Internet de las cosas

¿Alguna vez ha pensado en conectar un refrigerador, la estufa, el calentador, la iluminación o el aspersor a Internet? Evidentemente suena más que una locura, como una inversión poco práctica e innecesaria. Si lo vemos desde un punto de vista simplón, lo es; sin embargo, desde hace algunos años investigadores y empresas se han dado a la tarea de interconectar todo aquello que esté a disposición del ser humano. A esto le han llamado "Internet de las cosas" (Internet of Things o IoT). El objetivo de IoT es lograr que todo artefacto, mediante el uso de sensores y red de datos, pueda conectarse en cualquier momento y lugar con otro dispositivo o persona, todo ello para mantener un monitoreo y control total de los procesos que cada uno de estos artefactos realice.

La forma más sencilla de entender este concepto es en la industria. Por ejemplo, Rockwell Automation, empresa dedicada a la automatización de procesos industriales en colaboración con Microsoft, ha instrumentado un sistema basado en IoT para monitorear todos los elementos clave que forman parte de la extracción, el transporte, la refinación y la venta de gasolina. En cada punto de la cadena de suministro, existen dispositivos con sensores que continuamente están transfiriendo datos a través de la nube; una vez recibidos, son almacenados y procesados mediante un *software* especial para la mejor toma de decisiones. Cualquier falla que pudiese ocurrir en alguno de los puntos es inmediatamente detectada y corregida, lo cual evita al máximo retrasos o errores que a la larga terminarían afectando al consumidor final.

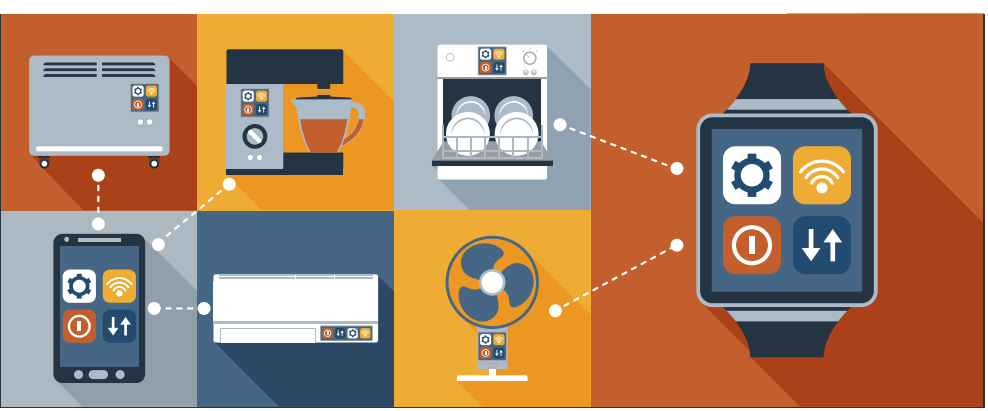
Otro ejemplo es DHL, dedicada a brindar servicios de mensajería y paquetería a nivel internacional. A cada paquete enviado se asigna una etiqueta denominada RFID (Radio Frequency Identification), que realiza una función similar a un código de barras, pero con beneficios adicionales, como poder leer la información del paquete sin necesidad de colocar un lector frente a él, registrar cientos de productos con una sola lectura, tener mayor capacidad de almacenamiento traducida a mayor información sobre el tipo de paquete que se está transportando, entre otros. El uso de esta tecnología en conjunto con IoT está permitiendo a DHL crear sus contenedores inteligentes (*intelligent boxes*). Mediante el uso de sensores basados en RFID, es factible medir las condiciones en que los paquetes son transportados (altas o bajas temperaturas, humedad, movimientos bruscos, etc.). Como es de esperarse, con ello se pueden abrir oportunidades interesantes para las industrias alimenticia, farmacéutica, agraria, etcétera.

Para el usuario común, IoT depara varias sorpresas. Aunque la interconexión de dispositivos a través de una red de datos para monitoreo de ciertos procesos en una casa habitación o edificio es un concepto relativamente antiguo (se inició en la década de los 70 y se denominó domótica), hoy en día se pretende llevarlo un paso más allá. Supongamos que un día se levanta por la mañana, digamos a las 6, auxiliado por una alarma de un radio-reloj que a su vez emite una señal al calentador para encenderlo y mantenerlo a una temperatura previamente programada, y evitar el consumo innecesario de gas. Una vez que termina, un mensaje enviado a su *smartphone* le sugiere vestir con ropa ligera pues ha recibido una señal de los sensores de temperatura externos que han cruzado información con el servicio meteorológico, indicando que

habrá cielo despejado y calor durante el día. Paralelamente, se ha encendido la cafetera, que vierte cierta cantidad de café y lo mezcla con determinada cantidad de azúcar para que justo a las 6:45 esté listo para degustarlo. Asimismo, el horno de microondas se enciende cuando usted llega a la cocina, al tiempo que el refrigerador envía un mensaje alertando que hacen falta queso, leche y huevo, sugiriendo preparar cierto tipo de alimentos con base en los ingredientes que se encuentran en él o en la alacena, combinando esta información con el tipo de dieta que usted debe consumir. Al salir de la casa, se activa automáticamente el sistema de alarma, se apagan las luces y los aspersores se encienden siempre y cuando reciban información de que no lloverá.

Aunque todo lo anterior es una realidad que promete traer innumerables ventajas para el usuario, lo cierto es que deben satisfacerse ciertos requisitos de seguridad que aún no han sido resueltos. Por ejemplo, al interconectar dispositivos como la televisión, la lavadora o la tubería de agua, se convierten automáticamente en vectores de ataque para los *hackers* y más aún si los datos que viajan a través de los sistemas de comunicación no están debidamente encriptados, los cuales también son medios de acceso a información personal y altamente confidencial. ¿Qué sucedería si un *malware* ingresara a uno de los dispositivos de control de seguridad del inmueble y desactivara todos los accesos, enviando además mensajes erróneos a los electrodomésticos conectados a la red? En este sentido, es fundamental que los fabricantes de *hardware*, que darán vida en la nube a nuestros aparatos o todo aquello que interconectemos, estén conscientes de las amenazas existentes y tomen medidas preventivas que minimicen la intrusión de estos sistemas.

Es muy claro que nuestra dependencia de las tecnologías de la información es inevitable y va mucho más rápido que la habilidad para protegerla, razón por la cual debemos ser precavidos y actuar con mucha cautela al implementarla en nuestra vida cotidiana.



REFERENCIAS

- Discover Logistics. (2007). Radio frequency identification, DHL logbook en cooperación con Technical University Darmstadt. Tomado de https://www.dhl-discoverlogistics.com/cms/en/course/technologies/connection/rfid.jsp
- Evans, D. (2011). Internet de las cosas. Cómo la próxima evolución de internet lo cambia todo, CISCO Internet Business Solutions Group. Tomado de http://www.cisco.com/web/LA/soluciones/executive/assets/pdf/internet-of-things-iot-ibsg.pdf
- Microsoft. (2014). Moving from insight to action with Azure IoT services. Tomado de http://www.microsoft.com/en-us/server-cloud/customer-stories/rockwell-automation.aspx
- Vermesan, O. (2013). Internet of things – converging technologies for smart environments and integrated ecosystems, River Publishers. Tomado de http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf.

LINKS DE INTERÉS:

- http://siliconangle.com/blog/2013/06/04/2013-the-year-of-the-internet-of-things/
- http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf
- http://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&sqi=2&ved=0CFAQFjAE&url=http%3A%2F%2Fec.europa.eu%2Finformation_society%2Fnewsroom%2Fcf%2Fdae%2Fdocument.cfm%3Fdoc_id%3D1753&ei=EVITVZP-H4KeyATftYHwCQ&usg=AFQjCNHoRL11Ce0INElpI0SALOzVlFHcwQ&bvm=bv.89217033,d.aWw
- http://www.forbes.com/sites/symantec/2015/01/30/how-to-secure-your-personal-data-in-the-internet-of-things/
- http://www.informationweek.com.mx/analysis/hay-riesgos-de-seguridad-en-el-iot-hp/