Sobre internet de las cosas

Guillermo Andrés Musso Rodríguez
http://linkedin.com/in/guillermo-andrés-musso-rodríguez-42216423

Acerca del autor
Guillermo Andrés Musso Rodríguez es ingeniero electrónico de la UBA, y se desempeña como arquitecto de tecnología y arquitectura de redes y servicios en Telecom, en donde trabaja desde 2010. Además, es docente en la UBA desde 2007, a cargo de asignaturas de grado en las carreras de Ingeniería Electrónica y Electricista, además de dictar asignaturas en la carrera de Especialización en Automatización Industrial.

Para agendar

Para más información sobre Internet de las cosas (IoT), el autor de este artículo junto con su colega Marcelo Javier Segura, dictarán en AADECA el curso "Introducción a IoT e IIoT" entre el 5 de octubre y el 9 de noviembre.
https://aadeca.org/index.php/producto/introduccion-a-iot-e-iiot-5-12-19-26-10-2-9-11/

Internet of Things (IoT) o en español, "Internet de las cosas", es un concepto tecnológico que comenzó a impactar e impactará cultural-, técnica- y económicamente en nuestra sociedad con un efecto transformador.

Desde hace tiempo, existen soluciones de automatización y control. Ya en 1970 se comenzó a utilizar dispositivos para el monitoreo de la distribución eléctrica de centrales, usando líneas telefónicas. A partir de ahí se comenzaron a implementar distintas soluciones de telemetría, monitoreo, automatización y control (mayoritariamente implementadas en la industria manufacturera, la industria de producción de petróleo y la industria automotriz con SCADA) que evolucionaron a finales de los '90 con la llegada de *Machine to Machine* (M2M).

En el mundo actual, Internet de las cosas es un pilar fundamental para la cuarta revolución industrial que generará una gran transformación llamada "Industria 4.0".

Las áreas potenciales para el desarrollo de IoT (donde el ámbito gubernamental posee gran injerencia) son salud, transporte público, ciudades inteligentes (*smart cities*), educación, medioambiente, agricultura y ganadería, seguridad, defensa y/o uso militar, procesos industriales, generación, transporte y distribución de energía.

Cada cosa es identificable de forma única a través de su sistema informático y electrónico integrado, y es capaz de interoperar dentro de la infraestructura de Internet existente.

Definiendo IoT...

En términos generales, IoT se puede considerar como una red conformada por los siguientes elementos:

- Sensores, para generar información
- Identificadores, para identificar la fuente de datos (por ejemplo, sensores, dispositivos)
- Software, para colectar, analizar y procesar datos
- Conectividad, para comunicarse y notificar

En su conjunto, IoT es el internet de las cosas, con una clara identificación de elementos físicos integrados con inteligencia de software, sensores y conectividad.

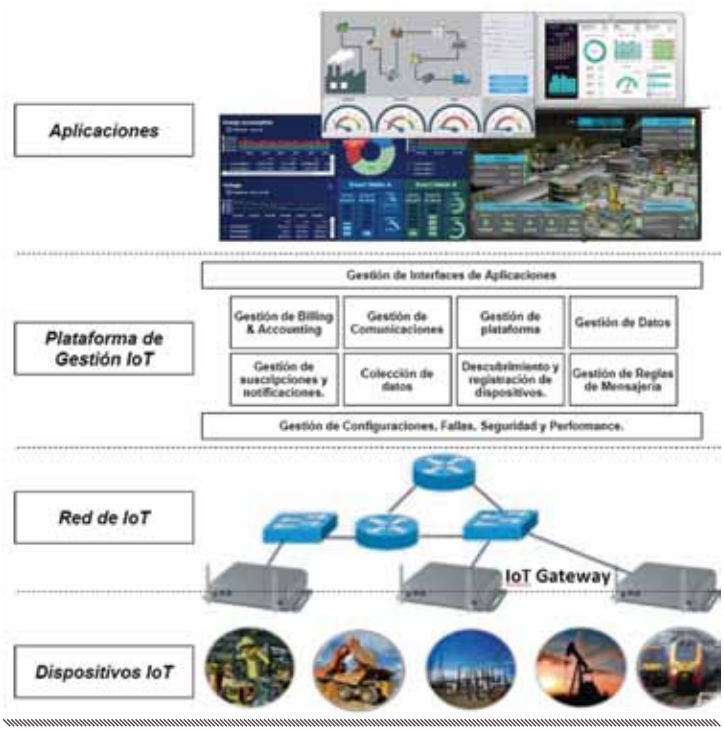
El IoT permite que cosas u objetos intercambien información con el fabricante, operador y/u otros dispositivos conectados que utilizan Internet. Posibilita que los objetos físicos sean detectados (para proporcionar información específica) y controlados de forma remota a través de Internet, creando así oportunidades para una integración más directa entre el mundo físico y los sistemas de cómputo, resultando en una mayor eficiencia, precisión y beneficio económico.

Cada cosa es identificable de forma única a través de su sistema informático y electrónico integrado, y es capaz de interoperar dentro de la infraestructura de Internet existente.

El principio de IoT es conectar físicamente cualquier cosa (por ejemplo, sensores, dispositivos, máquinas, personas, animales, árboles, plantas) y cualquier proceso a través de Internet para permitir funcionalidades de seguimiento y/o control. Las conexiones no se limitan a la información de los sitios, son conexiones reales y físicas que permiten a los usuarios llegar a las cosas y tomar el control cuando sea necesario. Por lo tanto, conectar objetos entre sí no es un objetivo por sí mismo, pero sí lo es el hecho de que recolectando la información generada por las cosas, y mediante inteligencia, se puedan enriquecer productos y servicios.

En términos generales, cualquier persona o cualquier máquina puede realizar el monitoreo y control de los servicios de IoT. Imaginemos como caso un ejemplo cotidiano: una persona monitorea su propiedad a través de un dispositivo móvil que se integra al sistema de seguridad autoinstalado y configurado, desde donde también puede controlar las luces, encender el aire acondicionado, apagar el calentador, etc. Otro ejemplo es el de un proveedor de servicios para monitorear y controlar servicios para sus clientes en un centro de operaciones de red (NOC, por las siglas en inglés de *Network Operation Center*).

La seguridad es una preocupación importante para evitar el acceso de personas no autorizadas, como también de dispositivos que tengan como objetivo atacar un servicio IoT.



Seguridad de dispositivos y de datos: un punto a tener en cuenta

Obviamente, la seguridad es una preocupación importante para evitar el acceso de personas no autorizadas, como también de dispositivos que tengan como objetivo atacar un servicio IoT. Se debe evitar accesos malintencionados a los sistemas y a las redes.

Las áreas de control son mucho más críticas para las aplicaciones sensibles a las compañías como, por ejemplo, el monitoreo de procesos industriales, pacientes médicos y aplicaciones bancarias.

Los datos generados por los dispositivos serán transportados por redes de IoT en todo momento, por ejemplo, desde sensores hasta el gateway y desde el gateway a los centros de cómputos de datos o también sensores. También existirá el caso del sentido contrario, desde el sistema de computación hacia los actuadores. Dado que en IoT se colectan datos producidos por los dispositivos, durante el transporte (seguridad de la red y del transporte) estos datos pueden ser interceptados por un dispositivo atacante que se interponga en el medio de la comunicación (comúnmente conocido como *man in the middle* —hombre en el medio—) a menos que los protocolos de transporte sean completamente seguros y estén cifrados.

En toda solución IoT, se pueden identificar cuatro capas que sí o sí estarán presentes: dispositivos IoT, red IoT, plataforma de servicios de IoT y aplicaciones IoT.

IoT: un modelo de referencia

En toda solución IoT, se pueden identificar cuatro capas que sí o sí estarán presentes: dispositivos IoT (cosas), red IoT (infraestructura que transporta los datos), plataforma de servicios de IoT (software que conecta las cosas con las aplicaciones y proporciona administración general) y aplicaciones IoT (especializadas, basadas en negocios, y aplicaciones tales como gestión de relaciones con el cliente —CRM—, contabilidad y facturación y aplicaciones de *Business Intelligence* —BI, 'inteligencia en los negocios'—). El control se transmite desde un nivel al siguiente, comenzando en el nivel de aplicación (o en la generación de datos y su correspondiente procesamiento), y procediendo a los dispositivos de IoT para nivelar y respaldar la jerarquía.