

Forewords

Dr. Shawn DuBravac

es economista principal de *Consumer Technology Association* y autor del libro de gran venta de *New York Times* "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate."

Podemos decir sin temor a equivocarnos que somos el comienzo de otra revolución industrial. El aumento de las máquinas y los objetos conectados conocidos como la "Internet de las cosas" (IoT, por sus siglas en inglés) competirá con maravillas tecnológicas del pasado, como la imprenta, el motor a vapor y la electricidad. Desde el mundo desarrollado hasta el mundo en vías de desarrollo, cada rincón del planeta experimentará un resurgimiento económico profundo. Aún más notable es la velocidad con la que este cambio sucederá. Una década atrás, había cerca de 500 millones de dispositivos conectados a Internet. Hoy, hay de 10 a 20 mil millones. En cinco años, podría haber de 40 a 50 mil millones.

A diferencia de las revoluciones industriales anteriores, sin embargo, a esta la vemos venir. La IoT no es un solo invento trascendental, como la desmotadora de algodón. Las industrias no serán atrapadas por sorpresa por una mejor trampa para ratones que convierta en obsoletos sus sistemas de fabricación y sus productos. De hecho, cada industria y empresa individual se posiciona con el fin de ganar y prosperar a través de la incorporación de objetos IoT en el modelo de su empresa y, como consecuencia, descubrir nuevas y mejores formas de hacer negocios. Lo que no quiere decir que no habrá trastornos y grandes riesgos. A medida que se engendren las nuevas industrias y desaparezcan los viejos modelos, las empresas enfrentarán un entorno económico y de riesgos totalmente nuevo. Pero el fenómeno de la IoT es único porque permite a las empresas visionarias prepararse, adaptarse y minimizar el riesgo en esta nueva era económica.

El aumento de la IoT también significa que estamos en el comienzo de una nueva era de datos. Dos componentes principales de un "objeto IoT" son su capacidad de capturar datos a través de sensores y su capacidad de transmitir datos vía Internet. Como este informe técnico deja en claro, la reducción en el precio de los sensores desde el comienzo del nuevo milenio ha sido un impulsor principal del aumento de la IoT. En síntesis, los sensores son extremadamente baratos hoy. Esto nos ha permitido capturar enormes cantidades de datos que antes estaban fuera de nuestro alcance.

Según la organización de investigación noruega SINTEF, el 90 por ciento de los datos del mundo han sido generados durante los últimos dos años. Cada segundo, se crean más de 205.000 gigabytes nuevos, lo que equivale a 150 millones de libros. Esta es la cantidad de datos creados en un mundo con 10 a 20 mil millones de objetos conectados y con sensores. El mundo está produciendo más datos que nunca antes y, de manera crucial, los mantenemos activos y los utilizamos, con una frecuencia cada vez mayor. Imaginen un mundo con 40 a 50 mil millones de objetos IoT.

La calidad con la que una industria o empresa individual utilice el flujo masivo de datos desplegados por objetos IoT determinará en gran medida su ventaja competitiva y su éxito futuro. De algún modo, cada organización tendrá que centrar sus aproximaciones y perspectivas en los datos. Serán los datos los que informen a un gerente de una cadena de suministros acerca de las ineficiencias o agujeros de seguridad en la cadena de suministros; serán los datos los que digan a un comerciante si los consumidores están respondiendo a la última campaña; y serán los datos los que den a las empresas un mayor conocimiento de sus procesos y productos que nunca antes.

La industria de seguros está en el centro de esta nueva revolución industrial y de datos. De hecho, las aseguradoras multinacionales han estado utilizando enormes cantidades de datos para comprender y mitigar el riesgo por décadas. A medida que los objetos IoT impregnen todos los niveles de la economía global, serán las aseguradoras las que estén mejor posicionadas para analizar estos datos y extraer conocimientos significativos y factibles: conocimientos que podrían hacer de nuestro mundo un lugar más seguro y productivo del que alguna vez podríamos haber imaginado.

Dr. Carlo Ratti

profesor del MIT SENSEable City Lab y diseñador de la Future Food District en la Milan Expo: IoT and the Future of Food.

Durante décadas hemos sido deslumbrados por nuevas y mejores novedades tecnológicas. Mejores computadoras; mejores reproductores de música; mejores televisores y mejores teléfonos. Esta tendencia ha hecho que la tecnología se asemeje a un largo tren de artilugios milagrosos que no tenían antecedentes en nuestras vidas. Se podría esperar que esto continúe, que la próxima tecnología revolucionaria venga en un nuevo contenedor plástico o metálico. Sin embargo, podría no ser así.

De hecho, hay otra revolución tecnológica emergente, pero es, por lejos, más simple y a la vez potencialmente más innovadora que cualquier dispositivo. Es una revolución impulsada por datos que podría acabar con muchas ineficiencias, confusiones, peligros y prácticas inseguras de la vida moderna. La industria de seguros global promete tener un rol vital en el centro de esta revolución tecnológica.

Llámenla la "Internet de objetos interconectados" o "Internet de las cosas"; la transformación se ocupa del continuo pero inexorable aumento de objetos conectados y con sensores: en síntesis, la digitalización en línea de nuestro mundo físico. Los objetos autónomos pueden adquirir, analizar y transmitir cantidades de datos que capturan de sus entornos constantemente. A su vez, las economías, las ciudades, los negocios y las personas responderán a este flujo de información, lo que abrirá un abanico de oportunidades sin precedente.

La Internet de objetos interconectados está dando lugar a redes digitales omnipresentes dentro del espacio físico: el alma en red de la "ciudad inteligente". No solo una red de servicios municipales, como la electricidad y el agua; las ciudades verdaderamente "inteligentes" combinan elementos de todos los accionistas urbanos, incluidos los ciudadanos, gobiernos y empresas. Y, una vez más, un amplio espectro de modelos de implementación está emergiendo en diferentes partes del mundo.

En los Estados Unidos, la idea general del espacio urbano inteligente ha sido primordial para la generación actual de nuevas empresas exitosas. El diseño en sí mismo tiene un impacto positivo sobre la revolución de la mayoría de los aspectos de la vida urbana, desde el traslado al trabajo hasta el consumo de energía y la salud personal. Estas nuevas iniciativas reciben un apoyo entusiasta de parte de fondos de capital de riesgo.

En América del Sur, Asia y Europa, todos los niveles gubernamentales identifican los beneficios potenciales de construir ciudades "inteligentes" y trabajan para liberar inversiones significativas en esa área. Río de Janeiro desarrolla la capacidad en su centro "Operaciones Inteligentes"; Singapur está por embarcarse en un esfuerzo ambicioso por una "Nación Inteligente"; el programa Horizonte 2020 de la Unión Europea ha destinado €15 mil millones en los años 2014-2016 un compromiso de recursos significativo para la idea de las ciudades inteligentes, especialmente en un momento de limitaciones fiscales.

El futuro mostrará cómo los diferentes modelos descritos arriba se desarrollarán. Por el momento, no hay duda de que la industria de seguros global tiene el potencial de jugar un rol primordial. ¿Cómo evaluaremos los riesgos asociados al territorio en gran medida inexplorado de la Internet de objetos interconectados? ¿Cómo podemos entender los desafíos que podrían provocar cambios fundamentales en la responsabilidad y la gestión de riesgos que ya conocemos hoy? Allí es donde las aseguradoras pueden liderar; no solo por el bien de sus empresas, sino para guiar a otras industrias, gobiernos y, sobre todo, a los ciudadanos.

Resumen ejecutivo

Según los analistas de la industria, hay entre 10.000 y 20.000 millones de cosas conectadas a Internet en la actualidad. Este ecosistema de objetos conectados constituye la base de la "Internet de objetos interconectados" (también llamada Internet de las cosas, Internet of Things, IoT). Aunque la tecnología que comprende la IoT existe desde hace años, solo se encuentra en sus primeras etapas. En la actualidad, la cantidad de objetos conectados parece insignificante si se la compara con la cantidad de objetos que estarán conectados dentro de apenas cinco años. Los cálculos varían pero, para 2020, el espectro de objetos conectados será de entre 40.000 y 50.000 millones e incluirá de todo, desde tazas y bolígrafos hasta viviendas, automóviles y equipos industriales.

IoT ofrece oportunidades nuevas sorprendentes para las empresas, entre ellas muchas que solo perciben los expertos. Los medios optan por centrar su atención en el ámbito del consumidor de IoT, como el mercado de objetos portátiles. Sin duda, estos productos ocupan un lugar prominente en el universo de la IoT, pero no dejan de ser un nicho. Las empresas sin una presencia en el mercado de artículos de consumo creen erróneamente que la IoT no tiene nada para ofrecer. Sin embargo, las repercusiones que tendrá la IoT en todos los niveles de las operaciones comerciales, independientemente de la industria de que se trate, oscilarán entre lo mundano y lo profundo. Los problemas que han asediado a las empresas durante siglos disminuirán drásticamente y, en muchos casos, desaparecerán completamente. En comparación con otros desarrollos tecnológicos, como la informática en la nube, las redes inteligentes, la nanotecnología y la robótica, el mundo de la IoT en el que estamos por ingresar representa un paso gigante hacia una economía de mayor eficiencia, productividad y seguridad, y mayores ganancias.

Según un estudio realizado por RAND Europe, para el año 2020 las estimaciones más altas del potencial económico mundial anual de la IoT en todos los sectores afectados van de USD 1,4 billones (alrededor de € 1,09 billones) a USD 14,4 billones (unos € 11,2 billones), lo que equivale aproximadamente al PIB actual de la Unión Europea. En efecto, para entonces la IoT no será un segmento aislado de la TI sino más bien la fuerza que impulsa una parte considerable de la actividad económica mundial. Dentro de cinco años, pocas serán las industrias que no se vean modificadas por la IoT. Ya en la actualidad, son contadas las industrias que no tienen nada que ganar del uso de los objetos de IoT en sus procesos o productos. No obstante, hay varias industrias pioneras en las que la IoT se ha convertido en un elemento indispensable para las operaciones. Como veremos, estas industrias ayudan a percibir con mayor claridad la promesa de la IoT en los años venideros.

Sin embargo, toda oportunidad implica cierto nivel de riesgo y, en lo que respecta a la IoT, los riesgos son tan importantes como las recompensas. De las transgresiones en Internet a los planteos cambiantes de responsabilidad de productos y propiedad, las empresas no pueden permitirse entrar sin preparación a este nuevo mundo tecnológico. Por ejemplo, cada objeto que se conecta con Internet es un punto de ingreso más a través del cual los ciberdelincuentes pueden ingresar al sistema empresarial de los negocios. Igualmente peligroso es el hecho de que, en un mundo donde las máquinas reemplazan a los humanos como encargados de tomar decisiones y donde los sensores capturan datos de manera continua, surjan interrogantes serios en materia de responsabilidad, daños físicos resultantes y privacidad.

El objetivo de esta serie de artículos técnicos es informar a los lectores sobre las oportunidades y los riesgos potenciales de la IoT. Aunque no podamos afirmar a ciencia cierta qué les espera a las empresas en cinco años, podemos predecir los problemas que cobrarán especial importancia. Un mundo de IoT es un mundo de complejidad económica en aumento, y el marco que las industrias y los gobiernos han adoptado para fomentar el crecimiento y la competencia no será adecuado en el largo plazo. El impacto de la IoT se hará sentir en todos los países y las economías del planeta, incluso en el mundo en desarrollo, al que históricamente se le han negado los beneficios del progreso tecnológico. Como argumenta Shawn DuBravac, economista principal de Consumer Technology Association, con sede en Washington, D.C., en su libro de gran éxito editorial, "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate":

Esto no es lo que podría suceder si eligiéramos este camino y no otro. Esto es lo que sucederá, sea cual fuere el camino que tomemos.

Para que las empresas adquieran plena conciencia del enorme potencial de la IoT, deberán estar preparadas para los riesgos que les esperan. La industria de seguros está particularmente bien posicionada para ayudar a las empresas a manejarse en este nuevo mundo tecnológico. En efecto, muchos de los elementos que han convergido en la IoT han sido utilizados desde hace tiempo por las aseguradoras para entender mejor los riesgos y mejorar la seguridad. Y, de la misma forma en que la industria de seguros ayuda a las empresas a adaptarse, se adaptará ella misma para mejorar sus procesos y funciones fundamentales.



¿Qué es la “Internet de objetos interconectados”?

La expresión “Internet de objetos interconectados” (Internet of Things) no es nueva. Fue acuñada a principios de 1999 por Kevin Ashton, pionero en tecnología, quien en ese entonces se desempeñaba como gerente auxiliar de marcas en Procter & Gamble. En 2007, Ashton amplió el concepto de su frase en un artículo:

“Si tuviéramos equipos que supieran todo lo que habría que saber sobre las cosas, mediante datos recopilados sin nuestra ayuda, podríamos rastrear y contar cada objeto y reducir drásticamente el derroche, las pérdidas y los costos. Sabríamos cuándo las cosas deben ser reemplazadas, reparadas o retiradas del mercado, y si son nuevas o anticuadas.

“Debemos empoderar a los equipos con sus propios medios de recopilación de información, de modo que puedan ver, oír y oler el mundo por ellos mismos, en todo su fortuito esplendor. La tecnología de identificación por radiofrecuencia (RFID, Radio Frequency Identification) y de sensores permite a los equipos observar, identificar y entender el mundo sin las limitaciones que imponen los datos incorporados por el hombre .”

Posteriormente, en 2012, Rand Europe intentó ampliar la definición de “Internet de objetos interconectados” en un informe de investigación preparado para la Comisión Europea. El informe decía lo siguiente:

“La Internet de objetos interconectados se construye a partir de la Internet actual al crear una red generalizada y organizada de forma autónoma, con objetos físicos conectados, identificables y direccionables que permiten el desarrollo de aplicaciones en los sectores verticales clave mediante chips, sensores y activadores incorporados, y miniaturización de bajo costo”.

Both Ashton’s and RAND’s definitions are true. Yet RAND’s version takes Ashton’s original Tanto la definición de Ashton como la de RAND son válidas. Sin embargo, la versión de RAND incluye el concepto original de Ashton, a saber, “equipos empoderados” y lo amplía para que incluya “objetos físicos”. En otras palabras, la “Internet de objetos interconectados” no depende principalmente de los equipos para existir. Más bien, cada objeto, incluso el cuerpo humano, podría incorporarse a la IoT si estuviera equipado con ciertos elementos electrónicos. Por cierto, estas piezas varían según la función que deba cumplir el objeto, pero se encuentran dentro de una de las dos categorías amplias siguientes: 1). el objeto debe poder recopilar datos, generalmente a través de sensores; y 2). el objeto debe poder transmitir esos datos a otros lugares a través de Internet. Por consiguiente, un sensor y una conexión son los dos “elementos” electrónicos principales de los objetos de IoT.

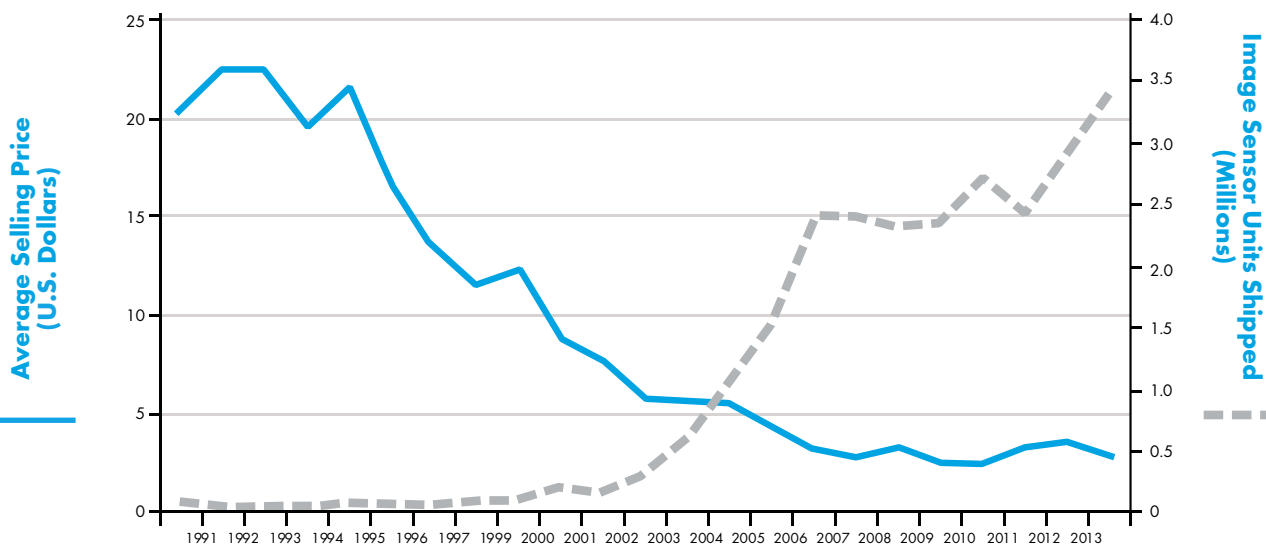


Si bien esta tecnología existe desde hace más de una década, en los últimos veinte años dos desarrollos han sido los impulsores principales del surgimiento de la IoT como fenómeno modificador del paradigma. El primero es el crecimiento meteórico de los dispositivos y las aplicaciones móviles, y la disponibilidad generalizada de la conectividad inalámbrica.

Un informe de Cisco publicado en 2011 destacó que, en 2003, había alrededor de 500 millones de dispositivos conectados a Internet, casi todos equipos personales. Al dividir la cantidad de dispositivos conectados por la población mundial, en ese entonces 6.300 millones, había menos de un

dispositivo (0,08) por persona en el planeta . Para 2010, el mercado de teléfonos inteligentes y tablet PC había detonado, con un aumento de la cantidad de dispositivos conectados a 12.500 millones, aun cuando la población mundial aumentó a solo 6.800 millones. En solo siete años, la cantidad de dispositivos conectados por persona en el mundo había aumentado en un 2.250 por ciento, de 0,08 a 1,8. En Europa, donde se registra una de las mayores difusiones de teléfonos móviles del mundo, hay 1.100 millones de suscripciones de móviles para una población de unos 800 millones de personas . Esto equivale a alrededor de 1,3 suscripciones de móviles por persona o, expresado en términos más simples, en Europa hay más suscripciones de móviles que personas.

El otro desarrollo se remonta aún más lejos en el pasado que la tecnología móvil: nos referimos a los sensores. Sin embargo, el alto costo de los sensores durante casi todo el siglo XX limitó su uso en todo, excepto en los productos de primera línea. A principios de la década de 1990, los sensores de imágenes en el estado sólido costaban entre USD 20 y USD 25. A fines de esa década, se vendían a USD 5. Lo que siguió fue un enorme aumento en el mercado de las cámaras digitales. En efecto, otros sensores, como los incorporados a los teléfonos inteligentes comunes, han seguido una trayectoria similar en cuando a potencia y costo. En 2007, por ejemplo, los acelerómetros que miden un solo eje de movimiento costaban alrededor de USD 7. Los acelerómetros actuales, que miden seis ejes de movimiento, cuestan menos de USD 0,50.



Source: DuBravac, Shawn. "Digital Destiny." P. 78

Claro que los teléfonos inteligentes actuales distarían de ser “inteligentes” si no fuera por la variedad de sensores incorporados a cada dispositivo. Los teléfonos inteligentes de la actualidad están equipados con cinco a nueve sensores, según el modelo. Estos incluyen:



Hace quince años, la inclusión de uno (ni hablar de nueve) de estos sensores hubiera aumentado el costo de un producto más allá de los medios del consumidor promedio. Actualmente, el costo de todos estos sensores asciende a menos de USD 5,00, y los sensores más económicos cuestan apenas USD 0,07%.

Sin embargo, los sensores no se limitan a habilitar funciones claramente definidas en nuestros teléfonos móviles. De hecho, son un elemento crítico que “enciende” la IoT. Al recopilar datos del entorno circundante de forma continua, los sensores reemplazan al ser humano como principal origen de los datos recibidos por los equipos. Y, dado que los sensores pueden recopilar datos a velocidades y en cantidades que ningún ser humano podría igualar, han generado el fenómeno conocido como datos masivos (Big Data), o sea, la adquisición y el análisis de conjuntos de datos extremadamente grandes.

¿Qué son estos datos? Son todo lo que nos rodea. En términos más prácticos, los datos que los sensores actuales pueden, y que los seres humanos no pueden adquirir, están revolucionando los procesos económicos y comerciales. De hecho, los fabricantes de automóviles de todo el mundo están utilizando sensores no solo en sus vehículos, sino también en sus plantas de fabricación, donde asisten a las máquinas autónomas y mejoran la seguridad de los trabajadores de la industria automotriz.

Otros factores que han contribuido a la IoT, en especial en el entorno empresarial e industrial, incluyen el almacenamiento rentable en la nube y el surgimiento del análisis de datos que permite a las organizaciones administrar y extraer información a partir de cantidades masivas de datos. Pero, nunca estamos demasiado lejos de las principales fuentes de datos. Son los sensores los que capturan datos y es la conectividad móvil la que transmite los datos a otro dispositivo o a la nube.

Debemos recordar que la IoT no es meramente un fenómeno único, fácil de definir. Hay diversos segmentos y mercados que componen la IoT. Para el consumidor, IoT implica la tecnología portátil y los artefactos “inteligentes”, como termostatos y televisores. En el sector industrial, IoT significa máquinas autónomas y equipos con sensores. En el espacio empresarial, IoT significa Big Data (Datos masivos) y análisis de marketing. En resumen, desde los procesos de fabricación hasta los productos de consumo, la IoT es tan diversa como la economía global en sí.

La cuestión entonces es la siguiente: ¿Cómo pueden las empresas utilizar estos objetos conectados para mejorar sus procesos, aumentar la productividad, reducir los costos y evitar riesgos?

Una nueva era económica

Para apreciar las oportunidades que IoT ofrece a las empresas, debemos comenzar por entender su impacto macroeconómico. En un documento de política para la Comisión Europea, RAND Europe ubica las estimaciones superiores del potencial económico de IoT entre USD 1.400 billones por año (alrededor de € 1.090 billones) y USD 14.400 billones (unos € 11.200 billones) en todos los sectores, a nivel mundial. Además, la venta de dispositivos y servicios conectados será de alrededor de USD 2.500 billones en 2020, mientras que las inversiones acumuladas indicadas por la conexión de miles de millones de dispositivos conectados alcanzarán como mínimo € 2.000 billones a precios actuales. Por ejemplo, el estudio de RAND observa que China ya ha destinado € 625 millones (USD 775 millones) a inversiones en la IoT^{viii}.

Sin lugar a dudas, en cinco años no habrá industria en la que la IoT no tenga un impacto directo. El ritmo de adopción, sumado a las expectativas y exigencias del consumidor convertirá rápidamente todas las industrias ajenas a la IoT, por no hablar de las empresas individuales, en reliquias de museo. Pero, aún así, muchas industrias tienen tiempo para entender la IoT y en qué áreas podrían mejorar sus objetivos estratégicos a largo plazo. Como primer publicación de esta serie, el objetivo de este artículo técnico es ofrecer a los lectores ejemplos actuales de cómo ciertas industrias han comenzado a utilizar la IoT. Esperamos que los lectores puedan comenzar a implementar una estrategia para su propio negocio en función de los ejemplos que proporcionamos a continuación. Dado que la IoT ofrece usos que abarcan el espectro comercial, hemos dividido la forma en que cada industria utiliza la IoT en cuatro categorías:

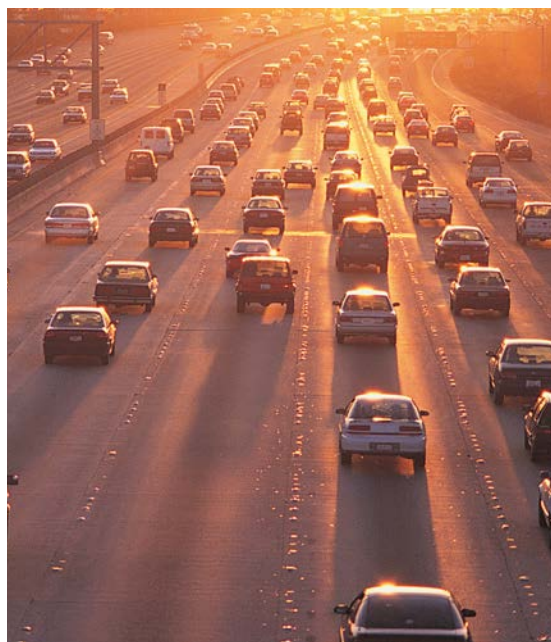
seguridad, eficiencia,
toma de decisiones impulsada por datos
e infraestructura

INDUSTRIA AUTOMOTRIZ

Seguridad: En 2010, la Organización Mundial de la Salud informó que 1,24 millones de personas en todo el mundo murieron como consecuencia de accidentes automovilísticos. Cada año, alrededor de 30.000 personas mueren en accidentes automovilísticos en Europa. En Estados Unidos, ocurre algo muy similar. En Asia, el problema es mucho peor. En China e India solamente, más de 400.000 personas mueren en accidentes automovilísticos cada año.

La tecnología de la IoT, en especial el auge de los sensores centrados en la seguridad incorporados a los automóviles, promete una reducción drástica del índice mundial de muertes causadas por accidentes automovilísticos.

Dado que la gran mayoría de los accidentes automovilísticos son causados por errores humanos, el reemplazo del componente humano de toma de decisiones en la conducción es el objetivo para los vehículos autónomos.



En mayo de 2015, Daimler Trucks North America, empresa alemana con sede en EE. UU., anunció que estaba lista para probar el camión sin conductor Freightliner Inspiration Truck, en las carreteras de Nevada. Pero, los automóviles sin conductor, como los que están desarrollando empresas como Google y Tesla, están entrando en funcionamiento lentamente. Muchos incorporan sensores de seguridad que ofrecen al conductor una vista de 360 grados de su vehículo, mientras que otros funcionan de forma autónoma y protegen el vehículo sin intervención directa del conductor. Las empresas automotrices también usan los datos que estos sensores recopilan para producir automóviles más seguros y eficientes. Si bien estos dispositivos de recopilación de datos plantean ciertas inquietudes de privacidad, son el próximo paso en la evolución de los automóviles.

SECTOR BANCARIO

Eficiencia: El sector financiero ha ayudado a liderar el uso de la tecnología para móviles para que las transacciones bancarias sean más sencillas para el consumidor promedio. Un ejemplo obvio es el que la IoT y la industria bancaria se cruzan es el de los cajeros automáticos (ATM), que es posible equipar con tecnología de sensores. Es posible que un usuario con los identificadores biométricos adecuados pueda algún día retirar dinero de un cajero automático dotado de sensores, sin necesidad de sacar su tarjeta de débito. Con una perspectiva de futuro, puede decirse que la IoT promete conectar las actividades financieras del consumidor con otros aspectos de su vida. Un ejemplo es conectar el monitor de salud del usuario con su cartera financiera. Como observó Deloitte, una crisis de salud captada por el monitor podría enviar una señal al banco del usuario para que equilibre automáticamente su cartera y reduzca así al mínimo su exposición financiera^{xv}.

En un informe de 2014 sobre el "Bank of Things" (Banco de cosas), Accenture destacó: "El Banco de cosas anticipará las necesidades de los clientes y responderá a sus circunstancias cambiantes al ofrecer soluciones relevantes y oportunas que los ayuden a alcanzar sus objetivos. Seguirá siendo un asesor de confianza, un facilitador y un elemento que agregará valor para sus clientes, pero lo hará con una comprensión casi íntima de las necesidades y preferencias de cada cliente"^{xvi}.

SECTOR MARÍTIMO

Seguridad: Al igual que el resto de la industria del transporte, las empresas de transporte marítimo han equipado durante décadas sus flotas con diversos sensores para controlar los sistemas críticos de los navíos, las condiciones climáticas y marítimas y la carga. Actualmente, la tecnología de IoT permite que estos sensores recopilen datos que luego pueden analizarse para mejorar la optimización del viaje, la seguridad y los procesos de almacenamiento.

En un ejemplo, el software de fuente abierta utiliza los sensores de la embarcación para brindar información sobre el movimiento del navío en tiempo real a otras embarcaciones y a centros de coordinación del tráfico marítimo en tierra. En las palabras de un experto, el software de IoT “admite la toma de decisiones conjunta entre las partes interesadas clave para lograr operaciones marítimas más seguras, más eficientes y ecológicamente responsables^{xvii}.”

Toma de decisiones impulsada por datos: En el evento International CES 2015, la empresa Ericsson, con sede en Suecia, reveló una solución de IoT mejorada para el transporte marítimo. La plataforma basada en la nube conectaría los navíos en alta mar con “operaciones en tierra, proveedores de servicios de mantenimiento, centros de atención al cliente, socios de flotas/transporte y operaciones y autoridades portuarias”. La solución permitiría a operadores en mar y en tierra monitorear el consumo de combustible, el rendimiento de los motores, el clima, el tráfico y la navegación para alcanzar una mayor optimización del viaje, para el seguimiento de la ubicación y las condiciones del cargamento y, mediante comunicaciones mejoradas, las opciones de entretenimiento y telemedicina e incluso realzar el bienestar de la tripulación de la embarcación^{xviii}.

PROPIEDADES (BIENES RAÍCES)

Eficiencia: En cuanto a propiedades, ya hay objetos “inteligentes”, como termostatos y otros aparatos, que ayudan a los propietarios a mejorar la eficiencia energética y reducir los costos de los servicios públicos. Podemos esperar que estos productos proliferen a medida que la vivienda esté cada vez más “conectada”. Pero el valor real de la IoT en las viviendas aparecerá cuando estos aparatos conectados y otros objetos del hogar se comuniquen entre sí. Por ejemplo, un termostato inteligente de la vivienda conocerá la temperatura exterior y transmitirá los datos correspondientes al sistema de armarios de la vivienda, el cual sugerirá el atuendo adecuado para el día. Otro ejemplo es la sincronización de un sistema de la vivienda, por ejemplo el clóset, con el calendario del usuario. El clóset “sabe” entonces si el usuario tiene una reunión ese día y selecciona la indumentaria adecuada.

Toma de decisiones impulsada por datos: En la industria de bienes raíces, una vivienda equipada con IoT puede hacerlo todo excepto ocupar el lugar de un agente humano. Puede incluirse en las listas de venta apropiadas de bienes raíces y programar presentaciones porque “sabrán” cuándo los propietarios estarán fuera del hogar. Algunas empresas de corretaje de bienes raíces ya están experimentando con la tecnología iBeacon de Apple y carteles “En venta”. El concepto es que un posible comprador que pase por una casa en venta reciba un mensaje en su teléfono inteligente a través de iBeacon y brinde detalles al instante sobre la casa. Dentro de la casa, la tecnología iBeacon puede utilizarse para ofrecer a los posibles compradores los planos de la planta, testimonios en video de los propietarios anteriores e incluso oportunidades de renovación, probablemente en asociación con una tienda de mejora de viviendas y ferretería^{xxi}.

Infraestructura: Inundaciones, incendios y deterioro estructural: estos son los riesgos que toda empresa debe aceptar. No obstante, la tecnología de IoT, en especial los sensores incorporados en áreas de riesgo específicas, puede ayudar a reducir y, en algunos casos, eliminar estos problemas perdurables. Por ejemplo, los sistemas eléctricos pueden estar equipados con sensores que controlan el flujo de electricidad a través de un edificio. Cuando un cable o una conexión falla o está por fallar, con el consiguiente aumento de la probabilidad de incendio, los sensores pueden advertir de inmediato a los técnicos. Las empresas de bienes raíces pueden usar sensores de IoT en sus propiedades para controlar diversos incidentes relacionados con los riesgos, como la presencia de gases peligrosos, infestaciones de termitas, mal funcionamiento del sistema de calefacción, refrigeración y ventilación y las calderas, y el uso y desgaste general. Aunque una estructura en particular en apariencia esté en condiciones óptimas, los analistas pueden examinar la cantidad masiva de datos recopilados por estos sensores incorporados para identificar indicios de problemas futuros.



ENERGÍA

Eficiencia: La industria energética ya obtiene enormes ventajas de la tecnología de la IoT. A nivel del consumidor, los usuarios pueden utilizar aparatos avanzados y dispositivos “inteligentes” para reducir el uso y los costos de la energía. Las empresas también pueden utilizar estas tecnologías, pero a un nivel mucho más avanzado. Un edificio de oficinas con muchos locatarios independientes, por ejemplo, puede capturar y monitorear los usos de la energía de cada piso. Al analizar los datos, el edificio puede identificar las áreas de uso ineficiente de energía y reducir los costos.

Mientras tanto, la industria de la energía ha estado durante mucho tiempo a la vanguardia de la tecnología de la IoT, principalmente gracias a las formas novedosas en que las empresas de servicios públicos leen de forma remota el uso de energía por parte de clientes comerciales, industriales y residenciales. En efecto, Ericsson indica que, según se espera, la cantidad de dispositivos conectados que manejan las empresas de servicios públicos a nivel mundial aumentará de 485 millones en 2013 a 1.530 millones en 2020. De hecho, la industria de servicios públicos es la segunda fuente de ingresos más importante de los proveedores de servicios “máquina a máquina”, después de la industria automotriz y la industria del transporte. “Estos dispositivos van desde medidores, sensores de red eléctrica y activadores, a cajas de energía y aparatos eléctricos. Se utilizan para aplicaciones como supervisión y control de redes eléctricas, medición, administración y seguimiento de activos, y comunicaciones con operadores de campo”, afirma Ericsson^{xxii}.



INDUSTRIA AEROESPACIAL

Seguridad: Los sistemas de “vuelo digital por cable” han sido esenciales durante décadas para la industria aeroespacial. En términos simples, el “vuelo digital por cable” permite al piloto centrar su atención en el pilotaje del avión, mientras los sensores y sistemas automáticos se encargan del resto. En efecto, el “vuelo digital por cable” está avanzando a tal punto que, en muchos sentidos, los aviones son vehículos prácticamente autónomos. Por ejemplo, cuando el capitán Chesley B. “Sully” Sullenberger realizó un aterrizaje de emergencia en el río Hudson poco

después de despegar del Aeropuerto LaGuardia de Nueva York, piloteaba un Airbus A320, cuyos modelos anteriores lideraron el uso de los sistemas digitales de “vuelo digital por cable”. No es menospreciar la intervención del capitán Sullenberger decir que el “Milagro en el Hudson” pudo haber terminado en tragedia si no hubiera sido por los sensores altamente desarrollados de la aeronave que le permitieron enfocarse en el aterrizaje seguro del avión en el río^{xxiii}.

Eficiencia: En tierra, las empresas aeroespaciales están empleando la tecnología de la IoT para mejorar el mantenimiento y las medidas de seguridad. Por ejemplo, la empresa de mantenimiento de motores de aeronaves de General Electric utiliza sensores de a bordo en los motores de aviones a reacción para capturar en tiempo real datos del rendimiento de los motores. El volumen de datos que este proceso produce permite a GE aumentar la eficiencia de los motores, reducir los costos de combustible y acortar los tiempos de viaje^{xxiv}.

ATENCIÓN MÉDICA

Toma de decisiones impulsada por datos: Puede decirse que no hay ámbito de la atención médica que no emplee la tecnología de la IoT. A nivel del paciente, los objetos portátiles habilitados por la IoT permiten a los médicos capturar datos de salud que de otro modo no se conocerían. Los exámenes físicos anuales podrían llegar a ser obsoletos, ya que los médicos cuentan con abundantes datos de cada paciente que les permiten saber si se justifica un examen en persona. De igual manera, los pacientes con indicios de salud inquietantes que podrían no causar síntomas serían detectados por el médico antes de que surjan problemas más graves. Los médicos clínicos pueden usar estos datos no solo para entender mejor la salud de cada paciente, sino también para crear conjuntos de datos detallados de los subgrupos de pacientes, con el objeto de tratar y prevenir las enfermedades más antiguas de la humanidad.

Mientras tanto, los hospitales, que siempre han producido y almacenado volúmenes enormes de datos, pueden usar la tecnología de la IoT para encontrar correlaciones factible en los datos que recopilan. Por ejemplo, muchos hospitales acaparan intencionalmente inventarios excesivos para evitar la falta de suministros esenciales. Los escáneres con medios para aprovechar la IoT ofrecen a los administradores de hospitales una perspectiva directa de sus stocks y les permite conocer el momento en que ocurre la escasez. Además, los dispositivos de la IoT pueden mejorar drásticamente el tratamiento en los hospitales, en especial en situaciones de emergencia. Un asistente médico puede usar los dispositivos de la IoT para registrar los signos vitales y otras estadísticas del paciente, que luego se transmiten instantáneamente a la sala de emergencias. Cuando llega el paciente, los médicos ya no tienen que perder tiempo valioso en entender la afección del paciente porque ya la conocen.

FABRICACIÓN

Seguridad: Además, la IoT promete reducir drásticamente la tasa de lesiones y muertes relacionadas con el lugar de trabajo. Según la Organización Internacional del Trabajo, a nivel mundial mueren 2,3 millones de personas al año a causa de accidentes y enfermedades relacionados con el trabajo. Según la Comisión Europea, cada año más de tres millones de trabajadores son víctimas de accidentes graves en el trabajo, y 4.000 mueren por accidentes en el lugar de trabajo. La IoT puede ayudar a mantener a los empleados a salvo, en especial los que trabajan solos en áreas peligrosas, como las obras de construcción. Por ejemplo, la tecnología de objetos portátiles incorpora sensores para determinar cuándo un trabajador podría estar esforzándose de manera peligrosa o realizando una maniobra poco segura. Los sensores también pueden controlar las condiciones ambientales peligrosas, como las temperaturas extremas y la presencia de sustancias tóxicas. Además, los datos de comportamiento recopilados a través de estos sensores portátiles pueden ayudar a los gerentes de seguridad a entender cuándo hay probabilidades de que un trabajador sufra un accidente. Este elemento de pronóstico de la IoT, si bien en muchos sentidos sigue siendo teórico, es una de sus características más interesantes (y con potencial de explotación).

Toma de decisiones impulsada por datos: Las empresas también pueden utilizar los productos de la IoT para garantizar la integridad, la garantía de calidad y la seguridad de los componentes en sus cadenas de suministro complejas. Gartner, Inc., empresa de asesoramiento e investigación sobre la TI, estima que "un aumento de 30 veces en los dispositivos físicos conectados a Internet para el año 2020 modificará significativamente el acceso a la información para los líderes de cadenas de suministro y la exposición a riesgos informáticos". Los dispositivos de la IoT incorporados a toda la cadena de suministro ofrecerán a los gerentes por primera vez una perspectiva más profunda de sus procesos. De la visibilidad en tránsito a la seguridad de las estaciones de vehículos, los objetos de la IoT prometen revolucionar la manera en que las empresas diseñan, protegen y mantienen sus cadenas de suministro sensibles.

FOOD

Eficiencia: Las empresas de entrega de productos ya ofrecen a los consumidores la posibilidad de rastrear sus pedidos empaquetados en cada estación de procesamiento, pero la tecnología es mucho más útil cuando se la aplica a los negocios. Los sensores de IoT incorporados en el momento y el lugar correctos pueden ayudar a las empresas a rastrear los activos en tiempo real. Los datos recopilados pueden permitir a las organizaciones identificar los factores de ineficiencia y los cuellos de botella en sus cadenas de suministro. No menos importante es que los sensores instalados en medios de almacenamiento, como camiones con cámaras frigoríficas, puedan advertir a las empresas cuando el mecanismo de enfriamiento falla o está por fallar. Esto evita que el conductor (quien tal vez no verifique los productos sino varias horas después de la falla del enfriamiento) deba responsabilizarse de la vigilancia, y ofrece a las organizaciones un recurso para salvar cargamentos valiosos antes de que se desperdicien. En agricultura, la tecnología de la IoT incorporada a los campos, permite a los agricultores seguir de cerca la información crítica, como el uso del agua. Por ejemplo, un sensor puede informar al agricultor en qué áreas hay brechas en el sistema de riego o si está usando demasiada agua en un campo específico. Los adelantos de la IoT, especialmente cuando se los aplica en el mundo en desarrollo, prometen ser agentes de innovación en la producción y la distribución de alimentos.

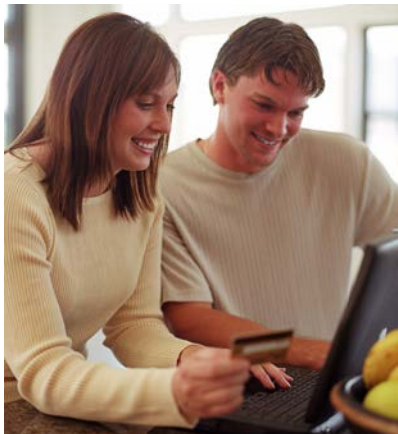


Riesgos de la IoT

En efecto, las promesas y el potencial de la nueva era de la IoT son portentosos. En muchos sentidos, las posibilidades de la IoT se ven limitadas solo por nuestra imaginación. En especial, cuando consideramos todos los datos que no se registran, toda la información que se nos escapa y cómo la IoT nos permite capturar finalmente estos datos y utilizarlos de una manera que ha eludido a la humanidad durante años y años, es fácil pasar por alto el lado oscuro del nuevo mundo de IoT. Pero las empresas no pueden permitirse invertir en sus sistemas de IoT sin entender primero los principales riesgos propios a todo sistema conectado a Internet. Desde el día en que encendimos el primer equipo, sabemos que nuestra dependencia de la tecnología puede generar alteraciones de mayor o menor envergadura. Esto no impide que las empresas adopten la IoT; por el contrario, las oportunidades superan con creces los riesgos. Sin embargo, cada empresa debe entender que cada problema resuelto por la IoT genera otro problema. Los siguientes son cuatro de los riesgos más importantes que conlleva la IoT:

PRIVACIDAD

Cuando los miles de millones de sensores del mundo adquieren constantemente datos del entorno que los rodea, lo cual incluye a los seres humanos, las inquietudes de privacidad adquieren importancia vital en el mundo de la IoT. Casi todo el mundo desarrollado ha intentado proteger a los consumidores del uso ilegal de la información confidencial pero, en muchos casos, las leyes no son adecuadas para proteger la enorme cantidad de maneras nuevas de recopilar y usar la información personal. El intento reciente de la Unión Europea de actualizar las leyes de derechos de autor (ver a continuación) es un síntoma de que muchas de las leyes del mundo desarrollado han perdido vigencia.



En las primeras etapas de Internet, los consumidores se familiarizaron (aunque no estuvieron realmente cómodos) con el software de rastreo, también llamado cookies. Dado que no había leyes específicas que limitaran el uso de cookies de un sitio web para rastrear el comportamiento de navegación del usuario, muchas empresas simplemente adoptaron la práctica sin dar especial importancia a las inquietudes del usuario. De hecho, fueron los navegadores los que respondieron a la ansiedad del consumidor con herramientas para limitar el uso de cookies y eliminarlas después de la sesión de navegación. En la actualidad, la legislación de la Unión Europea regula la manera en que se usan las cookies y el tipo de datos de los usuarios que pueden recopilar^{xxviii}, pero con el auge de la tecnología

móvil, que no necesita cookies para rastrear el comportamiento de los usuarios, muchas de estas leyes son cada vez más obsoletas e inadecuadas en un mundo de IoT.

De manera similar, EE. UU. también depende de modelos de reglamentación antiguos para los dispositivos y sistemas nuevos de IoT. Pero no hay ninguna ley federal que rija la recopilación y el uso de los datos personales. En cambio, EE. UU. depende de una mezcla dispar de leyes federales y estatales existentes para proteger la privacidad del consumidor. El clamor público ante el gobierno federal, en especial la Agencia Nacional de Seguridad (National Security Agency), por las actividades de "minería de datos" relacionadas con la aplicación de la ley y el contraterorismo, es un presagio de los debates públicos sobre política que surgirán en el futuro.

En enero de 2015, la Comisión Federal de Comercio (Federal Trade Commission) de EE. UU. publicó un informe que examinaba el estado de la IoT en EE. UU. y sugería “mejores prácticas” para su implementación por parte de las empresas en materia de datos y seguridad del consumidor. No obstante, el informe de FTC mantiene el enfoque de “toque ligero” del gobierno federal en lo que respecta a la reglamentación de Internet y, por consiguiente, de la IoT. Por ejemplo, el informe concluye “que cualquier legislación específica de la Internet de objetos interconectados sería prematura en este momento, dada la rápida evolución de la tecnología. Sin embargo, el informe insiste en el llamado reiterado de la Comisión para alcanzar una sólida legislación sobre seguridad de datos y notificación de transgresiones.”^{xxix}

Privacy concerns extend to the workplace as well. There are lots of programs on the marLas inquietudes de privacidad se extienden también al lugar de trabajo. Hay muchos programas en el mercado que permiten al empleador realizar un seguimiento del comportamiento de los trabajadores, generalmente a través del equipo personal del trabajador. Pero la IoT permite a los empleadores incorporar sensores que cubran prácticamente toda la oficina para controlar los hábitos de los empleados. Por ejemplo, un antiguo ejecutivo de ventas de California presentó una demanda contra su empleador alegando que fue obligado a descargar a su teléfono inteligente una aplicación de rastreo que el empleador utilizó para vigilar su paradero durante el horario de trabajo y después. La capacidad de IoT de rastrear y capturar las acciones humanas plantea diversas preguntas éticas que aún no se han respondido plenamente, como:

- ¿Un trabajador puede ser castigado por los datos recopilados a través de un objeto de IoT?
- ¿El empleador debe comunicar a sus empleados la existencia de sensores que rastrean su comportamiento?



CIBERSEGURIDAD

En la actualidad, las transgresiones en el ciberespacio son una amenaza importante para las empresas. Según una estimación, cada año los delitos informáticos cuestan USD 400.000 millones a las empresas. Desde la perspectiva de la IoT, lo más inquietante es que los ciberdelincuentes violan sistemas ostensiblemente seguros, con varias capas de protección. La complejidad de garantizar la seguridad de los dispositivos de IoT es un área de

mejora para las empresas, en especial al prepararse para el día en que aparezca el “ecosistema de IoT”, donde miles de millones de objetos estén conectados a Internet y entre sí.

Debemos recordar que cualquier dispositivo con conexión a Internet es una posible vía de ingreso para los piratas informáticos. Por ejemplo, en 2014 un pirata informático pudo penetrar un monitor de bebés para acosar a una niña de dos años de edad. La investigación de seguimiento sobre el producto, producido por la empresa china Focsam, descubrió que 40 000 de 46 000 dispositivos no habían sido actualizados con una medida de seguridad que hubiera evitado la violación.^{xxxii}

También debemos recordar que cuanto más automatizamos y conectamos ciertos sistemas, en especial los sistemas industriales, más abiertos estarán estos sistemas a la piratería informática. Una ciudad que construye una red inteligente de electricidad podría obtener importantes ahorros en los costos, gracias a la manera en que el sistema optimiza la resolución de los problemas. Al mismo tiempo, el sistema también ofrece al posible pirata informático una manera sencilla de interrumpir el suministro eléctrico de toda una ciudad desde su equipo.

En un ejemplo más, en abril de 2015 la Oficina de Rendición de Cuentas (Accountability Office) del gobierno de EE. UU. publicó un informe que analizaba las amenazas que conlleva la mayor interconexión entre los sistemas terrestres y de las aeronaves. “Esta interconexión potencialmente puede servir de acceso remoto no autorizado a los sistemas de aviónica de las aeronaves”, advirtió el informe^{xxxiii}. En otras palabras, un pirata o terrorista informático podría usar el sistema para asumir el control de la aeronave.

Debido a la interconexión en red inherente a la IoT, donde cada objeto conectado utiliza los datos de otros objetos conectados, también existe el riesgo de que el funcionamiento incorrecto genere fallas catastróficas en el sistema. Un objeto en mal funcionamiento podría hacer llegar datos incorrectos a otro dispositivo que funciona normalmente. Sin embargo, a medida que los datos inapropiados se desplazan hacia el sistema, comienzan a infectar cada vez más sistemas. Si consideramos un desastre natural, como una inundación, el mal funcionamiento de los sensores que vigilan la integridad de las represas y los diques, podría causar daños físicos masivos e incluso la pérdida de vidas.

Los ejemplos como estos enfatizan los nuevos riesgos de ciberseguridad de la IoT que muchas empresas enfrentarán. Si bien podemos esperar que los fabricantes de estos dispositivos mejoren con el tiempo sus medidas de seguridad, la cantidad misma de cosas conectadas está aumentando exponencialmente.

RESPONSABILIDAD

Cuando se trata de vehículos autónomos, como los automóviles sin conductor, nos enfrentamos a un dilema ético obvio: Segundos antes de un accidente, ¿un vehículo sin conductor debería hacer todo lo posible por proteger a los pasajeros aunque esto implique perjudicar a otros automovilistas o peatones? Cuando los seres humanos conducen, los daños colaterales, por terrible que pueda parecer, no plantean un problema ético. No se puede culpar a un ser humano en peligro cuando su instinto de supervivencia le hace girar bruscamente el automóvil hacia el peatón. Pero cuando son las máquinas las que toman las decisiones, ¿el peatón perjudicado en el accidente tiene una reclamación válida contra el fabricante del automóvil? ¿El conductor tiene una reclamación válida contra el fabricante del automóvil después del accidente en el que sufrió lesiones? Como lo establece el informe de la Comisión Europea sobre los dilemas éticos inherentes a la tecnología de la IoT, “la gente no está acostumbrada a objetos que tienen una identidad o actúan por su cuenta, en especial si su accionar es imprevisible.”^{xxxiv}

Otras preguntas sobre responsabilidad surgen cuando consideramos la propiedad de los datos. Con miles de millones de dispositivos que recopilan datos, las líneas divisorias no son tan claras en lo que respecta a quiénes son responsables de qué datos. Los objetos de la IoT funcionan de forma autónoma y junto con muchos otros objetos. Los datos se comparten, se procesan, y se vuelven a compartir y procesar rápidamente antes de que los ojos humanos puedan verlos. En otras palabras, es muy simple relacionar un dispositivo con ciertos datos, debido a que gran parte del potencial de la IoT yace en la constante transferencia de estos datos entre los objetos. Por ejemplo, un monitor cardíaco de IoT no se limitará a controlar el corazón del paciente para buscar signos de advertencia de un ataque cardíaco inminente. También podría acceder a los datos de otro objeto que rastree la rutina de ejercicios del paciente que, a su vez, toma los datos del dispositivo que controla la ingesta de alimentos. Si el paciente sufre un ataque cardíaco, ¿quién es responsable?



Los dispositivos de la IoT también plantean preguntas complejas en lo que respecta al mal funcionamiento de los dispositivos. Los sensores pueden estar incorporados a elementos de infraestructura de importancia crítica, como diques, puentes y carreteras para controlar la integridad estructural y las condiciones ambientales que podrían debilitar la integridad estructural. Una carretera próxima a un área de inundaciones podría tener sensores incorporados que saben en qué momento las precipitaciones superan el punto que advierte con anticipación a los ingenieros en caso de inundación. En efecto, la protección de la infraestructura es uno de los aspectos más interesantes de la IoT. Sin embargo, al volcar cada vez más nuestros sistemas críticos de infraestructura y seguridad a los objetos de IoT, corremos el riesgo de que se produzca una catástrofe si estos objetos fallan.

También podemos aplicar esto al sector privado. Por citar un ejemplo no letal, en abril de 2015 varios vuelos de American Airlines se retrasaron cuando el mal funcionamiento de software inutilizó las tablets que los pilotos utilizan para fines de navegación^{xxxv}. Si bien el mal funcionamiento se corrigió fácilmente con una actualización de software, los ejemplos muestran hasta qué punto estamos expuestos debido a nuestros dispositivos conectados. Cuando fallen, ¿estaremos preparados?

La situación de la IoT en Europa, EE. UU. y Asia

EUROPA

Con sus altas tasas de penetración de móviles, Europa está en una excelente posición para capitalizar la revolución de la IoT que se avecina. Pero, aunque la llegada de la IoT es inevitable, quedan obstáculos que las economías individuales deben superar para alcanzar el máximo potencial de la IoT. Un obstáculo es la simple competencia. Por ejemplo, en marzo de 2015, durante una conferencia de la Comisión Europea celebrada en Bruselas, representantes de la industria pesada europea, fabricantes de automóviles, fabricantes de electrodomésticos, empresas de telecomunicaciones y legisladores se reunieron para analizar cómo mejorar la competitividad del continente en lo que respecta a la IoT, en especial cuando las empresas de EE. UU., como Apple y Google, parecen estar logrando más adelantos.

El resultado de la conferencia fue una nueva alianza de la industria europea, respaldada por la Unión Europea, que incluye empresas del más alto nivel, entre ellas Phillips, Bosch, Orange, Alcatel, Nokia, Siemens, Telefonica y Volvo, para estimular la innovación en materia de IoT. Como afirmó Anne Lauvergeon, presidente de Sigfox, la nueva empresa francesa de trabajo en red y miembro de la nueva alianza de IoT: "Crear un ecosistema para la innovación vinculada a la IoT es fundamental para hacer frente a la competencia internacional."^{xxxvi}

Al mismo tiempo, la Unión Europea está trabajando para alcanzar un mercado digital único al someter a escrutinio las leyes actuales en materia de telecomunicaciones. El objetivo de la nueva legislación es eliminar los impedimentos para la transferencia de datos "al derribar las barreras nacionales en áreas como el comercio electrónico y las leyes de derechos de autor", según el Wall Street Journal. Esta necesidad de revisar el entorno regulatorio es reflejo de la naturaleza cambiante de la nueva economía de IoT, donde la capacidad para transferir e intercambiar rápida y fácilmente cantidades masivas de datos se convertirá en un sello del éxito de una región.

Además de actualizar la legislación, la nueva economía de IoT también exigirá una inversión significativa en infraestructura tecnológica. En marzo de 2015, European Investment Bank (EIB) organizó una conferencia en Berlín sobre el tema "Momentum for Europe—Innovation and Competitiveness" (Impulso para Europa: innovación y competitividad). Durante el discurso principal, Jeremy Rifkin, presidente de Foundation on Economic Trends y asesor de política para Francia, Alemania y la Unión Europea, habló sobre la forma en que la extensión y el despliegue de la IoT ayudará a la "Europa digital" a acceder a una "Tercera revolución industrial."^{xxxix}

No obstante, Rifkin observó que la inversión europea en plataformas tecnológicas "anacrónicas" alcanzó un total de USD 741.000 millones en 2012. Si el 25 por ciento de estos fondos se reorientaran en cada región de la Unión Europea hacia la infraestructura de IoT, los beneficios plenos de la "Europa digital" se podrían alcanzar para el año 2040. Es decir que, según la opinión de un experto, se están invirtiendo demasiados euros en el fortalecimiento de un modelo económico más antiguo a expensas del futuro.

ESTADOS UNIDOS

En 2014, las empresas de capital de riesgo invirtieron casi USD 11.900 millones en empresas específicas de Internet, la mayor inversión desde 2000 y la cúspide de la burbuja "Dot Com" (punto com). Si bien no todo este capital se invirtió en dispositivos específicos de IoT, el interés en la IoT en EE. UU. es por cierto más alto que nunca. En marzo de 2015, por ejemplo, IBM anunció que invertiría USD 3.000 millones en una nueva "división de Internet de objetos interconectados."^{xlii}

En efecto, el sector privado está tratando de mantener a EE. UU. a la vanguardia de la revolución de IoT. En 2014, los gigantes del sector de software y tecnología, como AT&T, Cisco, General Electric, IBM e Intel, anunciaron el Consorcio de Internet Industrial (Industrial Internet Consortium) para crear normas de ingeniería en torno a los objetos de IoT. La Casa Blanca y otros organismos gubernamentales también están involucrados en este ente no vinculante. Aunque FTC sugirió que el gobierno federal evite la reglamentación de la IoT por el momento, las agencias gubernamentales han comenzado a trabajar de forma paralela a las empresas privadas para producir aplicaciones públicas para la tecnología de IoT. Por ejemplo, en 2014, los representantes de Defense Advanced Research Projects Agency (DARPA), el Departamento de Transporte y la Administración de Salud de Veteranos se reunieron en Washington para analizar la tecnología de IoT en el sector público.^{xliv}

No obstante, Estados Unidos se ha quedado atrás de otros países desarrollados, en especial de Asia, en lo que respecta al acceso y las velocidades de banda ancha. Según Akamai, la empresa de tráfico digital, EE. UU. ocupa el puesto 14 en cuanto a velocidad de banda ancha. Si bien la conectividad general en EE. UU. es una de las más altas del mundo, la infraestructura obsoleta, los obstáculos que representan las reglamentaciones locales y el alto costo del acceso a la banda ancha limitan el avance de EE. UU. en materia de adopción e innovación en IoT.

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^{xlvi}.

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.^{xlvii}

Aunque IDC pronostica que para el año 2020, 1 de cada 5 objetos conectados a Internet estará en China, advierte que el tamaño del mercado no es lo mismo que la madurez del mercado. "Si bien la oportunidad del mercado en China hace parecer pequeños a los otros países líderes, como Corea del Sur, India, Indonesia y Australia, en términos de valor monetario esto no significa que sea el más maduro", afirmó Charles Reed Anderson, vicepresidente asociado y director de movilidad e Internet de objetos interconectados en IDC Asia/Pacific Anderson. "Para evaluar la madurez de un mercado, comparamos la cantidad total de cosas conectadas a la población general para obtener una cifra de conexiones por persona. Teniendo en cuenta este cálculo, descubrimos que los tres mercados principales más maduros eran Corea del Sur, Australia y Nueva Zelanda, en tanto que China ocupa el sexto lugar de los 13 países de la región de Asia-Pacífico excluido Japón."^{xlviii}

No obstante, en su condición de centro de fabricación mundial, Asia continúa obteniendo notables ganancias de una economía de IoT.

Conclusión

No es una exageración decir que la IoT dará lugar a una nueva era económica para todo el mundo. Las promesas de la IoT no se limitan a las mejoras de los procesos y los modelos económicos actuales, sino que tienen un alcance transformacional. La economía de la IoT revolucionará la manera en que las empresas producen, funcionan y rinden. Y el cambio se está produciendo más rápido que cualquier otra revolución industrial anterior.

Al mismo tiempo, la IoT presentará desafíos significativos en todos los sectores y para todas las industrias. A medida que resuelva los problemas que han acosado a las empresas durante décadas, y tal vez siglos, también creará dilemas completamente nuevos, vinculados tanto a los procedimientos como a la ética. Las inquietudes sobre privacidad, ciberseguridad y responsabilidad de productos y propiedad no tardarán en alcanzar una envergadura comparable a las oportunidades que presenta la IoT. Si bien las empresas deben comenzar a implementar la tecnología de IoT si esperan sobrevivir a largo plazo, también deben implementar estrategias que respondan a los numerosos riesgos relacionados con la IoT.

En la próxima entrega de esta serie, investigaremos en detalle estos riesgos y presentaremos los pasos prácticos para que las empresas los eviten o los minimicen. También plantearemos la manera en que la industria de seguros se preparará para ayudar a las empresas a explorar este nuevo mundo de IoT. En muchos sentidos, la industria de seguros se posiciona para obtener el máximo beneficio de los sensores incorporados que generan cantidades masivas de datos, lo cual ofrecerá perspectivas más profundas sobre la reducción al mínimo de los riesgos para los clientes. La industria de seguros, que desde hace tiempo está en el centro de los análisis impulsados por datos y la mitigación de riesgos, estará lista para ayudar a maximizar las oportunidades de IoT de las empresas y minimizar su exposición.

Citations

- i <http://www.rfidjournal.com/articles/view?4986>
- ii RAND: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, 2012
- iii CISCO: The Internet of Things How the Next Evolution of the Internet Is Changing Everything (La Internet de objetos interconectados, cómo la próxima evolución de la Internet está cambiando todo), 2011
- iv <http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-europe.pdf>
- v Dubravac, Shawn. "Digital Destiny." P. 68
- vi HBR-Verizon INTERNET OF THINGS: SCIENCE FICTION OR BUSINESS FACT? (INTERNET DE OBJETOS INTERCONECTADOS: ¿CIENCIA FICCIÓN O REALIDAD EMPRESARIAL?), 2014
- vii RAND: Europe's policy options for a dynamic and trustworthy development of the Internet of Things (Opciones de política de Europa para un desarrollo dinámico y confiable de la Internet de objetos interconectados) , 2012 p. 14
- viii ibid
- ix http://www.who.int/gho/road_safety/mortality/en/
- x http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm
- xi <http://morth.nic.in/writereaddata/mainlinkFile/File1465.pdf> and http://www.chinadaily.com.cn/china/2011-01/07/content_11808453.htm
- xii <http://www.forbes.com/sites/dougnewcomb/2015/05/08/daimler-autonomous-truck-has-huge-commercial-implications/>
- xiii © 2012 Google Inc. All rights reserved. Google and the Google Logo are registered trademarks of Google Inc.
- xiv Copyright 2002-2015 Tesla Motors, Inc. All Rights Reserved.
- xv <http://www2.deloitte.com/us/en/pages/finance/articles/internet-of-things-financial-services-industry.html>
- xvi <http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Bank-of-Things.pdf>
- xvii <http://osdelivers.blackducksoftware.com/2015/02/11/industrial-internet-of-things-in-the-maritime-industry/>
- xviii <http://www.rcrwireless.com/20150106/featured/ericsson-maritime-platform-targets-shipping-connectivity-tag2>
- xix <http://www.inman.com/2014/07/08/internet-of-things-could-be-most-disruptive-to-real-estate/>
- xx iBeacon is a trademark of Apple Inc., registered in the U.S. and other countries.
- xxi <http://realtormag.realtor.org/technology/feature/article/2015/03/real-estate-and-internet-things>
- xxii <http://www.ericsson.com/res/docs/2014/gtwp-op-transforming-industries-awprint.pdf> p. 4
- xxiii <http://www.cnn.com/2009/OPINION/11/18/langewiesche.miracle.hudson.flight/index.html?iref=24hours>

- xxiv <http://www.forbes.com/sites/ptc/2014/06/23/will-the-internet-of-things-revolutionize-the-aircraft-industry/>
- xxv <http://www.ilo.org/global/topics/safety-and-health-at-work/lang--en/index.htm>
- xxvi <http://www.euractiv.com/sections/social-europe-jobs/commission-publishes-health-and-safety-strategy-eu-workers-302665>
- xxvii <http://www.gartner.com/newsroom/id/2688717>
- xxviii http://ec.europa.eu/ipg/basics/legal/data_protection/index_en.htm
- xxix <https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices>
- xxx <http://www.techweekeurope.co.uk/mobility/lawsuit-tracking-app-168043>
- xxxi <http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/>
- xxxii <http://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/>
- xxxiii <http://www.gao.gov/products/GAO-15-370>
- xxxiv http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1752
- xxxv http://www.nytimes.com/2015/04/30/business/several-american-airlines-flights-are-delayed-by-an-app-malfunction.html?_r=0
- xxxvi <http://blogs.wsj.com/digits/2015/03/25/europe-wants-to-bring-its-industry-online-before-google-apple-make-it-obsolete/>
- xxxvii <http://www.wsj.com/articles/eu-considers-new-telecom-rules-to-level-the-playing-field-1427295277>
- xxxviii <http://www.eib.org/infocentre/events/all/momentum-for-europe.htm>
- xxxix <http://www.automatedtrader.net/headlines/153295/digital-europe-the-rise-of-the-internet-of-things-and-the-transition-to-a-third-industrial-revolution>
- xl *ibid*
- xli <http://nvca.org/pressreleases/annual-venture-capital-investment-tops-48-billion-2014-reaching-highest-level-decade-according-moneytree-report/>
- xlii <http://www.theglobeandmail.com/report-on-business/international-business/us-business/ibm-to-invest-3-billion-in-new-internet-of-things-unit/article23722378/>
- xliii http://bits.blogs.nytimes.com/2014/03/27/consortium-wants-standards-for-internet-of-things/?_php=true&_type=blogs&_r=1
- xliv http://www.washingtonpost.com/business/on-it/dot-va-reps-discuss-how-the-federal-government-could-use-internet-of-things/2014/08/06/d9ac6410-1d84-11e4-ae54-0cfe1f974f8a_story.html
- xlv http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf?WT.mc_id=soti_Q114
- xlvi HBR-Verizon INTERNET OF THINGS: SCIENCE FICTION OR BUSINESS FACT? INTERNET DE OBJETOS INTERCONECTADOS: ¿CIENCIA FICCIÓN O REALIDAD EMPRESARIAL), 2014 p. 7
- xlvii <http://www.idc.com/getdoc.jsp?containerId=prHK25553415>
- xlviii *ibid*

The Consumer Technology Association (CEA) is the technology trade association representing the \$286 billion U.S. consumer electronics industry. More than 2,000 companies enjoy the benefits of CEA membership, including legislative and regulatory advocacy, market research, technical training and education, industry promotion, standards development and the fostering of business and strategic relationships. CEA also owns and produces CES – The Global Stage for Innovation. All profits from CES are reinvested into CEA's industry services. Find CEA online at CE.org, InnovationMovement.com and through social media at ce.org/social.

American International Group, Inc. (AIG) es una organización líder de seguros a nivel internacional que presta servicio a clientes en más de 130 países y jurisdicciones. Las compañías de AIG prestan servicio a clientes comerciales, institucionales y a personas físicas a través de una de las más amplias redes internacionales de seguros de propiedad y de accidentes, de cualquier aseguradora. Además, las compañías de AIG son proveedoras líderes de seguros de vida y servicios de jubilación en Estados Unidos. Las acciones ordinarias de AIG se cotizan en las bolsas de valores de Nueva York y Tokio [New York Stock Exchange y Tokyo Stock Exchange].

Información adicional acerca de AIG se puede encontrar en www.aig.com | YouTube: www.youtube.com/aig | Twitter: [@AIGinsurance](https://twitter.com/AIGinsurance) | LinkedIn: www.linkedin.com/company/aig

AIG es el nombre de comercialización de bienes-siniestros de las operaciones internacionales de seguros generales, de propiedad y accidente, de vida y jubilación de American International Group, Inc. Para más información, visite nuestro sitio web en www.aig.com. Todos los productos y servicios están emitidos y son prestados por subsidiarias o afiliadas de American International Group, Inc. Es posible que los productos y servicios no estén disponibles en todos los países, y la cobertura está supeditada al lenguaje real de la póliza. Los productos y servicios que no sean de seguro podrían ser prestados por fuentes externas independientes. Ciertas coberturas de seguros de propiedad y accidente podrían ser brindadas por un asegurador de líneas excedentes. Los aseguradores de líneas excedentes generalmente no participan en fondos de garantía del estado, por lo que los asegurados no están protegidos por tales fondos.

© American International Group, Inc. Todos los derechos reservados.

12/15 SP812T



Bring on tomorrow®