Problemas comunes del uso de una herramienta de Business Intelligence

Es innegable que implementar una herramienta de BI trae consigo beneficios, tales como la reducción de costes, reducción para los tiempos, accesibilidad de la información para la toma de decisiones, formulación de estrategias competitivas, entre otros. Sin embargo, tras la fuerte inversión de capital para la herramienta y el proceso ETL, a la hora de hacer uso de la herramienta se dan cuenta que los resultados obtenidos no son los esperados. ¿A qué se debe esto?

En unos casos el problema reside en que la cúpula de las empresas creen que las herramientas del BI son la panacea y sus expectativas en lo que puede hacer están infladas.

En otros casos, el problema varía aunque estos suelen los más comunes:

La herramienta no cuadra con el negocio

Uno de los problemas más comunes es que la herramienta no sea completa o que no cuadre al 100% con el negocio. Esto se debe a una falta de comunicación o malentendidos durante la fase de definición de requisitos, en la que el desarrollador TI intenta desarrollar la herramienta con una lista de requisitos errónea o incompleta.

La datos no son limpios

Las herramientas de BI dependen de la exactitud de los datos. Estos pueden ser adquiridos desde distintas fuentes, desde ERPs automatizados a empleados que anotan los resultados en un bloc de notas. Lidiar con un entorno donde los datos no están actualizados o donde presenta incoherencias ralentiza el tiempo de generación de la solución de BI o puede proporcionar resultados imprecisos.

Puntos ciegos en los datos

En toda organización hay tipos de datos que son fáciles de conseguir en grandes volúmenes y datos que no lo son tanto, esta diferencia puede provocar que los análisis resultantes sufran por preferencia de selección, lo que conlleva a resultados poco precisos.

La herramienta no se mantiene

En otros casos la herramienta en cuestión no pertenece a la empresa y su desarrollo o mantenimiento se ha externalizado. Dependerá del contrato establecido con dicha organización establecer quién se encargará del mantenimiento, actualización, fase de adoptación, etc. Es esencial establecer minuciosamente todos estos datos si no queremos que una vez terminado el desarrollo de la herramienta perdamos el soporte de los desarrolladores.

No se usa

La adopción de los usuarios es siempre una de las fases más duras de todo proyecto. Se estima que el 22% de los empleados se encuentra a gusto con una herramienta de BI. Los motivos pueden ser los siguientes:

- No les gusta la solución.
- Los usuarios no están lo suficientemente preparados.
- Los usuarios no quieren cambiar.

No es future ready

Cabe destacar que medida que la empresa va evolucionando junto con el negocio se dan cuenta que su herramienta de negocio se queda atrás, que no es future ready. Las características que más se echan en falta en sistemas transaccionales son las siguientes:

- Poder añadir nuevos tipos de datos.
- Comunicarse con las API emergentes del mercado.
- Opciones de generación de gráficas y funciones analíticas más avanzadas. (Especialmente para los científicos de datos)
- Interfaz de usuario que no soporta el look&feel de las demás herramientas de la organización.

Como conclusión, son muchos los factores que pueden poner en peligro la implementación o el uso correcto/limitación de una herramienta BI, es por ello que se necesita de una planificación estratégica previa en la que se monitorice que se cumplen todos los objetivos necesarios para evitar estos problemas y obtener la solución esperada.

Internet of the things: Interactividad

sí, pero solo con mis amigos.

Cada vez se oye hablar más del Internet of Things (IoT) y de las bondades que trae consigo el uso de esta tecnología. Teléfonos, televisiones, relojes, casas… todos estos y más elementos han cambiado mucho en los últimos 10 años pero el cambio más revolucionario que han tenido en común ha sido sin lugar a dudas la posibilidad de conectarlos a la red y poder así interactuar entre otros dispositivos, ofreciendo nuevos servicios y ventajas.

Cada vez existen nuevas tecnologías y protocolos que facilitan y mejoran la conectividad entre dispositivos tales como el Bluetooth LE, WiFi Direct, Zigbee, etc. Sin embargo, los fabricantes han decidido crean un "ecosistema" de dispositivos en los que solo puedan interactuar entre ellos éstos están limitados por plataforma. Aún hoy en día si un usuario de Android quiere enviar un fichero a otro usuario de iOS tiene que utilizar herramientas de terceros para realizar dicha función, dado que el sistema operativo corta la conexión cuando detecta que dicho dispositivo no pertenece a la "familia".

Este ejemplo no es un saco aislado en telefonía, también ocurre con los "wereables", sistemas de domótica, etc. La raíz del problema está en que no existe un estándar para entablar comunicaciones entre los distintos dispositivos es por eso que los fabricantes realizan implementaciones baratas de un protocolo de handshaking propietario y lanzan sus productos al mercado, al fin y al cabo, no hay mejor forma para entablar un estándar que adquirir la mayor cuota de mercado.

Lamentablemente esta es la etapa que nos toca vivir. Cabe destacar que las grandes empresas del sector como Intel, Qualcomm, Samsung, Microsoft, entre muchos otros ya han entablado conversaciones y han generado asociaciones que tienen como objetivo la creación de estandares que solventen este y muchos otros problemas.

Una vez concluyan se definan las especificaciones y se lancen estos nuevos dispositivos bajo la certificación del estándar se podrán llevar a cabo proyectos de gran envergadura como las Smart Cities y solventar las limitaciones a las que se enfrentan a día de hoy.

Sin lugar a dudas esta tecnología supondrá una revolución y supondrá un cambio drástico en la forma con la que interactuamos con las "cosas".

Network Connected Devices (Internet of Things): Estándares y beneficios

Estándares

Si bien llevamos más de una década conviviendo con el IoT no fue hasta el 2013 cuando se comenzaron a nombrar los estándares. Sin embargo, mientras surgen consorcios y alianzas la industria no permanece a la espera y se genera una lucha entre las organizaciones por establecer cuál de las tecnologías fabricadas por cada casa prevalecerá en el mercado, tal y como pasó en su día con *La guerra de los navegadores* o *La guerra del formato óptico para la alta definición*.

Muchas veces estas guerras se ganan o se pierden antes incluso de que se establezca un estándar. En el 2013 se crearon ciertas alianzas entre los líderes del sector y se comenzaron a producir dispositivos con certificación que avalaba que cumplian con las especificaciones que se había decretado en dichos estandares.

El IoT implica establecer un vínculo entre los dispositivos interconectados, con los que en la mayoría de los casos no hubiera sido posible establecer una conexión. Por otra parte, involucra la gestión de esos dispositivos y la creación de aplicaciones que establecen una relación entre ellos para realizar tareas o funciones que no serían posibles de completar por ellos mismos como individuos. Todos los dispositivos del IoT están destinados a poder comunicarse entre ellos, sin embargo a día de hoy no existe ningún estándar formalizado o universal que permita llevar a cabo esta virtud.

Las Alianzas formadas intentan solventar esta problemática, así como establecer unas directrices de desarrollo, con el fin de reducir el alto porcentaje de dispositivos vulnerables que se han producido como resultado de no tener definida una lista de buenas prácticas a seguir en función de la tecnología escogida para el desarrollo de los dispositivos.

Las alianzas resultantes que caben destacar son las siguientes:

AllSeen Alliance

Este grupo es uno de los que más adeptos está reclutando, comenzó en Diciembre de 2013 formado por Qualcomm, Cisco Systems, Panasonic y otras empresas relacionadas con el sector electrónico. Desde entonces se ha cuadriplicado con 100 miembros.

El protocolo AllJoyn primero diseñado por Qualcomm ahora gestionado por la fundación Linux, es el estándar que originó la AllSeen Alliance. Alljoy es un

framework open-source que gestiona la conectividad y las operaciones de la capa de servicio para los dispositivos IoT con el objetivo de "*crear productos interoperables que sean capaces de buscar, conectarse e interactuar directamente con dispositivos, sistemas y servicios cercanos independientemente de la capa de transporte, tipo de dispositivo, plataforma, sistema operativo o marca*" .

Open Interconnect Consortium

Open Interconnect Consortium (OIC) fue fundada por Intel en Julio, apoyada por fabricantes que incluyen a la propia Intel, Samsung y Dell. El objetivo de esta asociación es definir un conjunto de especificaciones que ayuden a los dispositivos a buscarse y a trabajar entre ellos.

El *framework open-source* cubre las funciones tales como la búsqueda, comunicación y intercambio de datos. Este *framework* hace competencia directa al propio desarrollado por AllSeen Alliance, AllJoyn que ha resultado en disputas entre los grupos por asuntos de propiedad intelectual.

Thread Group

Fue fundada por compañías como ARM, Samsung y por la reciente adquisición de Google en termostatos y alarmas de incendios, Nest, al mismo tiempo que el OIC. El objetivo de esta alianza es crear un *framework* ambicioso centrado en la comunicación inalámbrica que gestiona la red, consumo energético, la seguridad y la compatibilidad de productos. Cabe destacar que cada dispositivo con certificación Thread dispone de una dirección IPv6, facilitando así muchos problemas de redes.

La ZigBee Alliance se unió recientemente a este grupo, lo que supone que ofrecerá una mayor visibilidad del protocolo para el estándar.

En lo que respecta a su relación con el protocolo AllJoy y el estándar de OIC, a diferencia de estos últimos Thread es un protocolo de radio, lo que posibilita la coexistencia de estas alianzas pacíficamente.

Industrial Internet Consortium

The Industrial Internet Consortium (IIC) fue fundada en Marzo de 2014, su labor se centra en el desarrollo de buenas prácticas relacionadas con las aplicaciones industriales del IoT. Le apoyan principalmente grandes empresas como GE, IBM, Cisco, AT&T e Intel.

La IIC ha comunicado que no está desarrollando un estándar por sí misma, sino que está trabajando en agrupar a las organizaciones y la tecnología necesaria para acelerar el crecimiento del Internet industrial mediante la identificación, agrupación y promoción de buenas prácticas.

IEEE P2413

El Institute of Electrical and Electronics Engineers (IEEE) ha formado un grupo para establecer un poco de orden en lo que se refiere a las especificaciones del IoT, siendo estas desarrolladas por el consorcio. Actualmente además de existir 350 estandares que pueden aplicarse al IoT, existe un borrador del estándar aunque se estima que el estándar se finalice a lo largo del 2016. Mientras tanto, el grupo está estableciendo relaciones con otros fabricantes y otros organismos relacionados con el IoT como el IIC y oneM2M entre otros.

ITU-T SG20

Grupo establecido en Junio de 2015. La International Telecommunication Union está en proceso de desarrollar un estándar que no solo cubre al IoT, sino tambien a las Smart Cities and Communities (SC&C). El estándar SG20 tiene el objetivo permitir el desarrollo coordinado de las tecnologías de IoT, incluyendo las comunicaciones maquina a maquina y las redes ubicuas de sensores.

OneM2M

Formada en 2012 y con el apoyo de siete de las organizaciones de desarrolladoras de estándares más prestigiosas del mundo, oneM2M es una organización global que tiene como objetivo crear un estándar escalable e interoperable para la comunicación de dispositivos y servicios usadas en aplicaciones M2M y el IoT. Ofrece un estándar que da soporte a aplicaciones y servicios tales como la red eléctrica inteligente, el coche inteligente, domótica, seguridad pública y salud.

Apple

Apple ha desarrollado su *framework* HomeKit, para comunicarse y controlar los acessorios conectados en el hogar del usuario. Como es de esperar, no es un estándar sino la “forma de hacer” que tiene Apple. Los desarrolladores pueden decidir si usarlo o mantenerse al margen.

Aunque el *framework* ya está disponible, no está teniendo el éxito esperado debido a la insistencia de Apple por usar una encriptación de 3072 bits y chips certificados por ellos mismos en los dispositivos que usen WiFi o Bluetooth. Esto supone que los desarrolladores tengan que rediseñar su línea de productos si quieren soportar el HomeKit.

Por otra parte, ya están saliendo al mercado dispositivos que soportan el HomeKit y nada fomenta más un estándar que productos en las estanterías de una tienda.

Beneficios

Hemos visto como el uso del IoT supone nuevos riesgos, el objetivo de las organizaciones consiste en definir los escenarios en los que los beneficios de la implantación sean mayores a estos nuevos riesgos o al menos alcancen un equilibrio.

Es innegable que el IoT ofrece beneficio y valor añadido a las organizaciones, y estas no pueden ignorar estos hechos. Entre todos los beneficios que otorga el IoT caben destacar los siguientes:

- **Reducción de costes: Los costes pueden reducirse debido a un aumento en la eficiencia de los activos, procesos y mejoras de servicio. *General Electric* estima que la mínima mejora en los procesos que permitan una reducción en el consumo de energético, puede suponer un ahorro de miles de millones.**
- **Aumento de la eficiencia de uso de los activos:** Con la mejora de los procesos y la monitorización de los recursos, la industria se puede beneficiar de las ventajas de la visualización en tiempo real de sus activos pudiendo localizarlos o realizar mantenimientos preventivos de piezas críticas mejorando el procesamiento de los productos.
- **Aumento de la eficiencia de los procesos:** La introducción de los procesos de monitorización en tiempo real mejora la toma de decisiones, minimiza la intervención humana y reduce, por ello, los costes operativos y totales.
- **Aumento de la productividad:** Mejora la productividad de la organización gracias a los entrenamientos *just-in-time* solventando la escasez de habilidades disponibles frente a las necesitadas, mejorando la eficiencia laboral.

Network Connected Devices (Internet of Things): Riesgos (parte 2, Final)

Mitigación y Priorización

En este apartado se analizará y se profundizará más en cada uno de los riesgos descritos en la subsecciones anteriores, finalizando con una tabla

que contendrá un resumen con el impacto del riesgo y su probabilidad.

Salud y Seguridad

Los riesgos de salud y seguridad están relacionados estrechamente con el negocio. El impacto en todos los casos es alto, dado que involucra vidas humanas o repercute en el medio ambiente. La probabilidad de que se dé depende del negocio en cuestión y de las funciones de las que se encargue el dispositivo IoT.

Este riesgo está sensiblemente relacionado al resto de los riesgos de negocio, operacionales y técnicos ya que cualquiera de estos puede comprometer tanto a la salud como a la seguridad.

Para mitigar este riesgo es necesario realizar un modelo holístico para prevenir, detectar y corregir las posibles vulnerabilidades del dispositivo. Este modelo consiste en identificar a los *Stakeholders* para poder definir el ámbito de uso. Una vez definido esto, se realiza una evaluación de los riesgos para identificar las posibles vulnerabilidades y determinar el impacto de negocio que supondría que ocurrieran dichos riesgos. A continuación, es necesario desarrollar un plan de contingencia que garantice la seguridad y el buen funcionamiento del dispositivo. Por último, y no menos importante, se requiere realizar un proceso de monitorización continua para salvaguardar y/u obtener evidencias de que todo va según lo establecido y realizando siempre un análisis actualizado de las posibles vulnerabilidades que pudieran comprometer la seguridad del dispositivo.

Cumplimiento de la regulación

Los riesgos de cumplimiento de regulación dependen del país en el que resida la sede de la organización y de la legislación de los países en los que ofrezca servicio.

Una organización se enfrenta a estos riesgos, mayormente, cuando se producen cambios en la ley o la regulación que afectan a la industria o un negocio, que pueden implicar cambios en los procesos, *frameworks* y costes. Dependiendo del negocio, estos cambios pueden suponer el cierre del mismo por lo que supone un impacto alto, aunque, con una buena gestión, es dificil que esto ocurra por lo que la probabilidad resultante es media.

Para mitigar los posibles riesgos referentes al cumplimiento de la regulación es necesario hacer una gestión de la misma. Ésta casi siempre va de la mano de una auditoría, ya sea externa o interna, en la que se definirá qué rasgos de la regulación afectan más a la empresa. Con esto, se exigirán las evidencias que demuestran que se cumple con la regulación para asegurarse que todo funciona como lo exige la ley. Este proceso requerirá realizar una monitorización periódica para controlar los posibles cambios jurídicos que puedan surgir.

Privacidad del usuario

La privacidad del usuario está ligada a las vulnerabilidades del dispositivo,

leyes de los países en los que se opere y de cómo la organización gestione los datos de carácter personal. Teniendo en cuenta que más del 90% de dispositivos contiene información sensible y de que de éstos el 70% presenta algún tipo de vulnerabilidad, la probabilidad de este riesgo es alta. El impacto representa una sanción económica por parte del órgano judicial, así como una pérdida de confianza de los usuarios, por lo que supone que el impacto sea alto.

Para mitigar estos riesgos, por una parte el usuario ha de estar concienciado y entender lo que suponen los siguientes factores del IoT:

- La interoperatividad entre dispositivos y tecnologías.
- Como la información se transmite entre dispositivos y aplicaciones.
- Los términos “privacidad” y “condiciones de uso” de los dispositivos.
- El riesgo de compartir información entre los dispositivos y las redes sociales.
- La implicación de vincular cuentas presentes en las redes sociales.

Conociendo estos factores el usuario entenderá cuales son sus derechos y se pensará dos veces qué tipo de contenido comparte en la red.

Por otra parte, la organización debe cumplir según la regulación de los países en los que opere. Se establecerán las responsabilidades de las organizaciones externas que tengan acceso a dicha información y se llevarán a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Costes inesperados

El hacer uso de esta nueva tecnología supone una implantación y un desarrollo más lento. Por otra parte, un cambio en los estándares exigiría una nueva planificación, modificación de fechas de entregas y una inversión de fondos adicionales. De todas formas, haciendo un análisis de los riesgos, no serán tan arriesgados como para poner en peligro la organización. Es por ello que la probabilidad de este riesgo es media y el impacto es bajo.

En estos casos, es aconsejable seguir las novedades que realizan los organismos responsables del estándar para poder planificar de antemano cualquier imprevisto y asignar un margen de costes para solventar o mitigar dichos imprevistos.

Acceso inadecuado

Una vulnerabilidad en el dispositivo, puede implicar un acceso inadecuado al mismo. Por otra parte, con la reducción de coste de los dispositivos, cada vez son más los que se sitúan en áreas desprotegidas exponiendo, físicamente, la integridad del sistema. Debido al alto número de dispositivos que presentan vulnerabilidades y a la creciente disposición de dispositivos sin monitorización, la probabilidad de acceso inadecuado es alta, siendo su impacto alto dado a que pueden afectar tanto a la salud y seguridad como a la privacidad de la información del usuario.

Para mitigar este riesgo, es necesario restringir el acceso al dispositivo, bien físicamente o mediante un sistema de autenticación y autorización lo suficientemente robusto. Por otra parte, será necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Uso inapropiado

Las vulnerabilidades del dispositivo implican que usuarios no autorizados puedan acceder a los procesos de los dispositivos y alterar su funcionamiento. Por otra parte, los usuarios, como tal, pueden utilizar el dispositivo o componentes del mismo con fines para los que no fueron diseñados. En el primer caso el riesgo es alto, dado que pueden comprometer la salud, la seguridad y la privacidad de los datos. Debido al alto número de dispositivos que presentan vulnerabilidades y a la creciente existencia de los mismos, sin monitorización, la probabilidad de que se dé un uso inadecuado del dispositivo es alta.

Para mitigar este riesgo, sobre el uso inadecuado por parte del usuario, es necesario definir una política de uso que exhuma de responsabilidad a la organización de su uso indebido. Por otra parte, será necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Rendimiento

El rendimiento se puede ver alterado por un uso inapropiado de los recursos causado por una vulnerabilidad del dispositivo o por un mal diseño, esta última siendo menos probable. Dependiendo de la funcionalidad que desempeñe el dispositivo, el impacto variará. Como ejemplo, no es lo mismo un sistema de monitorización de aviones que el sensor que monitoriza la temperatura de la calefacción de una vivienda, es por ello que el impacto puede ser alto o bajo. En lo que respecta a su probabilidad, debido al alto número de dispositivos que presentan vulnerabilidades, la probabilidad de una alteración del rendimiento es alta.

Para mitigar este riesgo, es necesario realizar un modelo holístico para descubrir las posibles vulnerabilidades del diseño del dispositivo así como cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Vulnerabilidades del dispositivo

Superar este reto es sin lugar a dudas uno de los retos más duros a los que se enfrenta el IoT dado a la diversidad de vulnerabilidades que se han encontrado en los dispositivos ya existentes en el mercado. Se calcula que cerca del 70% de los dispositivos IoT presentan algún tipo de vulnerabilidad, entre las que cabe destacar:

- El 80% de estos dispositivos tiene una contraseña débil o corta o políticas de seguridad insuficientemente complejas.
- El 70% de los dispositivos falló a la hora de encriptar los servicios de

transmisión de datos por la red local e Internet.

- El 60% de los dispositivos con interfaz web permiten realizar ataques de *cross-site scripting*, mantienen las credenciales por defecto o realizaban una mala gestión de la sesión.
- Por otra parte, al no haber un estándar universal definido, seguido de unas buenas prácticas del desarrollo para comunicación entre dispositivos, muchos de ellos realizan conexiones inalámbricas de protocolos que presentan vulnerabilidades, como los que se pueden mostrar en la parte inferior de la figura 2.

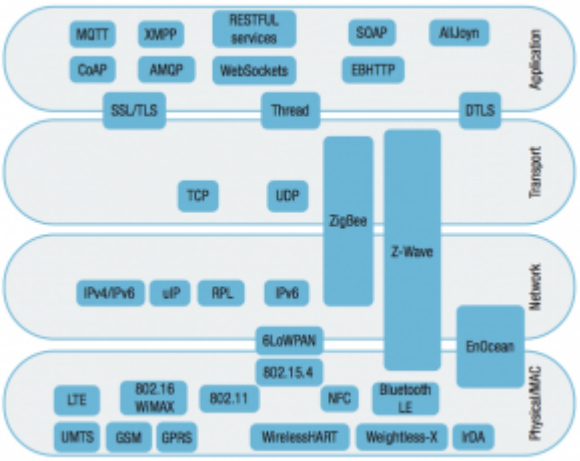

Figura 2: Protocolos más usados en el IoT

Como se deduce, la probabilidad de que un dispositivo presente vulnerabilidades de algún tipo es alta. Por otra parte, tal y como se ha visto en las subsecciones anteriores, este riesgo compromete aspectos tan críticos como la salud, seguridad y la privacidad del usuario, por lo que el impacto que supone también es alto.

Para mitigar algunos de estos riesgos es necesario realizar las siguientes tareas:

- Desarrollar una legislación, políticas, estandares y buenas prácticas.
- Liberar el software propietario no compatible a la comunidad *open-source*.
- Asegurarse de que los sistemas embebidos remotos están monitorizados o su vida útil es finita.
- Integrar la seguridad en los procesos de diseño de los dispositivos.
- Realizar un estudios de los servicios que se utilizan para la comunicación y puedan crear situaciones inseguras o no deseadas y planear una arquitectura para salvaguardarse de estas vulnerabilidades.
- Definir y habilitar comprobadores de la integridad de los datos en los dispositivos.

Actualizaciones del dispositivo

Este riesgo consiste en no mantener al dispositivo y brindarle actualizaciones que solventen vulnerabilidades. Pero además, incluye las vulnerabilidades propias de dicho proceso:

- La comunicación entre el servidor y el cliente no está cifrada, pudiendo así acceder al contenido del mismo.
- Los clientes que no protegen el espacio de memoria destinado a la actualización, siendo posible la instalación de un código de terceros.

Al igual que los riesgos de seguridad, estos riegos comprometen aspectos tan críticos como la salud, seguridad y la privacidad del usuario, por lo que el impacto que suponen es alto. Por otra parte, debido al alto número de dispositivos vulnerables, la probabilidad de padecer este riesgo también es alto.

Mitigar este riesgo consiste en impedir que los usuarios consigan aprovecharse de las vulnerabilidades de dispositivos no soportados o no actualizados y asegurar los procesos de actualización. Para ello hay que llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos, así como definir un ciclo de vida para los dispositivos, monitorizados y darlos de baja cuando llegue el momento.

Gestión del dispositivo

Este riesgo consiste en salvaguardar los procesos de configuración, supervisión y mantenimiento de los dispositivos, donde entran en juego las vulnerabilidades y el acceso autorizado. Una mala monitorización o la configuración por un usuario no autorizado puede comprometer la salud, seguridad y la privacidad de la información, por lo que el impacto de este riesgo es alto. Por otra parte, debido a la gran cantidad de dispositivos que presentan algún tipo de vulnerabilidad, la probabilidad de este riesgo es alta.

Para mitigar este riesgo, es necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos, así como establecer un control sobre los usuarios que están autorizados para la manipulación del dispositivo sin olvidarnos de una continua monitorización.

Riego	Impacto	Probabilidad
Salud y seguridad	Alto	Bajo-Alto (Dependiente de Negocio)
Cumplimiento de la regulación	Alto	Bajo
Privacidad del usuario	Alto	Alto
Costes inesperados	Medio	Bajo
Acceso inadecuado	Alto	Alto
Uso inapropiado	Alto	Alto
Rendimiento	Bajo-Alto (Dependiente de la función que desempeña el dispositivo)	Alto
Vulnerabilidades del dispositivo	Alto	Alto
Actualizaciones del dispositivo	Alto	Alto

Gestión del dispositivo	Alto	Alto	

Priorización de los riesgos

Network Connected Devices (Internet of Things): Riesgos (parte 1)

Riesgos

Al igual que la introducción de toda nueva tecnología, el IoT supone nuevos riesgos que varían en función del negocio de la empresa que lo implemente. Es por ello que hacer un análisis previo que valore los pros y contras en la utilización de esta tecnología y de sus beneficios es imprescindible. Si bien los riesgos dependen del fin y el uso que se dé a la tecnología que incluya el IoT, ISACA define los siguientes a tener en cuenta por todos los sectores:

Riesgos de negocio

Se dividen en cuatro subcategorías que afectan al funcionamiento o rentabilidad de la empresa interesada en la implantación de esta tecnología.

- **Salud y seguridad:** Poner en peligro la integridad y bienestar de los usuarios o miembros de la organización afectando tanto a los procesos intermedios como al producto y servicio final.
- **Cumplimiento de la regulación:** Los aspectos legales y jurídicos a cumplimentar por la organización para mantenerse dentro de la legalidad.
- **Privacidad del usuario:** Lo constituyen todos los procesos y/o transacciones en los que se opere con información sensible de los usuarios.
- **Costes inesperados:** Los gastos derivados de los imprevistos que implican los cambios realizados en la planificación inicial.

Riesgos operacionales

Se agrupan en esta categoría los riesgos que genera el uso de sistemas embebidos, que acarrean las pérdidas de valor y en los que pueden intervenir procesos internos fallidos, personas, sistemas o agentes externos.

- **Acceso inadecuado:** Asegurar que solo el personal adecuado puede hacer uso de los procesos.
- **Uso inapropiado:** Salvaguardar que tanto los procesos intermedios como el producto o servicio final realicen la tarea para la que fueron diseñados.
- **Rendimiento:** Monitorizar y asegurarse de que todas las transacciones y

procesos se realizan en el periodo de tiempo estimado por la compañía.

Riesgos técnicos

Estos riesgos consisten en la exposición a posibles pérdidas que envuelven los procesos de diseño, ingeniería, producción y procesos tecnológicos entre los que se caracterizan los siguientes:

- **Vulnerabilidades del dispositivo:** Al igual que los dispositivos tradicionales, estos también pueden ser comprometidos por *malware*. Pero además, al tener una dirección en la red, pueden convertirse en objetivos potencialmente sensibles a ataques informáticos.

- **Actualizaciones del dispositivo: Mantener la seguridad tanto en el canal de comunicación así como en el acceso de escritura del dispositivo durante el proceso de actualización.**

- **Gestión del dispositivo:** Procesos de configuración, supervisión y mantenimiento de los dispositivos.

Network Connected Devices (Internet of Things): Contexto, definición y desafíos

Contexto y definición del IoT

La idea del internet de las cosas *Internet of the Things (IoT)* vio la luz por primera vez a principios de los años 70, por la comunidad de *Circa 2000*, con la invención de un sistema capaz de leer y escribir en etiquetas *RFID* pero que además era capaz de buscar información en Internet o en una base de datos acerca de dicha etiqueta.

Más adelante, ya entrados en los 90, Mark Weiser, científico jefe en Xerox PARC, publicó en la revista *Scientific American* el artículo científico *The Computer in the 21st Century*, en el que se introdujeron por primera vez términos como “La computación ubicua” y “la virtualidad tangible”. Este artículo realizaba una predicción del futuro sobre la comunicación entre dispositivos hardware y software por medio de cables o redes inalámbricas. Los dispositivos estarían tan mimetizados con nuestro entorno y serían tan ubicuos que nadie sería capaz de notar su presencia.

Gracias a esta publicación, se pasó de la idea específica relacionada a las etiquetas *RFID* a un concepto más general del IoT y por el cual es conocido en la actualidad. Este concepto recoge todos los dispositivos que pueden conectarse a la red e interactuar entre ellos y los usuarios, tales como: teléfonos móviles, cafeteras y lavadoras entre otros.

Lejos quedan los tiempos en los que se requerían grandes inversiones para fabricar los elementos básicos de las "cosas" *[the things]*, como pueden ser los lectores de etiquetas *RFID*.

En la actualidad la reducción de los costes de producción ha incentivado una producción masiva de objetos *Smart* que tratan de facilitarnos la vida en todas sus facetas.

La previsión que envuelve el crecimiento de IoT se estima que sea superior al de los demás dispositivos presentes en el mercado actual, ya sean PCs, Tablets, Televisores, etc. tal y como puede observarse en la figura 1.

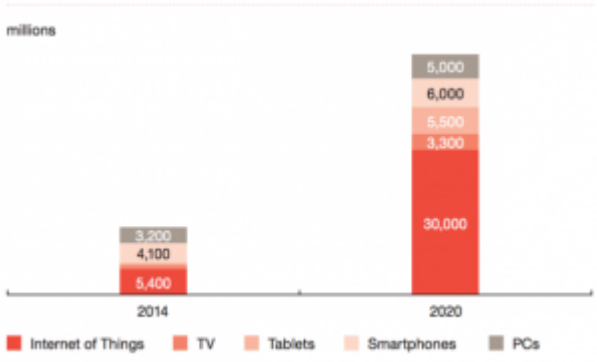

Figura 1: Estimación de dispositivos conectados en el 2020.

Desafios

Cuando una organización trate de instaurar el IoT se encontrará con múltiples barreras o trabas, tales como la priorización económica, confrontación de los nuevos riesgos y otros factores. Además de los desafíos técnicos relacionados con el consumo, latencia, integración y almacenamiento, hay una serie de desafíos críticos para la implantación del IoT entre los que se pueden destacar los siguientes:

- **Seguridad: Dado que el IoT promueve la conexión de dispositivos entre sí, induce a crear nuevos objetivos para el *malware* o a la manipulación de los mismos. Se deberán, por tanto, diseñar más capas de software, integración con middlewares, *API*s, comunicaciones maquina a maquina, entre otros, lo cual lleva a una mayor complejidad y a nuevos problemas de seguridad.**
- **Privacidad y confianza:** Con la entrada de sensores remotos y siendo la monitorización el caso de uso principal del IoT, conllevará a dar más relevancia a incrementar el control de acceso, definir quién es el propietario de la información, controlar a los socios y más aún en entornos donde estén en juego vidas humanas.

- **Complejidad, confusión y problemas en la integración:** Debido a las múltiples plataformas, numerosos protocolos y grandes cantidades de APIs, la integración de los sistemas de IoT al igual que su testeo, será todo un desafío. Por otra parte, el caos existente en lo que respecta a los estándares hará que se ralentice su implantación. Con la rápida evolución de los APIs, lo más probable es que se consuman un número inesperado de recursos del desarrollo, lo cual disminuirá las habilidades del grupo del proyecto para añadir una nueva funcionalidad esencial. Una implantación más lenta y un desarrollo no anticipado de los recursos probablemente modifique las fechas de entrega y ralentice los ingresos en el tiempo. Por tanto, esto requerirá de una inversión de fondos adicionales para los proyectos de IoT.
- **Arquitecturas cambiantes, guerra de protocolos y estandares:** Con tantas organizaciones e instituciones involucradas en el IoT, se producirán una lucha de intereses entre los sistemas propietario y los distintos estandares *open-source*.
- **Concreción de los casos de uso y proposiciones de valor:** La falta de casos de uso claros o de ejemplos contundentes de ROI ralentizarán las implantaciones de IoT. A pesar de las especificaciones técnicas, usos teóricos y conceptos futuros puede que estos no sean suficientes para los primeros usuarios que implanten esta tecnología. La implantación convencional de las IoT requerirá de comunicaciones bien fundamentadas y dirigidas al cliente y de mensajería en torno al "que hay en él para mi". Dar explicaciones detalladas de un recurso específico o detalles técnicos de un componente no detendrán el proceso cuando los compradores busquen una "solución completa" o un servicio de valor añadido completo. Los suministradores de IoT tendrán que defender los beneficios clave de sus servicios y el porqué de su implantación.

Sistemas de Información y las PYMES

Cuando te explican lo que hacen los Sistemas de Información (SI) te quedas asombrado de las cosas en las que te facilitan la vida, y más aún en una sociedad donde ofrecer un producto o servicio no garantiza la supervivencia a largo plazo de las empresas. Sin embargo, cada vez que veo al frutero de

turno, o al pequeño comercio, por ser más genérico, y contemplo un uso nulo de los SI me pregunto como consiguen subsistir y cómo mejorarían su situación si las usasen.

En general las pequeñas y medianas empresas cuentan con una mayor adaptación al cambio, cercanía al mercado local y más capacidad de crecimiento, pero aún con esto tienen un gran inconveniente, una resistencia a la tecnología.

En las grandes empresas la implantación de una nueva tecnología se produce más por imitación de la competencia más que por una planificación estratégica. En el pequeño comercio, por el contrario esta técnica no es de mucha utilidad, dado que carecen del presupuesto necesario para ponerse a experimentar y juguetear con una tecnología. Es por ello que para que realmente se establezca el uso de una tecnología ha de analizarse qué beneficios supone dicha herramienta y a aprender a beneficiarse de ella, de forma que su uso esté alineado con el negocio.

A continuación se listan brevemente qué beneficios podría suponer la implantación de un SI en las PYMES:

- **Rapidez en los procesos:** Las TI pueden ayudar a reducir los tiempos de completado de los diferentes tipos de procesos, desde la selección de materias primas hasta inspección de calidad, ventas, logística, y pago. Los SI pueden dar información sobre los procesos que posibilita analizarlos más en detalle para poder optimizarlos.
- **Reducción de costos: Al mismo tiempo que optimizan los tiempos de los procesos, indirectamente esto produce una reducción de los costes.**
- **Mejor servicio:** Al reducir los tiempo, a su vez se está mejorando el servicio, esto se convierte automáticamente en una ventaja competitiva que puede ayudar al negocio a competir con otras empresas más grandes.
- **Publicidad:** Los sistemas de información de propósito general permiten permiten a su vez generar páginas web con las que darse a conocer, genera un servicio en la que los clientes potenciales pueden acceder a información sobre la empresa que puede inducir a la venta del producto o servicio.
- **Aumento de Ventaja Competitiva:** Las tecnologías de información pueden proveer al negocio con una ventaja competitiva, incluso hay ocasiones en que el mercado obliga a las pequeñas empresas a incorporar TI en sus negocios, por ejemplo, si un competidor que tiene una cadena de supermercados que maneja código de barras se instala frente a otro que no cuenta con esta tecnología, este hecho podría representar una barrera para que los clientes que prefieran o valoren esta tecnología.

Cabe concluir que la mayoría de pequeñas empresas manifiestan un gran interés por la información y las tecnologías relacionadas con ella. Sin embargo, desconocen la oferta tecnológica disponible, como acceder a ella, como utilizarla y cuáles son los beneficios de su uso, por lo que creo que resultaría beneficioso para la industria del interior que el gobierno u otra entidad ofreciera información a las empresas formadas en este asunto, para

reducir los costes que supone decantarse por una u otra tecnología y así poder disfrutar de los beneficios que su implantación supone.

Planificación Estratégica

Desde que era pequeño siempre he tenido en cuenta que tiene que haber buenas prácticas que nos asegure la efectividad de nuestras acciones independientemente de la actividad que estemos realizando, además de pensar que dichas prácticas se adquieren por experiencia propia o bien por transmisión de la experiencia de los demás.

Cada vez que pienso en la estratégia no puedo evitar pensar en una partida de ajedrez, en la que el objetivo del juego, o más bien **su visión**, es por medio de unos recursos, las piezas del tablero y un set de movimientos en el tiempo que conforman los distintos turnos, **tumbar a el rey** del oponente.

Lo primero que aprendí fueron las reglas del juego, con las que me definía como un jugador de ajedrez, mi **misión**. Simplemente con esto me lanzaron al campo de batalla y comenzó por aquel entonces ardua tarea de derrocar al rey rival, aunque más bien se convertiría en un intento por sobrevivir.

Una a una iba perdiendo mis piezas, y con ellas la posibilidad de vencer. Aunque el otro jugador y yo supiéramos las mismas reglas algo no encajaba, mis movimientos, que más que razonados parecían al azar, me conducían paso a la derrota, mientras que los suyos impedían el avance de mis tropas.

Al final de la partida me reveló el porqué de mi derrota, movía cada pieza sin un rumbo definido, sin un **objetivo en común**, no utilizaba los recursos de los que disponía como un **equipo**, sino como piezas individuales a las que medía un valor numérico definido en las reglas. Por otra parte, reconoció que muchas de las jugadas que yo había hecho las había vivido en otras partidas previas, por lo que podía intuir y posicionarse diferentes posibles **situaciones estratégicas** que le favorecían.

Cuando investigué sobre solo encontraba información referente al plan estratégico empresarial, pero al igual que con el ajedrez, esto mismo puede

reflejarse a más ámbitos de la vida cotidiana. Hace relativamente poco realizamos una actividad que nos planteaba realizar un plan estratégico personal para los próximos cuatro años. En la que tuvimos que reflexionar sobre nuestra misión, visión, valores y objetivos estratégicos.

La actividad fue algo fuera de nuestra **zona de confort** y nos impactó tener que realizar una valoración personal sobre nosotros mismos. Los valores eran algo más trivial dado que es lo que nos constituye como individuos, pero el tener que definir una visión a **largo plazo** fue una tarea ardua y abstracta. Una vez hecho esto, se nos requería definir los objetivos estratégicos para cumplir dicha tarea, los cuales no fueron fáciles de definir al tener que detallar el **cómo** actuar para alcanzar dicho objetivo y poder **medir** nuestro avance.

En lo que a mi respecta, creo que hacer este tipo de actividad es beneficiosa, no solo para las empresas, sino para cualquier ámbito de la vida, incluido el personal, dado que nos ayuda a definir un objetivo y establecer las estrategias para hacerle jaque mate de forma eficaz.