IoT, un universo de posibilidades por desarrollar

No se trata de decidir a estas alturas si IoT, Internet de las Cosas, es un fenómeno de presente o de futuro, sino del ritmo al que se va a consolidar en nuestras vidas, porque ya son muchos los proyectos puestos en marcha, pero, en realidad, son una parte minúscula de los que pueden llegar a ser, porque ¿quién sabe cuál va a ser el desarrollo de esta tendencia?

MESA REDONDA IT

Para hablar de IoT, de presente y, sobre todo, de futuro, contamos con la presencia en esta Mesa Redonda IT de Ángel Arias, responsable de Preventa de Aerohive; Antonio Navarro, country manager de D-Link; Ramón Cano, director de servicios gestionados de Equinix; Juan Rodríguez, country manager de F5 Networks; Galo Montes, director de preventa de HPE; y Aitor Lejarzegi, responsable de IoT Industrial en Sarenet. Y la primera pregunta que quisimos trasladarles fue qué es IoT. Tal y como explicaba Ángel Arias, "el primer dispositivo conectado data de mediados del siglo XIX, y en su día Nicola Tesla ya predijo que todo estaría controlado por un gran cerebro central, que hoy en día es Internet. Pero la verdadera explosión de IoT vino con las comunicaciones inalámbricas, cuando pudimos conectar múltiples dispositivos a la red. En resumen, IoT no es otra cosa que la digitalización de nuestro mundo analógico".

Por su parte, Antonio Navarro comenta que "estamos en un punto de entrada a una nueva realidad que nos va a cambiar radicalmente. IoT podemos dividirlo en múltiples microsegmentos. En nuestro caso, cámaras de videovigilancia a las que se han unido sensores para crear un entorno domótico para el hogar, creando reglas y obteniendo datos. Por otro lado, tenemos la versión industrial. Y no podemos olvidar que, según Gartner, el año próximo habrá 20.000 millones de dispositivos conectados, y que otras fuentes cifran en 1 millón de dispositivos los que se sumarán al día a esta gran red".

Refuerza esta idea Ángel Arias aportando otro dato: "en 2022 habrá 30.000 millones de dispositivos conectados y en cada hogar habrá 20 dispositivos conectados", lo que nos deja, añade Antonio Navarro, que, "quizá, hay más dispositivos conectados en un hogar que en una PYME".

En palabras de Ramón Cano, "hay que entender IoT como un ecosistema, no un elemento aislado. Colaborarán los fabricantes de sensores, de redes de infraestructura, los fabricantes de procesamiento en el extremo o en el centro de datos, la interconexión de los diferentes partners... por eso nosotros apostamos por una única plataforma de interconexión de las diferentes figuras".

Tal y como nos explica Juan Rodríguez, "IoT es la interconexión de diferentes tipos de dispositivos y la transmisión masiva de datos. Es cier-

NUEVAS TENDENCIAS EN TORNO A IOT A DEBATE

“IoT es la digitalización de nuestro mundo analógico”

ÁNGEL ARIAS, RESPONSABLE DE PREVENTA DE AEROHIVE

Clica en la imagen para ver la galería completa

to que habrá 20.000 millones de dispositivos el año próximo, pero la mayor brecha de seguridad de este año ha estado en los thinbot. IoT no sólo está cambiando la sociedad, sino que está acarreando una serie de problemas, porque muchos dispositivos no tienen ningún elemento de seguridad. A modo de ejemplo, un gran casino de Las Vegas tuvo una brecha en el CPD por el sensor de temperatura de una pecera. El crecimiento es imparable, pero no se pueden obviar los problemas”.

Señala Galo Montes que en HPE ven IoT “como personas, lugares y cosas que se interrelacionan y se ponen en contexto. Todo ello genera información que, cada día, es más demandada por las empresas, una demanda que cada vez es mayor, lo que lleva a plantearse cómo extraer la información y cómo procesarla de forma rápida y con la mayor agilidad. Vemos una explosión de dispositivos en el extremo para procesar la información en los centros de datos o en la nube. Las consultoras estiman que el 10% de datos que se generan ahora en el extremo se convertirán en un 50% en cuatro años, lo que provocará que no se pueda procesar todo en los CPD y tengamos que procesarlo en el extremo. Vemos, por tanto, una gran oportunidad, donde hay que aplicar la seguridad, nuevos algoritmos y nuevos procedimientos para que la información pueda fluir por todo el ecosistema”.

“Se va a generar tanta información, la imagen va a ser crítica”, continúa, “que no va a ser posible almacenarla ni transportarla, y va a tener que procesarse en el extremo para extraer valor para las empresas”.

INDUSTRIAL IOT O INTERNET DE LAS COSAS INDUSTRIAL

Finaliza esta primera ronda de opiniones Aitor Lejarzegi, que comenta que “estamos en una evolución digital que necesita que se controlen los riesgos, sobre todo en el entorno industrial. Estas nuevas formas de conectar negocio, procesos, seguridad... va a generar una nueva cultura digital que hay que integrar en la sociedad. En el entorno productivo la progresión va a ser más lenta, porque muchos de los dispositivos conectados no están pensados para integrarse con internet. Por eso creo que hay que ayudar a la industria”.

No podemos olvidar, matiza Ángel Arias, que “el entorno industrial no es como el del consumo, donde un dispositivo nos dura dos o tres años”, a lo que añade Lejarzegi que en la industria “conviven dispositivos de diferentes ‘edades’, por lo que lo primero es ordenar para, posteriormente, interactuar. Hablamos de compartimentar y crear segmentos de red para que, si existe una brecha, no impacte en toda la empresa”.

Se muestra de acuerdo Galo Montes quien, por otra parte, discre-

pa en la velocidad “de la necesidad de aplicarla a la industria. La seguridad es crucial, pero si no evolucionas rápidamente, te come el mercado”.

En el entorno industrial, señala Juan Rodríguez, “los departamentos de OT e IT no dialogan, están totalmente separados. Muchas veces las personas de operaciones tienen sus propios protocolos de seguridad y sus procedimientos, pero el mundo ha cambiado, y es necesario que cambien también tus relaciones y tus comunicaciones”.

Apunta Galo Montes que la “seguridad es imprescindible, pero la agilidad es fundamental para la supervivencia de la empresa”, algo que comparte Ramón Cano, que indica que el que sufre la presión es el CEO, porque “u optimiza sus procesos a partir del análisis de la información que recibe de todos los sensores con los que cuenta la empresa, o la compañía no va a sobrevivir”.

Si hablamos de IoT Industrial, señala Aitor Lejarzegi, “hablamos de una rama de IoT con sensores conectados a máquinas para ofrecer información para mejorar los procesos, la calidad de los productos, proporcionar ahorros por la gestión de elementos defectuosos, ofrecer mayor agilidad en la toma de decisiones, mayor seguridad de todo el negocio... y eso se hace con conectividad que antes no existía y que nos puede proporcionar grandes beneficios”.

Hay un riesgo importante, afirma Ángel Arias, “porque un fallo en un proceso industrial puede

> “Estamos en un punto de entrada a una nueva realidad que nos va a cambiar radicalmente”
>
> ANTONIO NAVARRO, COUNTRY MANAGER DE D-LINK

Clica en la imagen para ver la galería completa

tener consecuencias importantes”, algo que recalca Juan Rodríguez cuando comenta que “un fabricante de coches vio como un fallo en uno de sus dispositivos cambió el grado de curvatura de una puerta, lo que impedía el correcto cerrado de la misma. Hablamos de casi un millar de puertas fabricadas antes de detectar el problema. El coste de parar una cadena de producción es incalculable”.

Aunque, como aporta Aitor Lejarzegi, “no todas las soluciones en este sentido pasan por internet. Puedes trabajar con un entorno controlado en una nube privada”. De hecho, apunta Ramón Cano, “hay informes que señalan que la conectividad privada en entornos industriales va a multiplicar por diez el crecimiento del propio tráfico en Internet en estos entornos”, o, incluso, soluciones, como añade Juan Rodríguez, que “mezclan nubes privadas, para unas funciones, y conectividad a la nube pública, para otras”.

Podemos hablar de clouds privadas y cloud pública, pero, al final, tal y como recalca Galo Montes, “el mundo es mixto. No puedes depender sólo de uno u otro, debes tener ambas opciones y repartir los diferentes procesos en función de las necesidades o su criticidad”.

En cualquier caso, se suma a esta idea Ramón Cano, “no debes renunciar a la cercanía para tratar un dato de un proceso local, pero tampoco a la flexibilidad de las plataformas como

“Hay que entender IoT como un ecosistema, no un elemento aislado”

RAMÓN CANO, DIRECTOR DE SERVICIOS GESTIONADOS DE EQUINIX

Clica en la imagen para ver la galería completa

servicio que ofrecen los proveedores de nube pública”.

¿CÓMO SE PROCESAN LOS DATOS?

Es importante preguntarse cómo se procesan los datos. Tal y como explica Galo Montes, “nosotros cogemos los datos y es importante saber cómo procesas el dato y cómo lo guardas. Por un lado, podemos enviar el dato a procesos tipo batch, y aprovechar el dato resultante que nos puede llegar en horas, días… pero, por otra parte, está el procesamiento en tiempo real, algo que no debe depender del retraso de milésimas por trasladar el dato desde un servidor u otro. Necesitamos arquitecturas que nos permitan decidir, de forma dinámica, cómo procesamos cada dato. No hay una única solución, debe ser una solución mixta, y es algo que nos encontramos en empresas que ya tienen desarrollados sus proyectos IoT”.

Para esto es muy importante la red sobre la que mover el dato, recalca Juan Rodríguez, “y el tipo de dispositivo, porque no es lo mismo un sensor industrial que tiene que emitir datos masivos, como también un coche conectado, o un reloj inteligente que transmite pocos datos. La necesidad de transmisión es importante, y de ahí que existan diferentes niveles”.

Sin olvidar el almacenamiento de los datos, donde un modelo capex es, a la larga, más rentable que su consumo en cloud, apunta Galo Montes, “si bien es menos flexible. Por eso todos los fabricantes hemos cambiado y ofrecemos soluciones como servicio con buffers de crecimiento gratuitos. El usuario consume lo que necesita y paga por ello, y los proveedores se lo renovamos cada cierto tiempo evitando que el usuario tenga todas esas transiciones. Es un modelo de consumo impulsado por el cloud”.

SECURIZAR PROYECTOS IOT

La securización de los proyectos de IoT debe tener en cuenta varios puntos, como comenta Ramón Cano, “debe securizarse la conexión del sensor, con cifrado de comunicaciones, por ejemplo; además, hay que proteger el almacenamiento y el proceso en el extremo; la conectividad entre los diferentes elementos del ecosistema…”.

El problema surge, y así nos lo explica Antonio Navarro, “por la complejidad de no hablar de una solución base, sino de una solución con innumerables capas de muchos fabricantes diferentes que todavía están viendo cómo interactuar. Todos los beneficios de IoT tienen una contrapartida, la necesidad de seguridad, que tendrá que encontrar un estándar. Dentro del consumo, por ejemplo, IoT está teniendo brechas de seguridad que

no conocíamos, como es el caso de los primeros problemas detectados en los asistentes de voz. Qué puedes hacer si el problema surge en el que se supone es el gran motor de desarrollo del IoT doméstico".

Para los dispositivos IoT, comenta Ángel Arias, "no podemos olvidar que la principal capa de acceso es la capa inalámbrica, y hay que ver cómo securizarla. No podemos instalar certificados 802.1X para todos los dispositivos, con lo que tendremos que buscar otro sistema de autenticación robustos. En todo caso, la seguridad es algo imprescindible y crítico en IoT".

Volviendo a la industria, señala Aitor Lejarzegi, "si vamos a conectar un dispositivo que está junto a una máquina, utilicemos gateways que tengan unos requisitos mínimos, no cualquiera, y segmentemos la red para aislar los posibles problemas. Porque, por ejemplo, un lector de códigos de barras en un smartphone para enviar información al software de gestión empresarial, si no cuenta con la securización adecuada en el dispositivo, puede acabar provocando una brecha de seguridad extremadamente grave en la compañía".

Hay otro elemento donde la seguridad es fundamental en IoT, apunta Antonio Navarro, "como son los mantenimientos predictivos. El control humano pasa a ser secundario, con lo que una brecha de seguridad puede descubrirse transcurrido más tiempo y la respuesta es más lenta de lo necesario".

"Los fabricantes llevamos años apostando por la seguridad predictiva. La clave está en trasladar esta predictibilidad a IoT"

JUAN RODRÍGUEZ, COUNTRY MANAGER DE F5 NETWORKS

Clica en la imagen para ver la galería completa

Tal es la importancia de la seguridad, indica Galo Montes, que este año "vamos a invertir 4.000 millones en dispositivos del extremo, gateways para el mundo del OT y el IT, y vamos a securizarlos de forma robusta. Tenemos que colaborar para que la seguridad tradicional del mundo IT se traslade al mundo OT. Creemos que es importante asegurar el Gateway y proteger las comunicaciones, monitorizando que el perfil o el comportamiento del Gateway no cambie con el tiempo y podamos detectar, de forma inmediata, cualquier cambio".

Además, continúa, "tenemos que asegurar la integridad del dato para que no sea modificado. Esto nos obligará a crear una complejidad extra sobre las tecnologías actuales para proteger información, que es crítica. Pero, además, dada la complejidad del ecosistema, necesitaremos sistemas más o menos grandes para detectar en milésimas de segundo cualquier anomalía en cualquier parte. Poder tomar decisiones antes de que se produzcan problemas mayores".

En este sentido, Juan Rodríguez destaca que "los fabricantes llevamos años apostando por la seguridad predictiva. La clave está en cómo trasladar esta predictibilidad al mundo IoT. En la parte de consumo, poco podemos hacer, porque es labor de la operadora, mientras que en el entorno industrial sí que podemos hacer algo más, como lo hemos hecho en los entor-

nos tradicionales. Con todo, es necesario que la infraestructura de red cambie, y en eso 5G nos va a ayudar mucho, si bien no va a ser imprescindible para todos los entornos".

La seguridad en IoT va a ser similar a la de cualquier entorno, continúa, "y hay que aplicar seguridad como en cualquier otro entorno, teniendo en cuenta las amenazas interiores y las exteriores".

INTELIGENCIA EN IOT

Si algo está conectado con todos los elementos mencionados hasta ahora es la IA y el Machine Learning. En palabras de Ángel Arias, "hay que ser capaces de, a partir de la información almacenada, procesar estos datos y promover acciones predictivas y proactivas. Si somos capaces de predecir o detectar el problema y corregirlo, esto es IA. Y por ahí va el camino de IoT".

> "Vemos IoT como personas, lugares y cosas que se interrelacionan y se ponen en contexto"
>
> GALO MONTES, DIRECTOR DE PREVENTA DE HPE

Clica en la imagen para ver la galería completa

PERO... ¿Y EL NEGOCIO?

En palabras de Ramón Cano, "IoT es ya una realidad en Industria y en verticales como Retail y Distribución, para trazabilidad y envíos de mercancías. Hay mucho interés en vehículo conectado, pero queda mucho todavía", a lo que se añaden otros tales como Sanidad. De hecho, Antonio Navarro comenta que cuando esté implantado 5G "se podrán realizar operaciones robóticas desde otro continente, dada la baja latencia".

También, recuerda Juan Rodríguez, "está avanzado en el sector de las Utilities, para controlar los dispositivos en la casa del cliente; en Agricultura, para controlar los niveles de regadía, por ejemplo; o el Transporte, para gestión de vehículos".

Desde HPE, apunta Montes, "creemos que el desarrollo potencial es brutal. De hecho, casi el 30% de los proyectos son en esta área. Vemos también con mucha fuerza Transporte y Distribución. Pero la Industria, que tira en otros países, se está quedando un poco por detrás".

Por último, señala Ángel Arias, "no podemos olvidar el consumo, porque el éxito de IoT en la empresa viene provocado por el anterior éxito en consumo".

De todas formas, estamos en una transición, recuerda Ramón Cano, "y hasta dentro de dos o tres años no veremos grandes inversiones en infraestructura para soportar proyectos IoT".

Es cierto que ya hay casos de éxito, reconoce Juan Rodríguez, "y vemos un gran potencial de facturación también por la parte de seguridad, si bien la explosión llegará en 2020", aunque dependerá, en opinión de Ángel Arias, "del vertical en el que te muevas. Y, además, dependerá del interlocutor, que en el caso de

“Estamos en una evolución digital que necesita que se controlen los riesgos, sobre todo en el entorno industrial”

AITOR LEJARZEGI, RESPONSABLE DE IOT INDUSTRIAL EN SARENET

Clica en la imagen para ver la galería completa

IoT, en las empresas, no debe ser solo IT, sino, por ejemplo, el CMO y los departamentos de Transformación Digital o Innovación, con lo que el éxito dependerá mucho de que seamos capaces de convencer a estos responsables”.

Al final, comenta Aitor Lejarzegi, “este tipo de proyectos abre la puerta a otras transformaciones en la empresa, con lo que los datos de 2018 se mejorarán en 2019”.

Para Galo Montes, “nosotros lo estamos viendo ya como algo tangible desde hace dos años, aunque ahora se está incrementando mucho. Pero, en nuestro caso, estamos presentes en muchos elementos del ecosistema, de ahí que estemos viendo resultados y crecimientos importantes”.

Finaliza Antonio Navarro recordando que la PYME “es una de las cartas a jugar como acelerador. Si conseguimos mostrarle los beneficios sin complejidades, va a ser el impulsor real de IoT en nuestro país”. ■

MÁS INFORMACIÓN

Nuevas tendencias en torno a IoT a debate