TEC DE MONTERREY CAMPUS CIUDAD DE MÉXICO

"INTERNET DE LAS COSAS, SEGURIDAD Y SALUD"

por; Elizabeth Rodríguez Fallas

La sociedad está en constante cambio. Uno de los cambios que más ha marcado al mundo fue la revolución industrial que dio paso a una nueva economía, una nueva sociedad y un gran avance para la tecnología. Pero este no ha sido el único, ha habido guerras, descubrimientos científicos, cambios en la naturaleza, entre otras cosas que han generado un cambio en el mundo. En especial hubo otro gran movimiento que al igual que la revolución industrial cambió al mundo completamente, el surgimiento de las computadoras y posteriormente el de internet.

El surgimiento de estas dos tecnologías que se complementan la una a la otra dio paso a lo que conocemos como un mundo globalizado ya que alteró notablemente la forma en la que la sociedad en general se comunica y percibe el mundo. Las personas en la actualidad buscan sistemas automatizados para la mayor parte de las cosas que hacen. Están en busca de una constante mejora en la tecnología, y como siempre lo repiten, la ciencia y la tecnología no descansan. Por ello ahora estamos entrando a una nueva era de muchos avances tecnológicos que es, por decirlo así, la continuación del surgimiento de las computadoras, la era del internet de las cosas.

El termino del internet de las cosas resulta bastante obvio al estar relacionado completamente con su nombre, "conectar todas las cosas a internet", sin embargo es un término complejo por todo lo que involucra. Uno de los ejemplos más usados del internet de las cosas es el de un refrigerador inteligente que te sugiere que puedes cocinar de

acuerdo a lo que tienes dentro de él y te proporciona una lista de supermercado con lo que te hace falta. O el ejemplo de los focos inteligentes que por medio de una aplicación y obviamente estar conectados a internet pueden ser encendidos o apagados desde cualquier lugar en el que estés. Estos dos ejemplos son los más utilizados debido a que son artefactos inteligentes que ya existen desde hace varios años pero pueden resultar un tanto aburridos ya que es el típico ejemplo que te brindan cuando alguien habla del internet de las cosas. La tecnología no se queda en estos dos aparatos, se estima que en un futuro próximo la mayoría de nuestros objetos personales estarán conectados a internet, lo cual es una idea asombrosa que promete un estilo de vida más controlado y mejor organizado.

Al igual que todo lo que existe, el internet de las cosas tiene sus ventajas y sus desventajas. Las ventajas son muchísimas, ya que al igual que el internet hoy en día, el internet de las cosas nos abre las puertas a un mundo lleno de posibilidades, en infinitas áreas como economía, comunicación, salud, etc. Pero ante una idea maravillosa debemos detenernos a pensar … ¿Tenemos la capacidad de red para abastecer todas las cosas? ¿Qué va a pasar con la seguridad y privacidad de la información que se maneje?

Uno de los puntos que pueden resultar más interesantes es la cuestión de seguridad y privacidad de la información personal que va a estar disponible en la red. Una frase común de escuchar en un ámbito de tecnologías de la información es “Si se puede programar se puede hackear”. Es alarmante saber que toda nuestra información personal, el registro de lo que hacemos, de lo que compramos, de lo que comemos, de nuestro entretenimiento sea accesible a cualquier persona que pueda hackear nuestros dispositivos conectados a internet. ¿Realmente queremos conectar nuestra vida a internet cuando alguien con un sencillo proceso puede tener acceso a todo?

Ahora consideremos que la tecnología avanza para mejorar la vida de las personas y algo donde aun hay mucho que mejorar es en la salud. ¿Qué va a pasar cuando una persona conecte su cuerpo a internet por cuestiones de salud, monitoreo, observación, aplicación de dosis, etc.? ¿Cómo se va a manejar que alguien hackeé el aparato que te administra medicina y tenga la capacidad de dañar tu salud con un solo click?

La preocupación del internet de las cosas relacionada con la salud abrirá paso a grandes dilemas éticos y a la búsqueda de mejoras en el ámbito de seguridad computacional. Y nos lleva a la pregunta más importante ¿Por qué deberíamos conectarnos a algo tan peligroso para nuestra integridad?

El internet de las cosas (IoT por la siglas en inglés Internet of Things) es un concepto que surgió en el MIT en 1999 y fue propuesto por Kevin Ashton tras investigaciones de radio frecuencia en red y funcionamiento de sensores. Se plantea que cada ser humano esta rodeado de 1000 a 5000 mil cosas y que estas cosas pueden conectarse a internet. En sí, el internet de las cosas es un concepto que involucra la comunicación efectiva entre las cosas y las personas, ayuda a mejorar la rapidez, el proceso y el análisis de la información para monitorear y tomar decisiones.

El internet de las cosas es simplemente una interacción entre el mundo virtual y el mundo físico que traerá grandes beneficios. Se estima que en 2020 existirán 30 billones de dispositivos conectados a una conexión IP, que esto traerá una mejora económica y ayudará a dar una experiencia más personalizada y predictiva con respecto a lo que se desee hacer y esté conectado a la red.

El IoT se relaciona con los términos big data, cloud computing, social networks y movilidad. Los cuales a lo largo de la historia del internet y con su evolución han ayudado a

mejorar aspectos tecnológicos y llevarnos a lo que se esta viviendo hoy en día en un mundo globalizado. Gracias a los avances tecnológicos, enfocándonos directamente en el internet se ha logrado reducir el costo de la comunicación y mejorarla, incrementar el interés por invertir en la tecnología, reducir los costos de conexión, hacer la tecnología accesible para todo el mundo.

Más específicamente el IoT involucra varios ámbitos como las cosas, las puertas, la nube, los routers, los repetidores, la seguridad, entre otras. Las cosas literalmente son las cosas o dispositivos que están comunicadas por medio de sensores y por medio de una conexión IP. Las puertas actúan como intermediarios entre la nube, proporcionan seguridad, conexión y capacidad de manejo a los dispositivos conectados. La red es la que se encarga de tener routers, gateways, repetidores, étcetera para garantizar una buena conexión para todos los dispositivos y de esa forma mantener un buen manejo de la información. La nube contiene la información obtenida por las cosas y la almacena de forma organizada. Todos estas en conjunto ayudan a que el IoT exista.

Una de las dudas constantes cuando se habla acerca del internet y el almacenamiento de información es la nube. La nube es simplemente una gestión de recursos e información que permite brindar servicios a través de la red. Hay tres tipos principales de nube, la pública, la privada y la híbrida. La pública es a la que todos los usuarios tienen acceso, ésta se controla por la empresa que brinde el servicio de conexión y no es necesario que el usuario tenga noción de qué pasa. La privada es más cara que la pública pero más segura, usualmente se utiliza en las empresas que necesitan tener su información más protegida. Y por último la híbrida es una mezcla de la pública y la privada

y es utilizada por las empresas que requieren menos seguridad que la de una nube privada pero más que la pública.

Pensar que en un futuro próximo todo estará conectado a la red y que esto nos dará beneficios es un planteamiento maravilloso, pero como se mencionó antes, todo lo que esté conectado a internet es vulnerable a ataques. Por ello surge el término hacker, que se refiere originalmente a las personas que tenían soluciones de mejora para la sociedad por medio de las computadoras pero que usualmente no respetan los protocolos ni las normas de la red. Generalmente se conoce a los hackers como las clásicas personas que sin permiso acceden a información privada y que se aprovechan de medios de internet para robar información y dinero. Los dispositivos que antes no estaban conectados ahora lo estarán y esto abre el campo de posibles ataques cibernéticos.

Tal vez se considere que el internet de las cosas es algo que tiende hacia el futuro pero como se mencionó anteriormente es algo de aquí y ahora. Además, el IoT no solo se concentra a las cosas físicas si no que está siendo utilizada como un gran medio para mejorar áreas como la salud de las personas. Por ejemplo 2015 fue catalogado como el año de los wearables. ¿Qué es un wearable? Es un dispositivo que está diseñado para que una persona lo porte y está orientado principalmente a monitorear temas de salud. En 2015 se introdujeron los smartwatches y los smartbands que son relojes o pulseras que miden la cantidad de pasos que se dan, el tiempo de sueño que se tiene, el ritmo cardiaco, entre otros. Estos dispositivos se conectan por medio de una conexión IP a dispositivos móviles y así la información que se tiene es almacenada en la nube. Con ellos se pueden brindar estadísticas acerca de la salud a nivel personal y a nivel zona.

Otro ejemplo es la intensa lucha contra la parálisis cerebral. Se ha creado un sistema que interpreta los deseos del cerebro y por medio de una conexión IP envía comandos de movimiento a las extremidades. Todo esto surgió con el deseo de que las personas que sufren algún tipo de parálisis puedan conectar inalámbricamente su cuerpo para recuperar el movimiento. El ejemplo más claro de esto es la paciente Cathy Hutchinson quien tiene parálisis completa y el 12 de abril de 2011 logró mover con su mente un brazo robótico.

De igual forma se ha implementado el internet de las cosas para combatir epidemias mundiales. En 2015 la empresa IBM lanzó un proyecto como medio para detener el contagio de ébola específicamente en África. El proyecto involucra a una máquina llamada Waston que es conocida por su capacidad para analizar y aprender información. Mediante una página de internet a la cual se puede tener acceso desde cualquier dispositivo móvil o computadora fija se registraban los casos sospechosos y confirmados de ébola. Esta página sirve para detectar donde estaba surgiendo la epidemia y después de comparar las características de los datos ingresados con otros casos dar un pronóstico y sugerir un tratamiento al paciente que probablemente no tenía acceso inmediato a un médico por la situación.

Este es uno de los muchos proyectos que se tienen acerca de consultas y seguimientos online. Las consultas online en general han mostrado un gran beneficio pero se estipula que es debido a la falta de confianza de las personas a este tipo de plataformas y la negación de los médicos a cambiar los métodos de servicio. Se espera que con el paso del tiempo y la integración de médicos jóvenes al ámbito de trabajo se aumente el uso de la tecnología para brindar un servicio de salud más eficaz.

Otro ejemplo actual es el concurso Wireless Innovation Project que es creado por una empresa llamada Vodafone, donde hay diversos proyectos de salud. Como el diafragma inteligente que es un monitor inalámbrico para embarazos de alto riesgo buscando prever problemas en bebés que nacen prematuros. Igualmente hay un proyecto de un estetoscopio inteligente que se conecta a un dispositivo android y ayuda a diagnosticar enfermedades pulmonares incluso mejor que los estetoscopios comunes. Otro proyecto del mismo concurso es el "Cellscope" que busca detectar y diagnosticar enfermedades por medio de microscopios, conexión a internet y conexión a una cámara de celular. Es importante destacar que todos estos proyectos están orientados principalmente a áreas de vulnerabilidad económica.

Existen miles de ejemplos adicionales a los ya mencionados de cómo por medio del internet de las cosas se puede solucionar problemas de alzheimer, cáncer, nutrición entre otras enfermedades. Nuevos proyectos surgen cada día y la esperanza en la salud aumenta, sin embargo sigue el conflicto de la seguridad, la protección de las personas y los datos.

La seguridad de la información en internet es un tema que siempre será conflicto ya que siempre existe el error humano y el internet está creado por los humanos. Ese error humano puede ser aprovechado por otro humano que lo detecte, filtrarse a los dispositivos y obtener información. Ahora con la implementación del internet de las cosas todo lo que conectemos a la red será vulnerable a hackeo, pero no solo a hackeo a nivel personal si no a nivel masivo. La información de las personas en conjunto puede ser muy llamativa para el sector privado, para el gobierno y para los ciberdelincuentes.

Una de las demostraciones acerca del riesgo de los aparatos conectados a internet fue hecha por unos científicos que ilegalmente accedieron a automóviles, desactivaron los frenos, apagaron las luces y repentinamente activaron los frenos sin autorización del conductor. De igual forma se puede acceder a los controles de GPS alterando la ruta y desviando a la persona para llevarla a lugares de vulnerabilidad. Otro ejemplo es en los hogares que cuentan con dispositivos conectados a internet se puede manipular la iluminación, el consumo de gas y el uso de puertas y de cámaras de seguridad teniendo control total sobre la casa.

Los ejemplos anteriores a algunos les podrían sonar inofensivos pero no lo son. Planteemos esas situaciones con la salud. Por medio de un hackeo a una aplicación como la del estetoscopio se pueden diagnosticar enfermedades erróneas y recetar tratamientos equívocos a las personas para beneficiar o perjudicar a algún sector. Se pueden vender los datos de los usuarios de una aplicación al sector privado y se prevé que ese será un gran negocio para los atacantes cibernéticos ya que se estima que se generarán mayores ganancias que al clonar tarjetas de crédito. Con la venta y alteración de los datos se pueden perder privilegios de los seguros por medio de diagnósticos erróneos.

Se pueden malinterpretar los datos de las epidemias con en el caso del proyecto de IBM y el ébola generando discriminación a las personas y a los sectores donde se encuentren más casos. Todo esto mediante una violación al protocolo de la privacidad de la información que puede ser alterado por varias áreas de distintas partes del mundo.

No solo resulta interesante toda esta información para el sector privado. El gobierno siempre ha controlado de alguna forma el Internet. En Estados Unidos de América por

medio de las cookies se controla todo lo que se hace en internet y de esta forma se centraliza la información por “seguridad nacional”. (Dan Schiller ,2014)

Hay personas como Andrew Keen autor de el libro “The internet is not the answer” que establecen que el internet no es tan bueno como pensamos ya que realmente es un medio para controlar la economía y generar un monopolio. Si lo ponemos en contexto, se estaría monopolizando nuestra salud. En parte puede tener razón, tal vez el internet de las cosas no esté totalmente orientado a mejorar la vida de las personas, pero en términos generales todo lo que se desarrolla busca un sustento económico.

Si hay un sustento económico, y claro que lo hay, para el internet de las cosas se pueden desarrollar proyectos como los del estetoscopio y los del diafragma que están orientados a lugares con vulnerabilidad económica y además ayudan a avanzar tecnológicamente en la salud.

Tal vez si se piensa en un objeto que conectaremos a nuestro cuerpo y nos diagnosticará una enfermedad no cause mucha gracia ya que siempre se necesita la empatía de un ser humano pero definitivamente es una forma más accesible de diagnosticar enfermedades y puede tener un gran potencial en zonas de recursos limitados y sin acceso a grandes hospitales además de poder complementar el trabajo de los médicos tradicionales.

Probablemente cada dispositivo conectado no será capaz de defenderse por si solo pero se pueden crear una base central de un sistema para administrarlo y protegerlo. Esto creara un sistema de sistemas lo que facilita el control del internet de las cosas y la seguridad. Se esta implementando que con el tiempo los desarrolladores de productos se

concentren en crear cosas que no sean vulnerables a los 10 ataques más comunes establecidos por la OWASP(Open Web Application Security Project) que adicionalmente se escriban las vulnerabilidades de los equipos en la etiqueta de venta de los mismos.

Como ya se mencionó si se tiene acceso a un dispositivo físicamente o por medio de la red los problemas de seguridad aumentan pero no son imposibles de controlar. Hay empresas de tecnología especializadas específicamente en redes y en seguridad computacional. Una de las más importantes es CISCO que además de concentrarse en su trabajo tienen certificaciones que ayudan a que la población se pueda especializar en seguridad computacional y tienen campañas como blogs donde se proponen soluciones a nivel persona para evitar actos de hacking.

Un caso que podría motivar a las personas es el del sistema operativo Windows XP que solía sufrir de muchos ataques en su época a los cuales Microsoft respondía con parches en el OS. Después de muchas pérdidas económicas y daños por los problemas del sistema Microsoft decidió que debía concentrarse en crear un OS nuevo y no seguir con los parches. Por ello surgió Windows 8 que estaba creado con una visión hacia el futuro y eliminó momentáneamente los problemas de ciberataques. Eventualmente se crearon nuevos virus y nuevas formas de penetrar el sistema, sin embargo este tipo de ataques ayudan a mejorar cada vez la tecnología. Al igual que la seguridad de Windows, se espera que la seguridad del internet de las cosas pueda mejorarse durante el paso de los años.

IoT no es algo que aparecerá de un día para otro pero es algo que inevitablemente surgirá ya que es una gran área de negocio para la industria y si crece en la industria de igual forma crecerá en otros ámbitos como los de la medicina. Probablemente muchas personas solo considerarán los riesgos que implica el internet de las cosas y lo verán como

una molestia. Es importante que la forma de ver esta nueva herramienta cambie ya que se espera que la mayoría de las empresas y la mayor parte del sector de la industria lo implemente en los próximos años.

La tecnología continuará con la ley de Moore y como esta lo establece se reducirá el tamaño de los procesadores y se mejorará la capacidad lo que llevará a que los precios sigan reduciéndose. Los sensores y los procesos necesarios para el avance tecnológico cada vez serán más económicos lo que facilitará la implementación del internet de las cosas en todo. Conforme avanza el tiempo los millennials crecerán e ingresarán cada vez más al ámbito de la industria de todo tipo lo que llevará a que la tecnología avance con ellos y se cambie drásticamente la forma en la que se manejan muchísimos sectores.

Es bien sabido que la tecnología genera grandes empresas y que ha cambiado la economía desde siempre y que con la invención de las computadoras este cambio es aún más notable. El internet de las cosas se está implementando por medio de los dispositivos móviles, específicamente los smartphones. Aunque uno de los cambios próximos que se esperan es que los werables sustituyan a los dispositivos móviles como los celulares sustituyeron al teléfono fijo en algún punto. Pero no solo existe el surgimiento de los wearables para sustituir a las tecnologías actuales, de igual forma se desarrollan tipos de conexión como Ipv6, zigbee y thread. Es decir la tecnología avanza hacia el IoT.

Será necesario reforzar la protección de los entornos cifrando datos, pidiendo mayor autenticación por parte de los usuarios y generando código más resistente y mejor preparado para grandes intentos de ataque. Se deberá pensar como un hacker y serlo, pero siempre considerando la ética para defender la integridad de las personas.

> Los ingenieros, más que todos los demás hombres, guiarán hacia delante a la humanidad […]. Sobre los ingenieros […] descansa una responsabilidad que los hombres nunca antes habían tenido que afrentar.(Akin 1977, 8)

Esto son retos especialmente para las personas de áreas de tecnología quienes diariamente se verán enfrentados a nuevas problemáticas y nuevas formas de manejar la información.

Pero no todo queda en manos de los desarrolladores de software, hardware y los especialistas en seguridad computacional. Es importante que el usuario aprenda a manejar el internet de las cosas implementando hábitos en su vida no tan complicados. Por ejemplo se deben crear contraseñas no predecibles y mantener cosas que no necesitan estar en la red fuera de ella mientras se mejora la seguridad.

Por último sería interesante preguntarnos ¿De qué otras forma podremos usar el Internet de las cosas para mejorar la salud y de esta forma mejorar la economía mundial?

Referencias:

Covadonga Fernández. (2015). Hacker Culture and Innovation: How to Make everything Easier. 25 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/en/hacker-culture-and-innovation-how-to-make-everything-easier/

Justin Montgomery. (2016). ImagineCare: A population health strategy. 25 febrero 2016, de Microsoft Sitio web: http://enterprise.microsoft.com/en-us/industries/health/imaginecare-a-population-health-strategy/

Francisco Doménech. (2015). What can a Smartwatch do for your Health?. 25 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/en/what-can-a-smartwatch-do-for-your-health/

Ahmed Banafa. (2016). Securing the Internet of Things (IoT). 22 febreo 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/en/securing-the-internet-of-things-iot/

Ángel Luis Sucasas. (2015). Tecnología inalámbrica para vencer la parálisis. 22 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/tecnologia-inalambrica-para-vencer-la-paralisis/

Ainhoa Iriberri. (2014). Tecnología para arrinconar al ébola. 22 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/tecnologia-para-arrinconar-al-ebola/

Rafael Pinilla. (2014). La comunicación médico-paciente a través de Internet. 22 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/la-comunicacion-medico-paciente-a-traves-de-internet/

Javier Barbuzano. (2015). A Smart Stethoscope you can Connect to a Mobile Phone to Diagnose Lung Diseases. 22 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/en/a-smart-stethoscope-connects-to-a-mobile-phone-to-diagnose-lung-diseases/

Larry Rand. (2011). Smart Diaphragm. 22 febrero 2016, de vodafone Sitio web: http://vodafone-us.com//wireless-innovation-project/past-competitions/2011/2011-winners/smart-diaphragm/

Dr. Daniel Fletcher, Dr. Erik Douglas, Dr. Wilbur Lam, Neil Switz, Robi Maamari, David Breslauer. (2009). CellScope. 22 febrero 2016, de vodafone Sitio web: http://vodafone-us.com/wireless-innovation-project/past-competitions/2009/2009-winners/cellscope/

Dan Schiller. (2014). El opaco control de EEUU sobre la red. 22 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/el-opaco-control-de-eeuu-sobre-la-red/

Ahmed Banafa. (2015). Internet de las cosas: Seguridad, privacidad y protección. 22 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/internet-de-las-cosas-seguridad-privacidad-y-proteccion/

Ahmed Banafa. (2015). Internet of Things: Opportunities and Challenges. 22 febrero 2016, de OpenMind Sitio web: https://www.bbvaopenmind.com/en/internet-of-things-opportunities-and-challenges/