IoT y cierre

Durante estas navidades he estado pensando el tema que trataría en este post, y finalmente he decidido que tratará del *Internet of Things* (IoT), pero antes de empezar a hablar sobre el tema quiero felicitar las navidades y el año nuevo a todos y esperando que el 2021 nos devuelta a la normalidad que teníamos antes.

El IoT, queramos o no ha ido ganando importancia en nuestro día a día, y esto es debido a la importancia que tiene el internet en la actualidad, especialmente gracias a las redes de telefonía móvil. Estas redes permiten que los dispositivos conectados puedan comunicarse con otros dispositivos, pudiendo enviar información en tiempo real sin ningún tipo de problema. Se dice que el 5G es un gran avance para estos dispositivos. Un ejemplo que se me viene a la cabeza relacionado con el uso de las redes de telefonía y los dispositivos IoT es el sistema que emplean algunas empresas de paquetería. El servicio que ofrecen dichas empresas consiste en indicar al cliente la ubicación en la que se encuentra su pedido en tiempo real.

Otro campo en el que está ganando importancia el IoT es en el *edge computing*. Esto permite a las empresas o emprendedores no necesiten hacer tanto uso de la computación en la nube. Esto es debido a que el procesamiento de la información o parte del procesamiento se realiza en el propio dispositivo IoT.

Aunque parezca que el IoT propone muchas ventajas, también trae consigo inconvenientes. Por dar un ejemplo, poco antes de Navidades Google sufrió una caída en algunos de sus servicios. Entre uno de estos servicios, se encontraban los timbres que vende la propia Google, que al estar sin servicio no sonaban.

Timbre no funciona porque Google está caido. Fuente: https://twitter.com/rubengmrs/status/1338459614967439363/photo/1

Otro inconveniente que veo, está relacionado con la privacidad del usuario, debido a que estos dispositivos pueden ser muy invasivos, puesto que los llevamos con nosotros a diario o tienen micrófonos que no sabemos si están escuchando lo que decimos o no.

Podría seguir hablando sobre lo que ofrece y no ofrece el IoT, entrando más en profundidad, pero creo que nos podemos hacer una idea general sobre el tema. Además, si alguien quisiera más información sobre el IoT para la asignatura de *Auditoría, Certificación y Calidad de Sistemas Informáticos* realicé otros 5 posts relacionados con este mismo tema, entrando en mayor detalle.

Cerrando este último post, quiero decir que me ha gustado la mecánica empleada en la asignatura de *Sistemas de Información*

Empresarial a la hora de realizar los posts debido a que teníamos total libertad a la hora de hablar de cualquier cosa tratada en clase. Por este mismo motivo quiero darle las gracias al profesor P. C. por darnos esta flexibilidad, debido a que a mi personalmente me cuesta mucho escribir sobre temas que no me motivan.

Más riesgos y cierre

Introducción

Durante esta lista de posts he ido hablando sobre diversos temas relacionados con el IoT. En el primero artículo introduje un poco el tema sobre los dispositivos conectados a la red. Durante el segundo hablé de las aplicaciones que tiene esta tecnología en la industria. Los últimos 2 post han sido sobre los riesgos que tienen estos dispositivos y que controles y auditoría necesitan estos dispositivos.

Este último post he decidido dedicarlo a introducir algunos riesgos más, en función del área al que pertenece, puesto que comenté que me parecía un tema interesante en mi post relacionado con los riesgos. Si bien es cierto, que algunos riesgos se repetirán, pienso que es importante categorizarlos.

Riesgos

A continuación, planteo un pequeño esquema que resume los riesgos de cada área y acto seguido explicaré detalladamente cada una de estas [1].

- Área financiera

        - Salud y seguridad
        - Cumplimiento normativo
        - Privacidad del usuario
        - Costos inesperados
    - Área operacional
        - Acceso inadecuado
        - Uso en la sombra
        - Rendimiento
    - Área técnica
        - Vulnerabilidad del dispositivo
        - Actualizaciones del dispositivo
        - Administración del dispositivo

Área financiera

El riesgo más grave que puede ocurrir en esta área es en el impacto en la salud y la seguridad si se modifica el funcionamiento de un dispositivo. Varias investigaciones han demostrado que se pueden realizar ataques a dispositivos biomédicos como un marcapaso o un desfibrilador. A su vez, también se pueden realizar ataques contra los coches, pudiendo deshabilitar el sistema de frenos cuando este está en marcha.

Además, como bien expliqué en mi post relacionado a los riesgos se puede obtener todo tipo de información de los dispositivos IoT. Si bien los dispositivos cuentan con medidas de seguridad como una contraseña, esta es opcional. Esto hace que la US Federal Trade Commision haya demandado algunas empresas por políticas de seguridad pobres.

También, los riesgos regulatorios son posibles, especialmente en los dispositivos embebidos. Los riesgos regulatorios ocurren principalmente cuando se está procesando información sensible, cuando se interactúa con procesos regulados por los gobiernos y por el impacto que tienen en sistemas críticos. Los dispositivos que procesan personales pueden estar tratando con información privada o sensible del usuario, lo cual implica un riesgo a la privacidad del usuario.

Finalmente, los costos inesperados suelen surgir cuando un se cambia un dispositivo no informático por uno que si lo es. Esto es debido a que el dispositivo informático requiera conectividad o soporte adicional para realizar la tarea completa.

Área operacional

Además de los riesgos financieros que implica utilizar un sistema embebido, hay que tener en cuenta otros riesgos. Uno de estos riesgos es contar con una comunicación M2M insegura. Esto hace que personal inapropiado pueda realizar cambios en el dispositivo u obtener telemetría de este.

También, la implementación de dispositivos sin una supervisión centralizada ni una gobernanza adecuada puede ser perjudicial para los dispositivos IoT. Este tipo de implementación se llama Shadow IT. Al no contar con nadie que se encargue de que los dispositivos estén protegidos, esto puede hacer asumir riesgos adicionales a la empresa la empresa.

Riesgos técnicos

Los dispositivos IoT embebidos suelen ser más complejos de configurara que los dispositivos tradicionales, causado por el gran número de dispositivos IoT. Estos dispositivos, al igual que los dispositivos tradicionales pueden ser atacados como bien mencioné en mi post sobre riesgos.

Los ataques realizados contra los dispositivos IoT ofrecen un desafío para los fabricantes, debido a que muchas veces la única manera de corregir la vulnerabilidad es actualizar el hardware.

Finalmente, desde el punto de vista de la administración de estos dispositivos, muchas empresas no están preparadas para poder proporcionar la seguridad necesaria a estos dispositivos. Esto hace que deban considerar cuestiones como

la realización de inventarios, la supervisión de acceso al dispositivo etc. al igual que en los sistemas tradicionales.

Conclusión final

Mientras buscaba información para realizar estos artículos he descubierto un sinfín de características que desconocía sobre los dispositivos IoT. A su vez, como he ido comentando a lo largo de varios artículos, el número de dispositivos IoT ha estado creciendo durante los últimos años y se espera que siga creciendo en los próximos años. Además, creo que esta tecnología está revolucionando todos los sectores de la industria y que va a seguir incluyendo muchas mejoras. Finalmente, me gustaría recordar que estos dispositivos tienen un gran número de riesgos, los cuales creo que irán decreciendo en los próximos años.

Bibliografía

[1] <<Internet of Things: Risk and Value Considerations>>, ISACA, consultado el 20/11/2020, https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpiot

---

Controles y auditoría IoT

En el post anterior comenté algunos riesgos asociados a los dispositivos conectador a la red. Por este motivo, sin cambiar mucho de tema, en este artículo hablaré sobre los controles a tomar en estos dispositivos, así como de los puntos clave que habría que tener en cuenta a la hora de realizar una auditoría.

Antes de empezar a listar los controles, creo que es importante recordar que existen muchos dispositivos IoT diferentes, así como los sistemas de comunicación que emplean estos dispositivos para comunicarse. Esto hace que no sea una tarea fácil crear un estándar.

En este caso, he decidido listar una seria de controles aplicables basados en la NIST 800-53 [1] [2]:

ID	Capa	ID NIST	Nombre del control	Objetivo del control
IoT-1	1	PE-3	Control de acceso físico	El fabricante verifica tanto las autorizaciones de acceso al dispositivo como las autorizaciones de acceso individuales. A su vez, mantiene registros de auditoría sobre el acceso físico y controla el acceso a las diversas áreas del dispositivo. Finalmente, el fabricante es el encargado de cambiar las combinaciones y claves del dispositivo cuando estas sean comprometidas.

ID	Capa	ID NIST	Nombre del control	Objetivo del control
IoT-2	1	SC-8	Transmisión, confidencialidad e integridad	Los dispositivos IoT protegen la confidencialidad e integridad de la información transmitida. Este control se aplica tanto a las redes internas como a las externas.
IoT-3	2	SC-7	Protección de límites	Los dispositivos monitorean y controlan las comunicaciones tanto en el límite externo como en los límites externos claves. Deben tener implementadas subredes para los datos de acceso público y deben conectarse a redes externas únicamente mediante interfaces administradas.
IoT-4	3	IA-3	Identificación y Autentificación del dispositivo	Los dispositivos deben identificar al resto de dispositivos antes de establecer conexión.

ID	Capa	ID NIST	Nombre del control	Objetivo del control
IoT-5	3	SC-15	Dispositivos de computación colaborativa	Los dispositivos únicamente pueden activarse remotamente cuando el fabricante lo permita. También, tienen que indicar el uso a los usuarios presentes en el dispositivo.
IoT-6	4	IA-2	Identificación y autentificación para los usuarios	Los dispositivos deben identifican y autentifican a los usuarios.
IoT-7	4	AC-2	Gestión de cuentas	El fabricante asigna las cuentas de respaldo y funciones comerciales. Además, establece administradores de cuentas y establece grupos y roles. Posibilidad de que el fabricante o el propietario pueda administrar cuentas del dispositivo.
IoT-8	5	CM-7	Funcionalidad mínima	El fabricante configura el dispositivo para realizar únicamente lo esencial. Además, restringe el uso de algunas funciones.

ID	Capa	ID NIST	Nombre del control	Objetivo del control
IoT-9	5	SC-28	Protección de la información en reposo	El dispositivo protege la confidencialidad y la integridad de la información en reposo.
IoT-10	5	PL-2	Plan de seguridad del sistema	El fabricante desarrolla un plan de seguridad consistente con la arquitectura empresarial y define los límites de autorización. También, describe el contexto y el entorno operativo del dispositivo y proporciona una descripción de los requisitos de seguridad. Además, describe los controles de seguridad implementados, junto con el motivo de estos.
IoT-11	6	PM-11	Definición de misión / proceso empresarial	El fabricante define la misión / procesos teniendo en cuenta la seguridad de la información y el riesgo resultante. Además, determina las necesidades de protección de la información que surgen.

ID	Capa	ID NIST	Nombre del control	Objetivo del control
IoT-12	7	PM-1	Plan del programa de seguridad de la información	El fabricante desarrolla y publica un programa de seguridad de la información. A su vez, ofrece una descripción de los requisitos y los controles para cumplir los requisitos.

Controles IoT basado en la NIST 800-53

Tengo que mencionar, que además de los controles, existen frameworks que permiten comprender ideas complejas mediante preguntas simples. Un ejemplo es el framework Zachman. Este framework se muestra en la siguiente imagen [3].

Figure 1—Zachman Framework Contextual Architecture for IoT Security

Questions	IoT Security
Why?	Examples of security breaches, threat modeling
How?	Device configuration and integration, standards, processes
What?	List of components and their relationships
Who?	User, administrator, vendor, industry bodies
Where?	At every layer and component in the architecture
When?	Design, configuration/implementation and operations

Source: H. Patel. Reprinted with permission.

Framework Zachman

A la hora de realizar una auditoría, el IoT no requiere habilidades adicionales que una auditoría TI tradicional. El IoT únicamente necesita un nuevo enfoque que vincule las estrategias con las soluciones IoT. Algunas preguntas que considerar a la hora de auditar IoT serían las siguientes [4]:

- ¿Como está el IoT desplegado en la organización hoy en

día y quién es el propietario o cuáles son sus respectivos componentes?

- ¿Sabemos qué datos se recopilan, almacenan y analizan, y hemos evaluado las posibles implicaciones legales, de seguridad y de privacidad?
- ¿Tenemos planes de contingencia implementados en caso de que nuestros dispositivos de IoT sean hackeadas o modificadas para fines no deseados?

En conclusión, existen un gran número de controles y frameworks para poder auditar correctamente entornos con dispositivos IoT y tener el entorno bajo control. En mi opinión, un gran número de incidencias ocurren por no cumplir con estos controles o no haberse preguntado algunas de las preguntas mostradas a lo largo de este artículo.

[1] <<An IoT Control Audit Methodology>>, ISACA, consultado el 23/11/2020, https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/an-iot-control-audit-methodology

[2] <<Control List>>, Twelve IoT Controls, consultado el 23/11/2020, https://twelveiotcontrols.com/

[3] <<IoT Needs Better Security>>, ISACA, consultado el 23/11/2020, https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/iot-needs-better-security

[4] <<Internal Audit, Risk, Business & Technology ConsultingThe Internet of Things: A Game Changer for IT Audit>>, Knowledge Leader, consultado el 23/11/2020, https://www.knowledgeleader.com/knowledgeleader/resources.nsf/description/HITheInternetofThingsAGameChangerforITAudit/$FILE/HI%20The%20Internet%20of%20Things%20-%20A%20Game%20Changer%20for%20IT%20Audit.pdf

Riesgos del IoT

Como he mencionado en mis entradas previas, el IoT ofrece un gran número de ventajas y comodidades tanto a los individuos como a las empresas. Pero al igual que con la gran mayoría de tecnologías, también hay que tener en cuenta los riesgos que conlleva utilizar dispositivos IoT o cualquier otra tecnología en general. Hay que tener en cuenta, que la mayoría de estos riesgos estarán relacionado con la seguridad.

El primer riesgo del que voy a hablar se encuentra en los fabricantes de dispositivos IoT. Al igual que todas las compañías, las empresas que diseñan dispositivos IoT están orientadas a los beneficios y al tiempo de comercialización. Esto hace que al diseñar un dispositivo pasen por alto algunas consideraciones de seguridad necesarias para el mismo. Esto permite a un atacante acceder a la información del dispositivo con un mínimo esfuerzo. Cabe destacar que esta información puede ser desde transmisiones de video y audio, hasta correos electrónicos y contraseñas. También, estos dispositivos mal diseñados permiten la ejecución de comandos remotos que pueden reprogramar el firmware del dispositivo [1].

El segundo riesgo que lastra el IoT son las *botnets*. Si los dispositivos IoT no tienen las medidas de seguridad apropiadas pueden ser infectadas por distintos tipos de malware. Si bien es cierto que un dispositivo infectado no significa un riesgo, el gran número de dispositivos conectados a internet sin seguridad si lo es. Es importante destacar que los dispositivos IoT son más vulnerables a ser infectados por un fragmento de software malicioso debido a que no reciben actualizaciones de seguridad regularmente [2]. Un gran número de dispositivos IoT es capaz de poner en peligro instalaciones críticas de nuestro día a día, o que suceda algo similar a la

botnet DDoS Mirai de 2016 [3]. Finalmente es necesario destacar que los dispositivos IoT han tenido el segundo porcentaje de infección más alto entre todas las plataformas, siendo de un 32.72% [4].

Otro riesgo que pueden generar los dispositivos conectados a la red es la perdida de privacidad y confidencialidad. Un gran número de terceros pueden utilizar este tipo de dispositivos para invadir la privacidad tanto de individuos como de organizaciones. Es necesario destacar que este grupo de terceros pueden ser los crackers (termino negativo del hacker), los gobiernos o los competidores empresariales. Si consiguen acceder a la información, ya sea de carácter confidencial o general, lo más probable es que esta información se utilice sin el permiso ni el consentimiento del propietario. Un par de ejemplos de esta pérdida de privacidad y confidencialidad serían los siguientes [2]:

- Obtener el control de una cámara de seguridad para conocer los hábitos del objetivo.
- Empezar a obtener datos de varios dispositivos IoT y utilizar los datos recogidos para extorsionar a la compañía o para vendérselos a compañías competidoras en el mercado negro.

El siguiente riesgo que voy a mencionar sobre el IoT es la visibilidad de los dispositivos en internet. El éxito de un ataque a dispositivos IoT está muy relacionado a la visibilidad que el dispositivo tiene en internet. Como he mencionado anteriormente en este artículo, los dispositivos IoT son propensos a estar infectados y empiezan a formar parte de una botnet. Esto es debido a que muchos dispositivos están conectados con direcciones IP públicas, haciendo a dichos dispositivos vulnerables ante prácticamente cualquier ataque. Para reducir la infección, entre otras técnicas se encuentra contar con un traductor de redes (NAT). Emplear esta técnica reduce el número de dispositivos visibles al escanear una red.

Para finalizar este post, me gustaría concluir y resumir un poco todo lo que he mencionado a lo largo de este artículo. La mayoría de los riesgos que tienen los dispositivos conectados a internet, es decir, los dispositivos IoT está relacionado con la seguridad. Estos riesgos no surgen únicamente por el desconocimiento de los usuarios finales. Los fabricantes muchas veces tampoco dan lo mejor de si para que estos dispositivos tengan el menor número de brechas de seguridad. A su vez, como he mencionado a lo largo de este post, tanto los dispositivos personales como los empresariales están comprometidos, y muchas veces no es necesario contar con un gran nivel de conocimiento para poder aprovechar dichas brechas de seguridad. En el área empresarial, que creo que es la que más perdidas puede generar, ISACA menciona 3 áreas de riesgo para tener en cuenta: el área operacional, el área financiera y el área técnica [5]. Finalmente, aunque estas áreas de riesgo me parecen un tema muy interesante, no voy a profundizar en las mismas en este post.

Bibliografía

[1] <<Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations>>, Oceano, consultado el 20/11//2020, https://ieeexplore-ieee-org.proxy-oceano.deusto.es/document/8688434

[2] <<7 biggest IoT risks facing businesses today – and what to do about them>>, TechGenix, consultado el 20/11/2020, http://techgenix.com/biggest-iot-risks/

[3] <<Breaking Down Mirai: An IoT DDoS Botnet Analysis>>, Imperva, consultado el 20/11/2020, https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

[4] <<Threat Intelligence Report Says IoT Attacks Doubled Within a Year, Predicts an Upward Trend>>, CPO magazine,

consultado el 20/11/2020, https://www.cpomagazine.com/cyber-security/threat-intelligence-report-says-iot-attacks-doubled-within-a-year-predicts-an-upward-trend/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Threat+Intelligence+Report+Says+IoT+Attacks+Doubled+Within+a+Year%2C+Predicts+an+Upward+Trend&utm_campaign=Weekly+Highlights

[5] <<Internet of Things: Risk and Value Considerations>>, ISACA, consultado el 20/11/2020, https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpiot

---

A buen viento, mucha vela, pero poca tela

Durante el debate que llevamos a cabo la semana pasada, tuvimos varios frentes abiertos en relación con los sistemas de información y otros temas relacionados. Para preparar dicho debate contamos con algunos artículos en la plataforma de la asignatura. En algunos artículos encontré ideas que compartía en mayor medida, pero otros me hicieron pensar. A continuación, daré mi opinión sobre estos temas.

El primer tema que me gustaría destacar proviene del artículo “Las TIC difuminan las fronteras de los negocios”. El artículo trata como bien indica el título que las tecnologías de la información y la comunicación (TIC) hacen posible la venta y distribución de artículos tanto a las grandes empresas como a las pequeñas, poniendo de ejemplo a Amazon y a un artesano de un pueblo de Teruel. Con esta parte estoy totalmente de acuerdo, pero lo que me hizo pensar es la segunda parte que

empieza así:

> *"No todas las empresas tienen capacidad para instalar el ERP más potente y costoso del mercado, ni tampoco el software de gestión de clientes, ni muchos otros… Pero la variedad en precio y la cantidad de aplicaciones existentes permiten también que pequeñas y medianas empresas cuenten con herramientas para la gestión digital de sus empresas que no tienen nada que envidiar a grandes soluciones."*

Después de darle unas cuantas vueltas en la cabeza estoy en desacuerdo con esta afirmación. No veo que una pequeña empresa necesite un ERP o un CRM u otro sistema de información si puede manejarse correctamente con hojas de cálculo. Los puristas o los expertos en la materia dirán que no es lo más optimo, pero a mi parecer el pequeño negocio puede utilizar una hoja de cálculo para llevar su contabilidad. Además, mientras realicé mis prácticas en empresa hablé del tema con un compañero, que había trabajado con ERPs anteriormente y me dijo lo siguiente: "Mientras puedas funcionar con un Excel no es necesario invertir en un ERP", con lo cual estoy de acuerdo.

El segundo tema que me llamó la atención está relacionado al artículo "El papel del cloud en la transformación del datacenter". En este artículo se menciona como el cloud está teniendo cada vez más importancia y que está haciendo que las tecnologías de la información (TI) estén siendo utilizadas como un servicio. A su vez, menciona que las plataformas en la nube ofrecen servicios en los que únicamente se paga por lo que se utiliza y se necesita. El artículo finaliza así:

> *"En este escenario, los clientes mantienen el control sobre los datos críticos de negocio, manteniendo la flexibilidad necesaria para escalar sus servicios en función de la demanda cambiante. Esto permite a una empresa controlar los costes, además de responder a las cambiantes necesidades del*

negocio.”

Este artículo me generó un gran número de preguntas mientras lo leía, entre las cuales se encuentran las siguientes: ¿Necesita una empresa el cloud? ¿Va a solucionar el cloud los problemas de la empresa? ¿Va a suponer un gasto adicional en vez de un ahorro?

Si bien es cierto que cada empresa debería hacerse este tipo de preguntas, muchas veces se omiten debido a que es lo que está de moda o es una “nueva” tecnología que promete solucionar todos los problemas, solo que no lo ven al realizar la inversión. Esto hace que las empresas contraten servicios que no necesitan y que en vez de suponer una ventaja competitiva es un lastre.

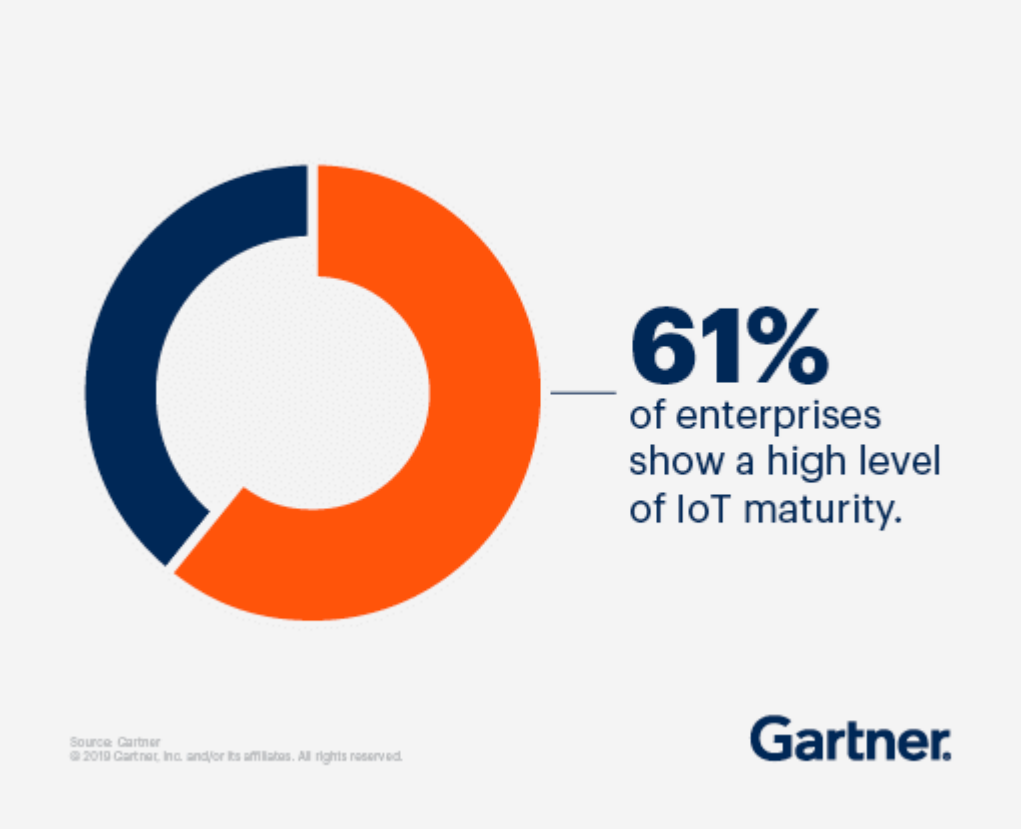
En conclusión, creo que algunas empresas invierten en nuevas tecnologías sin tener en cuenta si realmente las necesitan o van a conseguir mayores beneficios con las mismas. A título propio pienso que la adopción de nuevas tecnologías es completamente necesaria pero poco a poco y sin poner en riesgo la integridad de la empresa, siempre y cuando la situación lo permita.

IoT en la industria (IIoT)

Adopción del IoT en las empresas

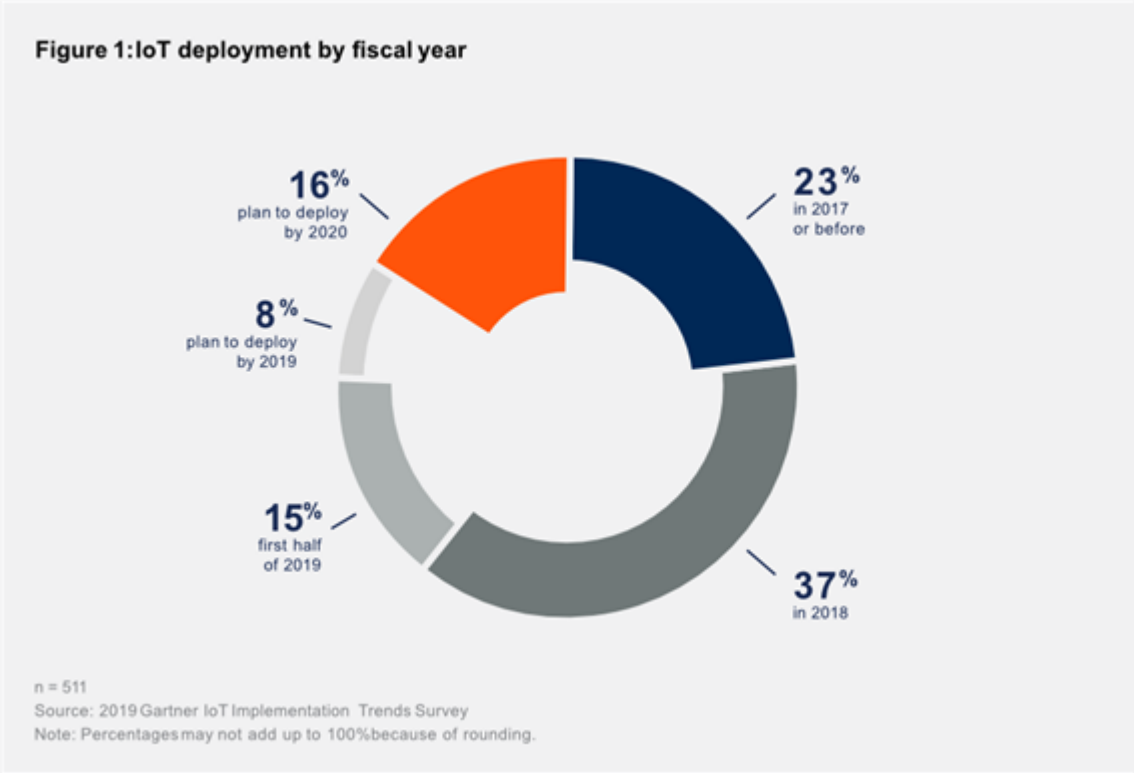
En la última década el mundo de la industria está teniendo su cuarta revolución, conocida como la Industria 4.0, que pretende interconectar productos y servicios. Para llevar esto a cabo de hace uso del IoT. La consultora Gartner no considera

el IoT como una tecnología emergente sino como una tecnología madura. Además, informa que el uso del IoT actualmente no se utiliza únicamente para operaciones internas, sino que para aumentar los beneficios y mejorar la experiencia del usuario, siempre sujetos al enfoque legal. Tamién, menciona que las empresas con un alto nivel de madurez en la materia del IoT obtienen mayor éxito al implementarlo. [1]



Madurez de las empresas en cuanto al IoT [1]

Finalmente, cabe destacar que según la consultora Gartner en 2019 el 75% de las empresas habían implementado al menos un caso de IoT, habiendo pasado de un 23% en 2017 a un 37% en 2019. [2]



Adopción del IoT en los últimos años [2]

Impacto del IoT en las industrias claves

Como comenté en mi post anterior, el IoT puede tener relevancia en cualquier empresa sin importar el sector al que pertenezca, aunque es verdad que algunos sectores realizan más avances que otros. A continuación, se muestra el impacto que tiene el IoT en algunos sectores industriales clave: [3]

- **Comunicaciones**: La revolución móvil está siendo lo más relevante en cuanto a la necesidad del IoT. En cuanto a las empresas consultadas el 53% de estas tenían IoT integrados en sus procesos y áreas de negocio más importantes. Estos dispositivos IoT más frecuentes son los dispositivos de audio y los teléfonos móviles, siendo la aplicación más frecuente el mantenimiento preventivo.

- **Servicios financieros**: Debido a que estas organizaciones necesitan un alto grado de seguridad emplean en gran medida el IoT en sus sistemas de seguridad. En cuanto a las empresas consultadas el 58% tenían implantados sistemas de IoT. Como se ha mencionado anteriormente, el IoT está presente en los sistemas de seguridad, en los análisis visuales para ser concretos. Más de la mitad de las empresas (51%) afirmaron que tenían desarrollado e implementado en sus sistemas de videovigilancia una IA para el análisis visual.
- **Servicios de salud**: Entre las empresas consultadas el 55% tenía implementado sistemas con IoT. Al igual que en el sector de las comunicaciones la mayoría de los dispositivos IoT son dispositivos de audio y teléfonos móviles, aunque el caso de uso más frecuente es el monitoreo de empleados junto con mejorar la experiencia de los clientes.
- **Frabricación**: Las empresas de este sector quieren medir y comprender el rendimiento de su maquinaria. Además, utilizan la visión artificial para seguir el movimiento de los productos pudiendo predecir o corregir acciones antes de que ocurran. El IoT ha facilitado al 51% de las empresas consultadas a ofrecer nuevas líneas de negocio y el 29% han podido ofrecer nuevos servicios o productos. Además, el 51% de las empresas han afirmado usar IoT y un 52% ha afirmado utilizar visión artificial junto con dispositivos IoT.

Tendencias del IoT en la industria (IIoT)

Gracias al IIoT han surgido nuevas tendencias en la industria. Entre las tendencias del IIoT de 2020 se pueden destacar las siguientes [4]:

- **Edge computing**: Todos los sensores y dispositivos de una fábrica obtiene información que se tiene que procesar. Además, esta información se tiene que juntar con información adicional para su posterior análisis. Esto hace que el gran número de dispositivos IIoT con los que cuentan las empresas no se puedan con el sistema de computación en la nube tradicional. Por este motivo, se trabaja con los datos en cada dispositivo, maximizando el rendimiento, minimizando costes y mejorando la latencia y la escala. Finalmente, es necesario destacar que las nuevas tecnologías como el 5G harán este proceso aún más valioso. En conclusión, con el edge computing se reducirán los cuellos de botella o incluso se eliminarán.
- **Digital Twins**: Gartner indica que el 75% de la empresas utilizan el IoT con los denominados *digital twins.* Los digital twins son la representación virtual de dispositivos u objetos físicos. Esto permite simulas objetos físicos en tiempo real. En resumén, los gemelos digitales permiten simular procesos y agilizar la producción.
- **Inteligencia artificial**: La inteligencia artificial y el *machine learning* han ganado relevancia

en los últimos
años, pero se espera que la conexión entre la IA y el IIoT aumente en los próximos
años. Actualmente se está invirtiendo en la coexistencia de varias
inteligencias artificiales y se están creando nuevas herramientas basadas en
esta tecnología. Por este motivo, aunque la complejidad sea elevada, se espera
que sea posible obtener buenos resultados con la inteligencia artificial en
muchas situaciones del campo del IoT. Por este motivo los CIOs tienen que construir
sus organizaciones con las herramientas y las habilidades de poder explotar la
inteligencia artificial en el IoT [5].

Conclusiones:

Creo que la relevancia del IoT está siendo cada vez mayor en la industria. Además, pienso que están surgiendo muchos campos anteriormente
desconocidos los cuales van a hacer que la industria evoluciones aún más rápido.
También pienso que el uso del IIoT tienes sus riesgos, pero de eso hablaré en
el próximo post.

Bibliografía

[1] <<Internet of Things: Unlocking True Digital Business Potential>>, Gartner, consultado el 12/11/2020, https://www.gartner.com/en/information-technology/insights/internet-of-things

[2] <<Internet of Things: Where Your Competitors Are Investing>>, Gartner, consultado el 12/11/2020,

https://emtemp.gcom.cloud/ngw/globalassets/en/innovation-strategy/documents/trends/iot-where-your-competitors-are-investing.pdf

[3] <<How IoT is impacting 7 key industries today>>, Forbes, consultado el 12/11/2020, https://www.forbes.com/sites/insights-inteliot/2018/08/24/how-iot-is-impacting-7-key-industries-today/?sh=2113f8de1a84

[4] <<5 Top Trends for IIoT in 2020>>, ElectronicDesign , consultado el 12/11/2020, https://www.electronicdesign.com/industrial-automation/article/21125147/5-top-trends-for-iiot-in-2020

[5] <<Gartner Identifies Top 10 Strategic IoT Technologies and Trends>>, Gartner, consultado el 12/11/2020, https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

---

¿Qué es el Internet of Things?

¿Como se define el Internet of Things?

Definir que es el *Internet of Things* (IoT) no es fácil. Esto es debido a que la definición varía en función del enfoque que tome la entidad que lo define y que activos se consideran más relevantes.

En 2015 el *Institute of Electrical and Electronics Engineers*

(IEEE) publicó un documento en busca de una definición neutral para el IoT[1]. En dicho documento se encuentran dos definiciones en función del escenario donde se quiera implantar, ya sea un escenario pequeño o un escenario grande.

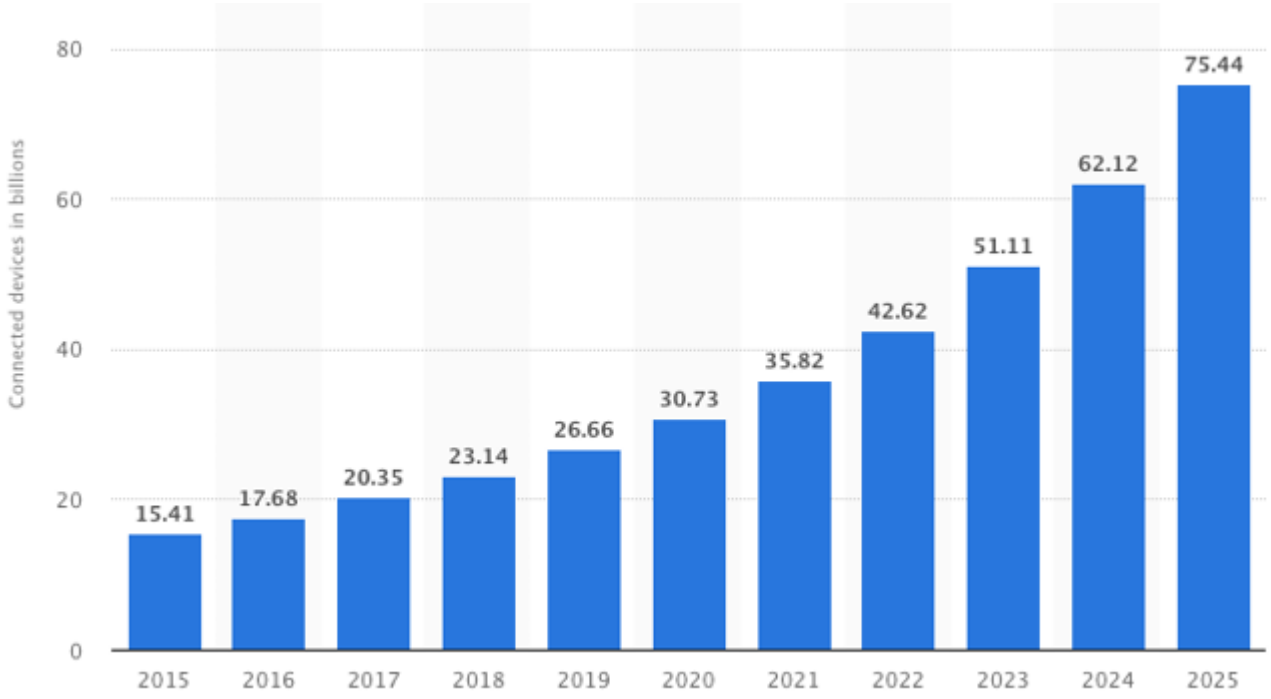
Deloitte por otra parte define así "¿Qué es IoT?"[2]:

> *«La definición de IoT podría ser la agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet, la red de redes), donde todos ellos podrían ser visibles e interaccionar. Respecto al tipo de objetos o dispositivos podrían ser cualquiera, desde sensores y dispositivos mecánicos hasta objetos cotidianos como pueden ser el frigorífico, el calzado o la ropa. Cualquier cosa que se pueda imaginar podría ser conectada a internet e interaccionar sin necesidad de la intervención humana, el objetivo por tanto es una interacción de máquina a máquina, o lo que se conoce como una interacción M2M (machine to machine) o dispositivos M2M.»*
>
> ***María Gracia** – Manager Especialista en el área de System Development & Integration, en la práctica de DxD de Deloitte*

¿Cuál ha sido la evolución del IoT?

El termino IoT surge en 2009, concretamente en un artículo publicado por Kevin Ashton. En dicha publicación se habla de la funcionalidad e información que otorga tener conectado todo tipo de dispositivos a la red. Cabe destacar que unos años antes se estimaba que había alrededor de 1000 millones de dispositivos conectados a internet.

A partir de 2011, gracias a la implementación del protocolo de direccionamiento IPv6 se hace posible el uso del IoT. La implantación de este protocolo otorga una expansión de las direcciones IP que pueden existir. Además, se estima que el número de dispositivos IoT va a crecer en gran medida con el paso de los años como se puede ver en la siguiente imagen. [3]



Evolución del número de dispositivos IoT conectados en miles de millones. [4]

¿Qué protocolos de comunicación utiliza el IoT?

Todos los dispositivos IoT, ya sean utilizado en entornos industriales como entornos domésticos, suelen compartir aspectos de kernel (normalmente kernel Linux) y servicios de bajo nivel, aunque las comunicaciones son diferentes. Esto hace que los protocolos de comunicación varíen en función del entorno[5].

En el entorno doméstico, cada fabricante suele tener su propio protocolo de comunicación, que suele ser de código cerrado. Entre los protocolos de este entorno se pueden destacar los siguientes:

- **Alljoyn**: Es un protocolo de código abierto que facilita la comunicación entre dispositivos y aplicaciones. Este protocolo está orientado a todo tipo de protocolos de la capa de transporte
- **OCF**: Es un proyecto de código abierto que pretende garantizar la interoperabilidad gracias a la

implementación de referencia y un programa de certificación.
- **Thread**: Es un protocolo basado en IPV6 utilizando cifrado AES.
- **MFI**: Protocolo propietario de Apple. Los productos de Apple incorporan un chip dedicado a este protocolo.

En el entorno industrial, surge el concepto de industria 4.0. Este concepto consiste en una digitalización completa desde los proveedores hasta los clientes. Para ello los dispositivos tienes que comunicarse, y suelen utilizar los siguientes protocolos:

- **HTTP REST**: Es un protocolo cliente-servidor de código abierto. Es efectivo para enviar gran cantidad de información como los datos recogidos por un sensor, aunque no es adecuado para enviar información en vídeo ni actualizaciones del orden del milisegundo. Se puede asegurar la información transmitida aplicando el protocolo criptográfico SSL/TLS.
- **MQTT**: Es un protocolo publicación/suscripción basado en el nivel de aplicación. Cuenta tanto con una versión basada en redes TCP/IP como con una versión no basada en este tipo de redes. En su diseño no incluye medidas de seguridad, pero se puede utilizar con TLS para asegurar las comunicaciones en la versión TCP o utilizar mecanismos compatibles par la comunicación no basada en TCP/IP.

En el entorno empresarial se utilizan más protocolos. En la siguiente tabla se resumen las principales características de algunos otros protocolos:

	Transporte	Modelo	Ámbito de aplicación	Conocimiento del contenido	Datos principales	Seguridad	Prioridad de los datos	Tolerancia a fallos
AMQP	TCP/IP	Intercambio de mensajes punto a punto	D2D D2C C2C	Ninguno	Codificados	TLS	Ninguno	Específica de la implementación
CoAP	UDP/IP	Petición/Respuesta (REST)	D2D	Ninguno	Codificados	DTLS	Ninguno	Descentralizado
DDS	UDP/IP (unicast + mcast) TCP/IP	Publicación/Suscripción Petición/Respuesta	D2D D2C C2C	Enrutamiento basado en el contenido, consultas	Declarados codificados	TLS, DTLS, DDS	Prioridades de transporte	Descentralizado
MQTT	TCP/IP	Publicación/Suscripción	D2C	Ninguno	No definidos	TLS	Ninguno	El nodo central (broker) es el punto único de fallo (SPoF)

Tabla de las carácterísticas de algunos protocolos de comunicación [5].

Conclusión:

El IoT es una tecnología que se está implementando tanto a nivel empresarial como a nivel personal. Además, esta tiene una gran relevancia
para las empresas, puesto que sus modelos de negocio se enfocan cada vez más en
los clientes, y con el IoT pueden ofrecerles más información a los clientes.
También, se están creando nuevos protocolos de comunicación, en función del
entorno en donde vaya a ser utilizado el dispositivo.

Desde mi punto de vista, creo que el IoT va a seguir evolucionando para hacer más sencillo el día a día, tanto de las empresas como de los particulares.

Bibliografía

[1] << Towards a definition of the Internet of Things (IoT) >>, IEEE, consultado el 25/10/2020, https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[2] <<IoT – Internet Of Things>>, Delloite, consultado el 25/10/2020,

https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

[3] <<A FONDO: ¿Qué es IoT (el Internet de las Cosas)?>>, Domodesk, consultado el 25/10/2020, https://www.domodesk.com/221-a-fondo-que-es-iot-el-internet-de-las-cosas.html

[4] <<Internet de las cosas: cuando todo está conectado>>, La Vanguardia, consultado el 25/10/2020, https://www.lavanguardia.com/vida/junior-report/20190301/46752655177/internet-cosas-dispositivos-conectados-iot.html

[5] <<IoT: protocolos de comunicación, ataques y recomendaciones>>, Incibe-cert , consultado el 25/10/2020 , https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

---

¿Existe un sistema educativo perfecto?

El sistema educativo español, en la mayoría de los casos se infravalora en comparación el de otros países. Cuando se hace un intercambio a un país extranjero y se obtienen buenas calificaciones se suele decir que aquí se les exige demasiado a los alumnos. Por otra parte, cuando el alumno no obtiene buenas notas, es debido a que el sistema no funciona. ¿Pero no puede ser que cuando el alumno saca buenas notas es debido a que este está bien preparado, o cuando saca malas notas es porque no ha realizado el esfuerzo necesario?

En España la educación se compone de 5 niveles[1]. Estos niveles se agrupan en la educación obligatoria y la no obligatoria. La educación obligatoria es entre los 6 y los 16 años, constando de la educación primaria (entre 6 y 12 años) y la educación secundaria (entre 12 y 16 años). La educación de carácter no obligatorio la constituyen la educación infantil (entre 0 y 6 años), la educación secundaria postobligatoria y la educación superior. Además, cabe destacar que cualquier nivel de educación se encuentra tanto en entidades de carácter público como privado, haciendo accesible la educación de cualquier nivel a todos los interesados.

Muchas veces he oído que el sistema educativo de Estados Unidos[2] es mejor que el español. El sistema estadounidense consta de doce años obligatorios, cinco años de primaria (entre 6 y 11 años) y siete años de secundaria (entre 11 y 18 años). Igual que en España en Estados Unidos se subvenciona la educación, pero únicamente la obligatoria. Esto hace que los estudiantes que quieren acceder a una universidad hagan uso de becas o pertenezcan a una familia adinerada.

Además, en los Estados Unidos se mide la competitividad de los centros educativos más que en España, haciendo que los estudiantes quieran acceder a estas instituciones. Por desgracia, un estudio realizado sobre los 146 colegios y universidades más competitivas, indicó que únicamente el 3% de los estudiantes admitidos provenían de familias modestas. ¿Es este el sistema educativo al que aspiramos? ¿Es el dinero el que decide el futuro que puede tener un estudiante?

Podría seguir comparando el sistema educativo español con otros sistemas educativos, como podría ser el finlandés, el chino, el japonés, etc. pero

no lo veo necesario, ya que todos ellos tienen sus pros y sus contras al igual
que el español.

Cada persona tiene en su cabeza lo que sería a su parecer el sistema educativo perfecto, pero como bien dice el dicho, “nunca llueve a gusto de todos”, y está claro que hay que marcar unos criterios generales. También pienso que hay aspectos que no se pueden enseñar, y que es necesario experimentar algún suceso para poder adquirirlos. Por tanto, la tendencia actual de criticar e infravalorar el sistema educativo, me parece una forma fácil de llamar la atención, puesto que me parece una chiquillada.

Referencias

[1]<<Sistema educativo de España>> Wikipedia, acceso del 20 de octubre de 2020, https://es.wikipedia.org/wiki/Sistema_educativo_de_Espa%C3%B1a

[2] <<Sistema educativo de Estados Unidos>> Wikipedia, acceso del 20 de octubre de 2020, https://es.wikipedia.org/wiki/Sistema_educativo_de_Estados_Unidos