LA IMPORTANCIA DE LA GESTIÓN DE RIESGOS Y SEGURIDAD EN EL INTERNET DE LAS COSAS (IOT)

Molina García Jorge Alberto,
Cundinamarca, Universidad Piloto de Colombia
Bogotá, Colombia
jorge-molina1@upc.edu.co

***Resumen*—** Este artículo pretende resaltar la importancia de la gestión de riesgos en el internet de las cosas (IOT), debido a la relevancia que va tomando en la vida cotidiana y en las organizaciones. La constante evolución del IOT hace necesario que las organizaciones deban contemplar estrategias para mitigar los posibles impactos que generen problemas de ciberseguridad y privacidad de la información de los usuarios, que puedan afectar la continuidad del negocio.

***Abstract*—** This article pretend to stand out the importance of consider the risk management in the internet of things (IOT), due to the relevance that it is taking everyday in organizations. The constant evolution of the IOT makes it necessary for organizations to contemplate strategies to mitigate the possible impacts that may arise, generating problems of cybersecurity and privacy of user information that may affect business continuity.

***Índice de Términos*—** IOT (Internet de las cosas), Riesgos, Seguridad la información, OWASP (Open Web Application Security Project).

I. INTRODUCCIÓN

El propósito de este documento es resaltar la importancia de incluir en la gestión de riesgos de las organizaciones, los procesos y dispositivos que usen IOT. En los últimos años se presentó una constante evolución en esta tecnología y para las organizaciones debe ser necesario considerar dentro de su sistema de seguridad de la información, planes y controles para tratar los riesgos de ciberseguridad que esta trae consigo.

El IOT se convirtió en parte de la vida cotidiana de los usuarios, ya que se puede ver presente en hogares, el internet de los vehículos (IoV), dispositivos de salud entre otros, lo que lo convierte en una parte muy importante de la transformación digital, pero paralelamente, también trae de la mano nuevos ataques y amenazas de ciberseguridad.

Aunque en las organizaciones se realiza un análisis de riesgos basado en diferentes normas como ISO3100 o RISK IT, el principal desafío que tendrán con IOT es su crecimiento acelerado, por tanto, se debe abordar la seguridad desde un enfoque de arquitectura, basado en políticas y aplicándola a las implementaciones de IOT desde el principio.

II. INTERNET OF THINGS (IOT)

Antes de tratar las amenazas y riesgos que trae consigo IOT, es necesario que se entienda el concepto de IOT y se conozcan sus características para que se tenga un mejor panorama de la importancia que está tomando en la cotidianidad de la sociedad.

Una interesante definición de IOT proviene del Instituto Europeo de Normas de Telecomunicaciones (ETSI). Se refiere a IOT como "*Una infraestructura de red global dinámica con capacidades de autoconfiguración, donde las cosas físicas y virtuales tienen identidades, atributos físicos y personalidades virtuales y utilizan interfaces inteligentes para conectarse entre sí y con las redes de datos*" [1].

Adicionalmente, la definición de IOT de la Unión Internacional de Telecomunicaciones (UIT) en su recomendación UIT Y.2060. afirma que una IOT "*Es un objeto del mundo físico (cosas físicas) o del mundo de la información (cosas virtuales), que es capaz de ser identificado e integrado en las redes de comunicación*" [2].

Es necesario resaltar que el IOT junto a otras tecnologías como cloud computing, Big Data, automatización, ciberseguridad y colaboración, se convirtieron en las bases de la transformación digital. Así mismo, con el uso de IOT es posible reducir costos y adicional generar nuevos ingresos mediante un mejor uso de los dispositivos, por otra parte, se cuenta con mayor eficiencia de la cadena de suministros y logística. Pero lo que se considera uno de los mayores aportes de IOT, es la posibilidad de automatizar gran parte de las tareas que actualmente requieren mucha intervención humana o consumen demasiado tiempo, simplificando los procesos relacionados.

En este mundo hiperconectado la informática de bajo costo, big data, la nube, las tecnologías de dispositivos móviles entre otros, pueden compartir y recopilar información con una mínima intervención humana. Los sistemas digitales pueden grabar, supervisar y ajustar cada interacción entre los dispositivos conectados. La recolección de datos personales de los usuarios está ligada al funcionamiento de los dispositivos

de IOT, lo anterior sin que se tenga en cuenta el nivel de consciencia que tiene el usuario en cuanto a la información personal que comparte con el uso de estos servicios, lo que trae consigo problemas de seguridad.

El entorno de tecnología de IOT abarca sistemas como redes de comunicación, hardware y software de dispositivos, plataformas, aplicaciones, entre otros, es por esto que se puede decir que existe un gran número de dispositivos que utilizan IOT, dentro de los que se resaltan relojes, neveras, alarmas de humo, bombillas, carros etc., en pocas palabras una cantidad importante de objetos pueden estar conectados a internet, por esta razón, es necesario que se tenga en cuenta diferentes medidas de protección, y adicional se deben poseer capacidades para manejo y análisis de la seguridad de los datos, con el fin de que se aproveche la unión entre los dispositivos y el internet. Con más de 7.000 millones de dispositivos de IOT conectados en la actualidad, los expertos prevén que este número aumentará hasta llegar a 10.000 millones en 2020 y a 22.000 millones en 2025[4].

En los últimos años se consiguieron avances en tecnología importantes que permitió la evolución de IOT y lo convierten en una realidad. Dentro de los avances de tecnología se pueden resaltar los siguientes:

1)*El acceso a tecnología de sensores de bajo coste y baja potencia*. Los sensores asequibles y fiables hacen que la tecnología de IOT sea posible para más fabricantes.

2)*Conectividad*. Un conjunto de protocolos de red para internet permite una conexión de sensores a la nube y a otras "cosas" para conseguir una transmisión de datos eficiente.

3)*Plataformas de Cloud Computing*. El aumento de la disponibilidad de las plataformas en la nube permite que tanto las empresas como los consumidores, accedan a la infraestructura que necesitan para ampliar la capacidad sin tener que gestionarlo todo.

4)*Machine learning y analítica*. Con los avances en machine learning y en analítica, junto con el acceso a enormes cantidades de datos de una gran variedad almacenados en la nube, las empresas pueden reunir información más rápido y de forma más sencilla. El surgimiento de estas tecnologías relacionadas sigue ampliando los límites de IOT, y los datos producidos por IOT también retroalimentan estas tecnologías.

5)*Inteligencia artificial (IA) conversacional*. Los avances en redes neuronales llevan el procesamiento de las lenguas naturales (NLP) a los dispositivos de IOT como, por ejemplo, los asistentes personales Alexa, Cortana y Siri, que los convierten en dispositivos atractivos, asequibles y viables para el uso doméstico [4].

Las empresas que utilizan dispositivos como sensores en sus procesos, pueden adaptarse de mejor forma a IOT, dentro de los tipos de empresa que utilizan estos dispositivos se destacan las siguientes:

A. Empresas de fabricación

Las empresas dedicadas a fabricar productos pueden alcanzar una ventaja contras sus competidores mediante la supervisión constante de la línea de producción, y de esta forma, tener la capacidad de realizar un mantenimiento preventivo en los equipos cuando se detecta un posible fallo, dado que los sensores permiten medir de manera eficaz los momentos cuándo la capacidad de producción presenta afectación. Si adicional a lo anterior, las organizaciones realizan configuración de alertas de los sensores, los fabricantes pueden reaccionar rápidamente y revisar los equipos para realizar su corrección o aislarlos de la operación hasta que estén reparados. Esto permite que se reduzcan los costos operativos, se obtenga mejor tiempo de actividad y se mejore la gestión del rendimiento de los activos.

B. Industria automovilística

La industria automovilística puede conseguir grandes ventajas con el uso de IOT, ya que adicional a los beneficios en los procesos de fabricación, los sensores pueden monitorear vehículos que ya están en la carretera y detectar fallos inminentes, lo que permite informar al conductor de forma oportuna sobre lo que está ocurriendo, y adicional se pueden generar recomendaciones. Gracias a la información reunida por las aplicaciones basadas en IOT, los fabricantes y proveedores de automóviles pueden obtener más información sobre cómo están funcionando los vehículos e informar de ello a sus propietarios.

C. Transporte y logística

Los sistemas de transporte también se benefician de las aplicaciones de IOT, ya que con la información obtenida de los sensores pueden recalcular las rutas según las condiciones climáticas, o percatarse si existen inconvenientes con el traslado de mercancías, tales como fallos en los medios de transporte, y de acuerdo a esto toman las medidas pertinentes para sortear los impases. El propio inventario podría estar equipado también con sensores para el seguimiento y localización para supervisar el control de la temperatura. Las industrias de alimentos y bebidas, flores y productos farmacéuticos, a menudo llevan un inventario sensible a la temperatura, por tanto, se beneficiarían enormemente de las aplicaciones de supervisión de IOT que envían alertas cuando las temperaturas suben o bajan hasta un nivel que supone una amenaza para el producto.

D. Sector público

Un ejemplo de los beneficios que tiene el sector público con el uso de IOT es la posibilidad que se tiene para notificar a los usuarios de cortes masivos en los servicios básicos como son agua, electricidad o alcantarillado. Las aplicaciones de IOT pueden recolectar información sobre el impacto de una falla y de acuerdo a esto, tomar las medidas necesarias para recuperar el servicio en el menor tiempo posible generando el menor impacto en la población.

E. Atención sanitaria

Una de las muchas ventajas que puede tener el sector médico con el uso de aplicaciones de IOT, es el monitoreo de activos. Con frecuencia los médicos, enfermeros y asistentes requieren saber con exactitud la ubicación de un dispositivo que ayude a un paciente, dentro de los cuales se pueden destacar aparatos como las sillas de ruedas, muletas, camillas entre otros. Si las sillas de ruedas, las muletas y las camillas

tienen sensores de IOT, se puede hacer un seguimiento, de tal forma que sea mucho más eficiente la búsqueda. Muchos otros activos de un hospital se pueden rastrear de esta forma para garantizar su uso apropiado, y adicional se puede tener un inventario de los activos.

F. Seguridad general en todas las industrias

Las aplicaciones de IOT no solo se pueden usar para rastrear activos físicos, o para reaccionar de manera oportuna a posibles fallas, también se pueden utilizar para trasmitir información a los empleados que poseen trabajos de alto riesgo, de forma oportuna, un ejemplo de ello son los trabajadores de minas, trabajadores en yacimientos de petróleo, centrales eléctricas, plantas químicas, con estas aplicaciones se les pueden informar de manera oportuna sobre la ocurrencia de un incidente mayor, ya sea para que se auxilie a un compañero, o se pueda contener un fallo de manera que no se vuelva una catástrofe. Otra forma de uso, se daría en el monitoreo del estado de salud de las personas de forma constante, que les permita tomar decisiones acertadas en momentos críticos. En fin, se tienen muchas ventajas en el uso de IOT en seguridad general de todas las industrias [4].

Como se puede ver la revolución de IOT tiene la capacidad de generar una transformación a niveles muy altos, pero al mismo tiempo, puede ser altamente perjudicial para las organizaciones. El valor de las empresas y la competitividad organizacional se pueden obtener a medida que se aprovechan estas nuevas capacidades para obtener más y mejor valor comercial de los dispositivos IOT. Con ese valor adicional viene un riesgo adicional, o al menos, nuevas vías de riesgo. Los dispositivos que se encuentran todo el tiempo conectados a la red, se convierten en objetivos para la posible divulgación de datos y la delincuencia, dado que están expuestos a ataques que posiblemente no se han visto en el pasado.

Con lo descrito anteriormente se ve la importancia que tiene IOT y la razón del porque es imperativo que las organizaciones tomen acciones dentro de sus sistemas de seguridad de la información, teniendo en cuenta el potencial que tiene IOT para redefinir la ecuación de riesgo.

II. IOT EN COLOMBIA

Como se mencionó, IOT trae consigo muchas aplicaciones en diferentes sectores, por tanto, Colombia no es ajeno a explorar todas las ventajas que ofrece esta tecnología. Una encuesta de opinión realizada por la ANDI, mostro el interés de los empresarios colombianos por el Internet de las Cosas (IOT) y por la transformación digital en general. Sin embargo, un 56,3% de los consultados no conoce bien las aplicaciones de IOT y un 78,5% considera importante promover su uso en las empresas [20].

Las empresas colombianas tienen una gran oportunidad para transformarse al utilizar IOT; dentro de los cuales se destacan el poder monitorear sus despachos, conocer el estado real de sus activos, tomar acciones antes de que se generen fallas y redefinir el negocio con nuevas y mejores opciones para que los usuarios aprovechen al máximo los servicios que ofrecen, siendo el momento perfecto para innovar y cambiar los paradigmas, así lo aseguró, Jorge Arias, Gerente General de Oracle para Colombia y Ecuador.

En febrero del presente año se realizó el "*Oracle IOT Tour*" en Colombia, un evento donde se mostraron distintas soluciones que utilizan esta tecnología para aumentar la eficiencia, mejorar la productividad y brindar mayor seguridad dentro del sector industrial. Durante la actividad se exhibieron casos de uso integrados a "*Oracle Internet of Things Cloud*", que ofrece un excepcional conjunto de funciones para empresas de diferentes rubros y tamaños [19].

Durante el evento, se presentaron algunas de las soluciones que ha diseñado Oracle y que implementan el internet de las cosas para las organizaciones en el país. Aquí algunas de ellas:

1)*Trabajador conectado*: las empresas pueden tener mayor control del estado y la seguridad de los trabajadores, mediante el uso de la aplicación Internet of Things Connected Worker creada por la empresa de origen estadounidense y el partner-ConectSen.

La app, en combinación con sensores ubicados en los cascos de los trabajadores o en wearables, permite seguir en tiempo real la ubicación de los colaboradores, para evitar que accedan a zonas de peligro. Esta también permite el envío de alertas para prevenir accidentes en terreno, o la creación de geocercas (perímetro virtual en un mapa) que delimitan el espacio seguro por donde puede transitar un trabajador, entre otras.

2)*Monitoreo de flota*: en transportes, público y privado, el IOT puede mejorar los procesos a niveles nunca antes imaginados.

Las aplicaciones de monitoreo de flota fueron expuestas en el evento por medio de una pista de carros a escala, donde los asistentes pudieron apreciar la funcionalidad de Oracle Internet of Things Fleet Monitoring Cloud Service, con la cual se puede obtener información precisa y actualizada sobre la flota de vehículos en cualquier parte del mundo y recopilar datos que determinan la disponibilidad de flotas, activación de viajes, gastos en combustible, medir la velocidad de los camiones, prevenir infracciones y resguardar la seguridad del conductor.

Esta solución no sólo se puede utilizar en el sector privado, sino que tiene un gran potencial en el sector público.

3)*Warehouse 4.0*: la solución, Oracle Warehouse Management Cloud, facilita a las empresas de todos los tamaños, liberarse de personalizaciones y actualizaciones, y ofrece velocidad y el ahorro de la nube, así como las mejores capacidades de optimización y gestión de almacenes. Esta permite integración con tecnologías emergentes como uso de drones, robots, IOT en el almacén, realidad aumentada entre otros, con el objetivo de reducir costos y ser más productivos.

4)*Planta inteligente*: con aplicación de Inteligencia Artificial, Machine Learning, y capacidades avanzadas de monitoreo y analítica, IOT Production Monitoring Cloud de Oracle permite a las organizaciones conseguir perspectivas significativas sobre el rendimiento de activos, máquinas,

trabajadores y vehículos de manera que se pueda optimizar su cadena de suministro, manufactura y logística, reducir el plazo de comercialización para los nuevos productos y permitir nuevos modelos empresariales [19].

IOT está tomando mucha fuerza en Colombia, un claro ejemplo es el lanzamiento realizado por Telefónica Movistar en el mes de septiembre del presente año, de la red de internet de las cosas en LTE, de acuerdo con la compañía, es la primera de este tipo en funcionar en el país.

Lo que hizo Telefónica fue abrir un espacio exclusivo en el espectro (como una autopista) para que por allí viajen los datos de estos objetos de manera eficiente. Esto quiere decir que la información de los dispositivos conectados a IOT no tendrá que luchar por un espacio en la red con las comunicaciones de celulares o de equipos de cómputo.

La implementación de esta red trae consigo muchas ventajas, por ejemplo, una ciudad podrá controlar en vivo todos sus postes de luz (a qué horas iluminan y qué tanto iluminan) en tiempo real desde un centro de control. Lo mismo ocurre con otros sectores o industrias como el agrícola, que podría controlar los sistemas de riego, transporte, semaforización, entre otros.

De acuerdo con Telefónica Movistar, en Colombia ya hay 700 nodos instalados que permiten la conexión de 600 mil dispositivos y el 50 % de las vías del país a la red de IOT. Según las estimaciones de la compañía, para 2025 habrá 25,2 miles de millones de objetos conectados a IOT en el mundo. Lo anterior genera mayor velocidad y eficiencia en la gestión de los equipos conectados a IOT, lo que se traduce en reducción de costos para las empresas mediante la toma de decisiones productivas.

Por ahora, esta red de IOT está disponible solo en algunos lugares de Colombia. Sin embargo, Carolina Navarrete, directora de B2B de Telefónica Movistar, afirmó que para finales de 2020 ya se habrá desplegado este servicio en el 100% de los territorios donde la compañía tiene cobertura [21].

Otro avance importante que se presentó en Colombia es la apertura en el mes de octubre del presente año, del primer laboratorio para emprendedores, creado por Telefónica Movistar y Wayra. El objetivo de este espacio es brindar a los diferentes actores del ecosistema emprendedor colombiano un ambiente propicio para desarrollar aplicaciones y herramientas con base en tecnología IOT y que se puedan probar sobre una red exclusiva [19].

Al laboratorio pueden asistir los diferentes actores del ecosistema emprendedor de Wayra y CEmprende al que estas tecnologías le apliquen dentro de su línea de negocio. Se recrea allí el ambiente operativo de las conectividades LPWA (Low Power Wide Area), con los siguientes componentes: un nodo habilitado con Narrow Band-IOT/LTE, SIM Cards con perfil NB-IOT/LTE-M, chipset que soportan tecnología LTE para IOT, módulos de comunicaciones que permitirán realizar interacciones a través de NB-IOT/LTE-M, kit de desarrollo de software y hardware basados en NB-IT/LTE-M. Adicionalmente en el laboratorio de IOT se crearán espacios de capacitación para los emprendedores donde podrán avanzar en temas de desarrollo de soluciones IOT, contarán con material de formación para las interacciones con los dispositivos dispuestos allí y el apoyo de personal capacitado. Este espacio es una caja de herramientas para que los emprendedores se apropien de la tecnología IOT y puedan innovar y experimentar con ella, además de desarrollar, profundizar o escalar sus soluciones basadas en Internet de las Cosas en la red LTE-M o NB [22].

Es necesario resaltar que Colombia cuenta con el Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IOT) que es una iniciativa impulsada desde el Ministerio de las TIC, con el apoyo de Colciencias, y corresponde a una estrategia que busca posicionar a Colombia como líder regional en TIC. Este centro tiene como misión el desarrollo de productos y servicios innovadores basados en IOT para un mayor bienestar de la sociedad y una mayor competitividad de la economía nacional, adicional también busca el fortalecimiento del ecosistema de innovación y emprendimiento en IOT para la proyección del país a nivel internacional.

Las líneas de trabajo priorizadas por el Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IOT) están alineadas con las metas del Plan Vive Digital 2014-2018 de Colombia, el cual busca que el país de un gran salto tecnológico mediante la masificación de Internet y el desarrollo del Ecosistema Digital Nacional. El Plan Vive Digital se estructura alrededor de 4 ejes: servicios, aplicaciones, infraestructura y usuarios.

Así mismo, las líneas de trabajo del Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IOT) están alineados con el Plan Nacional de Transformación Productiva (PTP), el cual define como áreas prioritarias: Manufacturas (textiles y confecciones), Agroindustria (hortofrutícola, acuícola y lácteos), y Servicios (Software & TI).

De acuerdo con lo anterior el CEA-IOT se especializa en las siguientes líneas de investigación y desarrollo: salud, logística, industria, vestibles, seguridad, agroindustrial y gobierno [23].

Los primeros proyectos que tuvo el Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IOT) fueron los siguientes:

1)*Sector salud*: Con el hospital San Ignacio, se desarrolla un proyecto para dar de alta de manera anticipada a algunos pacientes, para que en lugar de estar en observación en el hospital con los altos costos que implica, puedan estar en una su casa monitoreados desde el hospital.

También con el hospital San Ignacio se ejecuta un proyecto con sensores que permiten monitorear las condiciones del ambiente como humedad, temperatura, entre otros, para automatizar el cumplimiento de los estándares nacionales e internacionales en la materia.

2)*Sector logístico*: Con la zona franca Bogotá se trabaja un proyecto que permite medir la trazabilidad de los productos, desde que están en puerto hasta que llegan a las locaciones de zona franca, redundando en mayor productividad y seguridad.

3)*Industria:* Con Totto, se avanza en la investigación para desarrollar un morral inteligente, que permita ser ubicado en caso de pérdida, y que pueda monitorear los insumos que lleva adentro [24].

Como se puede ver en Colombia cada vez toma más fuerza el uso de IOT, y tanto el gobierno, como las empresas son conscientes de ello, sin embargo, es necesario que se tenga prioridad sobre la seguridad de estos dispositivos, ya que como se vio en otros países, se pueden presentar ataques de denegación de servicio explotando las debilidades de dispositivos del IOT.

III. RIESGO Y MITIGACIÓN DEL RIESGO

Para hacer de forma más eficaz la gestión de riesgos es necesario entender que esta implementación crea y protege el valor de la organización, y hace parte integral de todos los procesos que se tienen implementados, adicional, facilita la mejora continua. Para que la gestión del riesgo tenga resultados eficientes, consistentes y confiables debe ser sistemática, estructurada y oportuna, y se debe basar en la mejor información disponible (Datos históricos, experiencias, retroalimentación etc.) y de esta forma permitir a los encargados de la toma decisiones hacer elecciones informadas y priorizar temas. La gestión de riesgos debe ser transparente, inclusiva y adaptativa (contexto interno y externo) y debe considerar los factores humanos y culturales.

Actualmente se vive en un mundo digital que se encuentra en constante evolución, en donde no solo los PC portátiles, tablets, smartphones están conectados a internet, sino también gran cantidad de dispositivos diferentes, que van desde botellas de píldoras y sombrillas, hasta refrigeradores, relojes y automóviles. Esto implica un mayor riesgo inmediato de seguridad para las personas, los hogares y las empresas, que el riesgo causado por las tecnologías actuales.

La necesidad de poder construir edificios inteligentes que hagan un uso mucho más eficiente de la energía, con el fin de optimizar el uso de los recursos naturales, trae consigo el uso de nuevas tecnologías, las cuales se encuentran habilitadas para estar conectadas a redes de comunicación, no solo de manera local, sino que también se están integrando en sistemas fuera del perímetro de cada edificio, creando una red inteligente. Muchos de estos dispositivos inteligentes habilitados para internet no cuentan con una seguridad optima, lo que los convierte en blanco de ataques que podrían interrumpir el uso u operaciones normales y crear problemas de seguridad. Este es un problema crítico que se debe resolver.

A medida que aumenta la cantidad de dispositivos que pueden conectarse entre sí, también aumenta la cantidad de personas maliciosas que tienen como objetivo intentar comprometer estos dispositivos o ganar dinero causando estragos. Por ejemplo, los sistemas de gestión de edificios débilmente protegidos conectados a internet, son vulnerables y se encuentran expuestos a que un atacante entre en un sistema conectado a la misma red, pero fuera del objetivo original y realice actividades malintencionadas. Es por esta razón que los sistemas de seguridad se deben desarrollar de la misma manera y al mismo ritmo que todos estos nuevos sistemas inteligentes.

La amenaza que se observa actualmente no se basa solo en que un atacante pueda acceder a la red de una casa, o al sistema de gestión de un edificio, y genere interrupciones en los servicios, otro impacto potencial que existe es sobre la infraestructura tecnológica, y puede resultar en el acceso a información crítica ya sea de una persona o una organización, lo cual se puede ocasionar por una segmentación indebida entre la red de automatización y la red de seguridad de la infraestructura.

Normalmente los sistemas de gestión de hogares y edificios no se consideran dentro de los sistemas de TI; por esta razón no se monitorean, ni se supervisan por un oficial de seguridad de la información, y durante un largo tiempo se consideró tecnología operativa que se encuentra bajo la administración de diseñadores de instalaciones. Es claro que esto debe cambiar en el corto plazo, dada la importancia que está tomando el uso de dispositivos con IOT tanto en hogares como en organizaciones. No cabe duda que actualmente se tiene la necesidad que los diseñadores de instalaciones, los administradores y los expertos de TI deban trabajar juntos para identificar y mitigar los riesgos potenciales de seguridad. El IOT ofrece a las organizaciones muchas ventajas que permiten aprovechar la tecnología para conducir a un mañana mucho mejor. Pero no se recomienda centrarse solo en la seguridad de los datos y dejar de lado el comportamiento de las personas vinculadas al uso de aplicaciones de IOT, ya que estos pueden crear importantes riesgos de privacidad y seguridad.

Actualmente se puede decir que los dispositivos que usan tecnologías en IOT no son totalmente interoperables y por el momento no se tiene una arquitectura estandarizada. Sin embargo, es solo cuestión de tiempo antes que esto cambie, por consiguiente, los expertos en seguridad y control de la información deben comenzar a adaptar sus políticas de seguridad a esta tecnología.

Es claro que para las organizaciones el uso de dispositivos con aplicaciones de IOT genera beneficios financieros, de salud, seguridad y de calidad de vida, sin embargo, también está expuesta a nuevos riesgos potencialmente altos. Los escenarios de riesgo difieren entre las empresas que fabrican y venden sistemas embebidos con capacidad de comunicación y las empresas que son usuarios de estos dispositivos.

Para evaluar de una forma integral los riesgos que trae consigo la adopción de IOT, es de vital importancia considerar numerosas áreas de riesgo comercial, operativo y técnico, para equilibrar los beneficios comerciales descritos. Tal como se observa en la figura 1[9], a medida que aumentan los nuevos riesgos, los beneficios potenciales de negocio disminuyen.

Para analizar los riesgos de usar dispositivos con IOT es necesario tener en cuenta los riesgos del negocio, riesgos operacionales y riesgos técnicos.

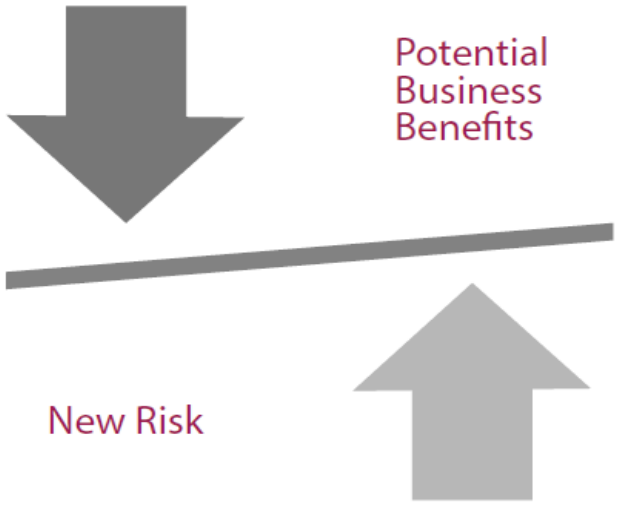

Fig.1 Gestión integral de riesgos [9]

Los riesgos del negocio se basan en el manejo de los siguientes aspectos:

1)Salud y seguridad.

2)Cumplimiento normativo.

3)Privacidad del usuario.

4)costos inesperados.

Para los riesgos operacionales se tienen los siguientes aspectos relevantes:

1)Acceso inapropiado a la funcionalidad.

Dentro de los riesgos técnicos se destacan los siguientes aspectos:

1)Vulnerabilidades del dispositivo.

2)Actualizaciones de dispositivos.

3)Gestión de dispositivos.

A continuación, se describe los aspectos relevantes mencionados anteriormente que afectan los riesgos de negocio, riesgos operacionales y riesgos técnicos.

A. Riesgo del negocio o comerciales

Si se enfocan los riesgos de negocio más significativos, se observa que el mayor impacto se puede tener en las organizaciones de la salud, ya que el bien más preciado, la vida, depende del funcionamiento de un dispositivo como un marcapaso o un desfibrilador, y si este se ve expuesto a ataques inalámbricos puede traer consecuencias letales.

Otros ataques sobre dispositivos que usan IOT que pueden atentar contra la integridad del ser humano, se presentan en la industria automotriz, ya que si el atacante logra acceder a la consola de manejo de un vehículo es possible desactivar los sistemas de frenado de un automóvil cuando está en movimiento, lo cual puede llevar a una tragedia.

Un factor de gran importancia que se presenta en los riesgos de negocios es la privacidad de los datos, y un ejemplo notable de ello se puede ver en los sistemas de monitoreo de hogares. La función principal de estos sistemas de monitoreo es proteger los bienes y habitantes del hogar, pero se puede ver expuesta la información que recolectan debido a que si no se toman las medidas pertinentes se encuentran vulnerables a los ataques inalámbricos comprometiendo la privacidad de los datos. Un ejemplo que se puede mencionar son los monitores que se usan para cuidar los bebes, los cuales se instalan en las habitaciones para controlar al niño de forma remota, si no se realizan las configuraciones de seguridad de manera pertinente, es decir cambiar configuraciones por defecto, agregar contraseñas fuertes, entre otras, la información de los niños puede ser hackeada por personas no autorizadas y difundidas en la red o manipuladas, lo cual se considera que viola el principio de confidencialidad en la seguridad de la información, y esto puede traer consigo consecuencias muy graves. Por tanto, al igual que los desafíos de cumplimiento, los impactos en la privacidad deben evaluarse antes de la implementación.

Adicional a los riesgos para la salud, la seguridad y la privacidad, también es posible tener riesgos por regulación, lo cual puede variar dependiendo de cada país. Los riesgos por regulación se pueden presentar cuando no se manipulan correctamente los siguientes componentes informáticos:

1)Procesar indebidamente datos potencialmente confidenciales.

2)Incumplir con los procesos comerciales regulados por la normativa.

3)Manipular de forma incorrecta infraestructura crítica de impacto.

Los mandatos reglamentarios a menudo no son claros en el manejo de dispositivos que utilizan tecnología IOT, lo que tiene como consecuencia que sea complejo el manejo de estos dispositivos dado que no se conoce de manera específica como se debe regular, y esto hace que se deba evaluar muy bien el costo beneficio, que pueda generar el incluir dispositivos de este tipo a la red de comunicaciones de las organizaciones. Por lo tanto, los profesionales deben evaluar si la conexión de un dispositivo a la red, agrega suficiente valor comercial para justificar posibles aumentos en el riesgo.

B. Riesgo operacional

Adicional a los riesgos del negocio, se debe dar prioridad a los riesgos operativos en un sistema integro que usa tecnología IOT. Por ejemplo, se debe realizar la configuración o configuraciones adecuadas para que la comunicación entre dispositivos solo permita acceso al personal autorizado, y no se permita cambios en la configuración no deseados ni fuga de información. En la mayoría de casos esto requiere tener planificación operativa, y adicional, se tiene que vincular con los controles de seguridad y monitoreo existentes, para garantizar que el nivel de acceso sea apropiado.

Otro desafío desde una perspectiva operativa, que se puede presentar, es el conocimiento de esta tecnología (IOT) por parte del personal que será el encargado de realizar las configuraciones, monitoreo, aseguramiento y mantenimiento de los dispositivos. Si no se tiene una supervisión centralizada y una gobernanza adecuada, esto puede tener un impacto perjudicial significativo en el uso de IOT, lo cual trae como consecuencia que las organizaciones asuman riesgos sin

saberlo, que están fuera del nivel deseado.

C. Riesgo técnico

Los riesgos a nivel técnico en IOT tienen un conjunto de desafíos más complejo que la TI tradicional. Los dispositivos que utilizan IOT al igual que los dispositivos informáticos tradicionales, se encuentran expuestos a ataques que pueden traer como consecuencia la interrupción del servicio o pueden verse comprometidos por un malware. Dado que los dispositivos IOT funcionan de forma bidireccional, están conectados a una red(Internet), y adicionalmente no está definida de forma clara la responsabilidad administrativa, esto los convierte en objetivos potenciales para las personas con intereses maliciosos, por lo anterior se convierte en una tarea compleja mantenerlos seguros.

Los ataques contra dispositivos IOT son un desafío constante para los fabricantes. En algunas ocasiones, el camino para solucionar las fallas de seguridad requiere una actualización de hardware en lugar de modificaciones solo en el software. Esta dinámica puede exponer a las organizaciones que utilizan dispositivos IOT a ataques, con una capacidad mínima para implementar medidas de control y aseguramientos. Incluso si una actualización de software remedia las vulnerabilidades encontradas, muy seguramente un nuevo ataque contra un dispositivo de hardware IOT será descubierto, es por estas razones que es muy importante que el personal de operaciones se mantenga al tanto de esos desarrollos, e implemente políticas de seguridad para responder.

Si se enfoca en la administración de dispositivos de IOT, se encuentra que muchas organizaciones no están equipadas para extender los mecanismos de administración de seguridad existentes a estos dispositivos. Se deben evaluar aspectos como la realización de inventario de activos, el control de acceso al dispositivo, la ubicación del dispositivo en la red entre otros desafíos, de la misma forma que se consideran para los componentes de TI tradicionales.

Es necesaria la participación y el conocimiento de todas las partes involucradas para realizar el manejo de riesgos en los dispositivos de IOT. Las siguientes son algunas de las preguntas que los ingenieros encargados de seguridad de la información deben realizar a las partes interesadas cuando se considera la implementación de dispositivos IOT:

1)¿Cómo se utilizará el dispositivo desde una perspectiva empresarial? ¿Qué procesos comerciales son compatibles y qué valor comercial se espera generar?

2)¿Cuál es el entorno de amenaza para el dispositivo? ¿Qué amenazas se anticipan y cómo se mitigarán?

3)¿Quién tendrá acceso al dispositivo y cómo se establecerán y probarán sus identidades?

4)¿Cuál es el proceso para actualizar el dispositivo en caso de un ataque o vulnerabilidad publicados?

5)¿Quién es responsable de monitorear nuevos ataques o vulnerabilidades pertenecientes al dispositivo? ¿Cómo van a realizar ese monitoreo?

6)¿Se han evaluado y comparado todos los escenarios de riesgo con el valor comercial previsto?

7)¿Qué información personal es recopilada, almacenada o procesada por los dispositivos y sistemas IOT?

8)¿Las personas sobre las que se aplica la información personal saben que su información se recopila y utiliza? ¿Han dado su consentimiento para tales usos y colecciones?

9) ¿Con quién se compartirán / divulgarán los datos?

IV. SEGURIDAD IOT

Para realizar un plan de actividades para la seguridad de IOT, es necesario tener una visión general del ecosistema y a partir de allí abordar las normas, marcos y propuestas de regulación que se hallan generado. La figura 2[6] representa un ecosistema de IOT en donde la seguridad de la información forma parte integral.

Fig.2 Ecosistema de IOT [6]

Una repercusión positiva del ataque DDoS (Denegación de Servicio) a Dyn recibido el 21 de octubre del 2016 en donde se observaron que vulnerabilidades sobre IOT pueden traer consigo pérdida de datos y servicio, fue el lanzamiento de principios y directrices para asegurar IOT por parte del Departamento de Seguridad Nacional (DHS) de los Estados Unidos. Estas directrices no fueron legalmente obligatorias, pero fueron sin duda un signo de un buen comienzo hacia la seguridad de los dispositivos [6].

Algunas de las siguientes directrices son bien conocidas por la mayoría de profesionales de seguridad de la información, dentro de las cuales se destacan las siguientes:

1)Aprovechar la seguridad de la fase de factibilidad.

2)Aplicar actualizaciones de seguridad, correcciones y gestión de vulnerabilidades.

3)Seguir las prácticas de seguridad probadas.

4)Priorizar los controles basados en la magnitud o el impacto.

5)Proporcionar supervisión y adecuada gobernanza de la IOT.

6)Conectar el dispositivo fuera de la red si no hay una necesidad absoluta de negocio.

El Consorcio Industrial de Internet, compuesto principalmente por empresas relacionadas con IOT, desarrolló en 2016 el IISF (Industrial Internet Security Framework), que describe las mejores prácticas para ayudar a los desarrolladores y usuarios finales a evaluar el riesgo de IOT y posibles medidas de defensa contra estos. A principios de 2017, la Comisión Federal de Comercio de los Estados Unidos (FTC,

por sus siglas en inglés) anunciaba que estaba otorgando premios en dinero a cualquier persona que desarrolle una herramienta innovadora que tuviera la capacidad de detectar y proteger los dispositivos del hogar de vulnerabilidades del software [6].

Otro desarrollo que se presentó en el marco de la seguridad IOT fue la necesidad de integración de estos dispositivos con los dispositivos ya existentes, tal fue el caso del marco de seguridad Sigma Designs S2, que formaba parte de cada dispositivo IOT certificado por Z-Wave, donde cada dispositivo que se fabricara después de marzo de 2017 sería compatible con versiones anteriores en los chipsets Z-Wave IOT existentes, lo que hace que los dispositivos sean más seguros [6].

Sin embargo, implementar en dispositivos IOT una política de seguridad correcta puede ser una tarea complicada debido al desconocimiento. Esto afecta a los consumidores, pero en mayor medida a los desarrolladores y fabricantes. La fundación OWASP, que tiene como objetivo apoyar a las empresas y organizaciones en la concepción, desarrollo, operación y mantenimiento de aplicaciones confiables a nivel de seguridad, con su proyecto enfocado en IOT, pretende concienciar sobre estos riesgos, apoyando a desarrolladores, fabricantes y consumidores en el despliegue y uso seguro de estas tecnologías.

A continuación, se detalla cada una de las vulnerabilidades recogidas por la fundación OWASP en la lista del último año:

1) ***Uso de contraseñas débiles o embebidas*****:** el uso de contraseñas que pueden ser fácilmente obtenidas mediante un ataque por fuerza bruta, que por defecto sean la misma para todos los dispositivos o que incluso estén públicas en Internet, son vulnerabilidades bastante arraigadas en las tecnologías IOT por su herencia de los sistemas de control. Esta es una de las vulnerabilidades más graves en el ámbito IOT, puesto que ya ha sido explotada, en ocasiones anteriores, con el fin de realizar ataques de denegación de servicio distribuido utilizando una red de bots formada por dispositivos IOT que tenían una contraseña por defecto en sus accesos. La solución a esta vulnerabilidad es bastante simple: utilizar contraseñas únicas entre dispositivos, asociadas a una cuenta o a un servicio de directorio activo, de tal manera que la contraseña no esté embebida en el dispositivo.

2) ***Servicios de red inseguros*****:** se deben evitar aquellos servicios de red innecesarios o inseguros que se ejecutan en los dispositivos en segundo plano y que están expuestos a Internet. Una explotación exitosa de las vulnerabilidades que pudiera haber en dichos servicios podría comprometer la confidencialidad, integridad o disponibilidad de los datos almacenados en el dispositivo o incluso permitir un acceso remoto al mismo. La solución pasa por la deshabilitación de aquellos servicios que no sean necesarios y la solución de problemas de seguridad en aquellos que sí lo sean.

3) ***Interfaces inseguras en el ecosistema IOT*****:** las herramientas externas a los dispositivos como interfaces web, API en el backend o servicios en la nube pueden estar configurados de una manera insegura, lo que comprometería los dispositivos y otros componentes que se gestionan a través de éstas. Adoptar medidas de control de acceso a dichas interfaces, filtrar las entradas y salidas de los servicios y asegurar las comunicaciones añadiendo algoritmos de encriptación son las medidas más efectivas para paliar el problema.

4) ***Falta de mecanismos de actualización seguros*****:** en este apartado se incluye la falta de mecanismos de validación de las versiones de firmware en los dispositivos, medios de transmisión inseguros, falta de mecanismos para evitar la vuelta a versiones previas y, por lo tanto, más inseguras y la falta de notificación sobre los cambios de seguridad que se incluyen tras cada actualización. En estos casos, siempre se recomienda que en el dispositivo a actualizar se revise la integridad del firmware, así como su procedencia antes de ser instalado, con el fin de evitar que versiones modificadas del firmware puedan ser instaladas.

5) ***Uso de componentes inseguros o desactualizados:*** el uso de componentes software y hardware inseguros u obsoletos pueden comprometer el dispositivo. La mayoría de los dispositivos utilizan componentes y librerías de terceros, sistemas operativos personalizados, así como componentes hardware de distintos fabricantes. Por ello, es importante asegurar que dichas librerías no están obsoletas o pertenezcan a una versión con vulnerabilidades conocidas, así como asegurar que los componentes hardware no provienen de un proceso de fabricación que ha sido comprometido. Se tiene como ejemplo los problemas que tiene Intel últimamente con las distintas vulnerabilidades en sus procesadores como Meltdown, Spectre o SPOILER.

6) ***Insuficiente protección de la privacidad:*** la manera con la que se manejan los datos del usuario almacenados en los dispositivos IOT y en su ecosistema actualmente es insegura, impropia y suele hacerse sin solicitar permiso. Una solución a este problema puede estar en establecer una política para la manipulación de los datos del usuario, de tal manera que solo se pueda acceder a lo que sea estrictamente necesario e informando siempre al cliente sobre a qué parte de su información se tiene acceso para cada servicio.

7) ***Falta de seguridad en el almacenamiento y transferencia de datos:*** es necesario utilizar algoritmos de cifrado cuando se manejan datos sensibles. También se debe llevar un control de acceso a los mismos dentro del ecosistema IOT. Por ejemplo, en las comunicaciones entre el interfaz web de un sistema domótico y los dispositivos que lo componen.

8) ***Inadecuada gestión de dispositivos:*** es necesario llevar a cabo controles de seguridad en los dispositivos de producción que incluyan, entre otros, la gestión de activos y actualizaciones, monitorización de los sistemas, políticas de desmantelamiento y borrado seguro de los dispositivos.

9) ***Configuraciones por defecto inseguras:*** las configuraciones por defecto de los dispositivos suelen ser inseguras. Por ello, es recomienda establecer configuraciones

enfocadas a proteger el sistema, aplicar políticas estrictas de filtrado de las conexiones y la gestión de permisos.

10) ***Falta de bastionado físico****:* incluye la falta de controles sobre el acceso físico al dispositivo, ya que si un atacante consigue este acceso las medidas de seguridad implantadas resultan inútiles. Para evitarlo se debe restringir el acceso físico a los dispositivos a personas autorizadas e implementar medidas adicionales de seguridad, como videocámaras o vigilantes de seguridad [14].

Un aspecto muy importante en seguridad es la regulación. En 2017, el gobierno de los Estados unidos aprobó la ley para el mejoramiento de la seguridad cibernética del internet de las cosas, que establece estándares de seguridad para los dispositivos IOT que los proveedores pueden vender al gobierno. La ley requiere que los proveedores de IOT garanticen que pueden reparar cualquiera de sus dispositivos con nuevas actualizaciones de seguridad, que no codificarán de manera rígida las contraseñas de sus dispositivos y que no venderán dispositivos que tengan vulnerabilidades conocidas.

Si bien la ley es un gran paso para fortalecer la seguridad IOT, en realidad solo protege al gobierno de las amenazas. Las empresas deberían priorizar la seguridad diaria del consumidor tanto como la del gobierno, pero este movimiento ha comenzado muy lentamente. Los proveedores de IOT como Amazon están creando soluciones de seguridad actualmente, pero todos sus productos aún se encuentran en las primeras etapas de desarrollo.

Algunos expertos en seguridad cibernética sugieren formar una asociación entre el gobierno y las comunidades de inteligencia y seguridad cibernética, lo que ayudaría a reforzar la seguridad de la tecnología. Juntos, pueden determinar el mejor conjunto de protocolos de seguridad para dispositivos IOT y convertir estas disposiciones en ley.

En Colombia la Comisión de Regulación de Comunicaciones (CRC) publicó, en agosto del 2016, un estudio denominado “Resumen recomendaciones normativas y regulatorias para promocionar contenidos y aplicaciones y el internet de las cosas”, en el cual analiza la situación del IOT en Colombia para ese momento; mostrando cifras del 2015, se reflejaba una inversión total de 124 millones de dólares, la mayor en dispositivos para el hogar, con 101 millones de dólares, seguida, en orden descendente, por dispositivos para vehículos, dispositivos de salud y *wearables*. Ahora, en el 2019 es notoria la masificación del uso de IOT en el país, y seguramente el cambio en el mercado desde las cifras del 2015 será notorio, por lo que se requiere un nuevo estudio del mercado que permita tener una perspectiva actualizada de la situación en Colombia [16].

En marzo del presente año, la CRC anunció que se encuentra trabajando en la “hoja de ruta para la modernización de las tecnologías móviles en Colombia”, lo cual debe incluir aspectos que beneficien el desarrollo del IOT y permitan su masificación en el país.

Fig.3 Evolución del número de dispositivos IOT [16]

Se calcula que el número de dispositivos IOT conectados alcanzará los 21 mil millones en 2025. La importancia de las tecnologías IOT, así como las ventajas que ofrecen en el día a día, es una realidad. Sin embargo, también presentan varios inconvenientes a tener en cuenta. La información que manejan estos dispositivos es cada vez más sensible o relevante, por lo que mantenerlos seguros resulta de vital importancia.

La defensa comienza a nivel de chip o hardware. El hardware en el que se construye el dispositivo IOT constituye la base para un dispositivo robusto y seguro. Esto es como establecer una base sólida cuando se está construyendo una casa para asegurar un producto final estable y sostenible. Se puede afirmar que el hardware del dispositivo es donde comienza el ciclo de vida y es también el momento adecuado para dirigir el proceso de seguridad en el camino correcto. Dentro las amenazas al hardware de un dispositivo IOT que se enfrentan se tienen que puede ser robado, modificado físicamente, reemplazado y clonado. Otros ejemplos de vulnerabilidad de hardware pueden incluir el uso de contraseñas predeterminadas, contraseñas débiles o las credenciales codificadas con código de seguridad y los circuitos integrados falsificados.

Sin embargo, la mejor contramedida para combatir las vulnerabilidades de hardware es regular el proceso de fabricación de un dispositivo IOT y de esta forma los fabricantes serán los únicos responsables de no adherirse a las normas. Hoy en día, no se tiene implicaciones legales si no se siguen los estándares, pero puede haber un retroceso en el nivel de la empresa en la adopción de un dispositivo IOT de calidad inferior. Esta adopción de tecnología de fabricantes que cumplan con los estándares puede evitar la mayoría de las vulnerabilidades de hardware y debilidades de software que pueden estar disponibles de forma inherente en dispositivos IOT. Si las vulnerabilidades de hardware no se manejan de forma adecuada y se toman las medidas pertinentes, el resto de los controles, metodologías, marcos, tiempo, recursos e inversiones para que los dispositivos IOT sean seguros no serán eficaces.

Otro aspecto al cual se le debe dar gran importancia son las amenazas al software o al firmware en los dispositivos IOT. Una de las principales amenazas de software que se tienen son las modificaciones o descompilaciones con el objetivo de extraer credenciales y apalancarse para realizar los ataques de

denegación de servicio. Algunas de las vulnerabilidades en el software que se tienen son las siguientes:

1) Código inseguro.
2) Contraseñas predeterminadas codificadas en disco duro.
3) Pruebas inadecuadas de software que conducen a puertas traseras.
4) Ausencia de autenticación fuerte.

Los dispositivos IOT también se encuentran expuestos a amenazas de red, dentro de los ataques más comunes se resaltan ataques de escucha espontánea, los ataques de man-in-the-middle (MiTM) y el robo de ancho de banda. Algunas actividades que se recomiendan para proteger los dispositivos contras las amenazas descritas anteriormente son:

1) Identificar e inventariar los dispositivos IOT en la organización y asegurarse de que estén integrados en el programa de gestión de activos empresariales.
2) Definir estándares y líneas base para la seguridad del dispositivo IOT basados en políticas y estándares empresariales.
3) Implementar los controles de seguridad necesarios para mitigar el riesgo de IOT.

Se recomienda ubicar todos los dispositivos IOT en una zona de red separada, realizando una segmentación, lo cual facilitaría la aislación en caso de que se presenten ataques o se tenga una violación de seguridad y de esta forma el resto de dispositivos de TI puedan continuar sus operaciones sin ningún impacto importante.

Si la segmentación y la zonificación no son factibles, se sugiere adoptar un modelo de red de software definido (SDN) que no sólo mejora la seguridad de IOT, sino que también ayuda a identificar la ubicación de la brecha en caso de ataques.

Otros controles que también se recomienda implementar en los dispositivos IOT son los que se aplican a la mayoría de dispositivos de la infraestructura de TI, tales como autenticación de dos factores, contraseñas más fuertes o autenticación basada en llaves.

El uso de autenticación de infraestructura de claves públicas (PKI) para la comunicación entre dispositivos IOT es una contramedida recomendada para evitar que un dispositivo sea comprometido para instalar software no autorizado. Sólo se debe permitir instalar software certificado durante las actualizaciones y parches.
Para las pruebas de contraseñas débiles, vulnerabilidades de desbordamiento de búfer, etc., en software IOT, se recomienda seguir las mejores prácticas de OWASP. Los dispositivos IOT también deben probarse en puertos USB para identificar vulnerabilidades. El objetivo siempre será reducir la superficie de ataque del dispositivo IOT en la mayor medida posible. Además, al igual que cualquier otro sistema de TI que esté cerca de Internet, se debe almacenar, transmitir y procesar sólo la cantidad mínima de información confidencial.
Forescout categoriza los dispositivos IOT en tres niveles:

1) ***Desastroso*****:** Dispositivos conectados a IP que conectados directamente a Internet están en alto riesgo. Pueden causar daños a la empresa al obtener acceso a información confidencial o causar deterioro de la infraestructura crítica.

2) ***Disruptivo*****:** Los sistemas interconectados, como los teléfonos e impresoras de voz sobre Protocolo de Internet (VoIP), pueden provocar interrupciones en las operaciones del negocio.

3) ***Perjudicial*****:** Los dispositivos tales como bombillas y refrigeradores inteligentes pueden usarse para husmear alrededor de la red de la empresa para obtener acceso a Metadatos sobre la red [18].
Los productos como Adaptive Defense proporcionan a los equipos de seguridad, información sobre los ejecutables que entran en la red, y adicionalmente tienen la capacidad de confirmar de forma proactiva un incidente, en lugar de solo generar alertas indicando que se tienen eventos anómalos. Determinar el punto en el que realmente ocurrió una intrusión después de detectar que sucedió es la clave para manejar las amenazas actuales y emergentes en tiempo real en toda la organización.

V. CONCLUSIONES

El potencial de IOT es enorme y ya está cambiando de forma determinante la forma como las personas trabajan, viven y se divierten. Aunque es claro que esta tecnología no ha alcanzado su máximo desarrollo, es más se puede decir que se encuentra en sus primeras etapas, ya se puede ver que está en todas partes, aunque la mayoría de personas no puedan notarlo. En Colombia las empresas de telecomunicaciones como Telefónica Movistar, ya están implementando redes para la transferencia de datos de aplicaciones que usen la tecnología IOT, y adicional están generando espacios para desarrollos de estas tecnologías. Por otra parte, empresas como Oracle ya se encuentra ofreciendo servicios para el uso de esta tecnología, lo que permite concluir que IOT cada vez tomara más fuerza y las empresas intentaran sacar el mayor provecho de su uso.

Como se vio a lo largo del artículo, el internet de las cosas se ha convertido en un concepto muy poderoso, pero utilizarlo de manera responsable requiere una visión de futuro, una planificación adecuada y un diálogo abierto. IOT como cualquier implementación de nueva tecnología, trae consigo riesgos y problemas nuevos y más complejos, por tanto, nace la necesidad de evaluar los riesgos de forma integral, con el objetivo de garantizar que el valor comercial se maximice mientras el riesgo se minimiza. Para realizar esta evaluación es necesario contar con la ayuda de todas las partes involucradas, incluidos los equipos comerciales, los equipos encargados de la operación, el equipo de seguridad de la información y todas las demás áreas pertinentes

Actualmente la comunicación entre dispositivos de red se está expandiendo de forma significativa, lo cual trae consigo nuevos tipos de riesgos, que pueden afectar no solo la privacidad, sino también la seguridad humana, tal como se vio en el artículo cuando se mencionaron las aplicaciones de IOT en la salud y la industria automotriz, donde se pudo observar que trae muchos beneficios, pero a su vez los riesgos pueden

ser altos. Es por estas razones que los profesionales de seguridad de la información deben mantener una sólida compresión de estas nuevas tecnologías y los riesgos que traen consigo, con el fin de poder aplicar los controles apropiados para la protección contra los ataques que puedan ser lanzados contra estos dispositivos. Adicional, se considera necesario la unión de Estados nacionales, las organizaciones profesionales, los organismos de normalización y las empresas, con el propósito de estandarizar y generar políticas que permitan elaborar un nivel adecuado de respuestas para tener protección frente a los nuevos ataques que recién emergen para tecnologías IOT.

A menudo la seguridad en IOT no tiene las consideraciones ni la importancia necesaria cuando se encuentran en su etapa de diseño e implementación, lo cual es un error grave. La seguridad no se debe centrar solo en los dispositivos, es necesario aplicar seguridad en todos los componentes y capas del sistema. Para garantizar el correcto funcionamiento y proteger los sistemas de IOT de forma adecuada, es de vital importancia que la seguridad sea contemplada en todas las etapas del ciclo de vida, incluyendo las fases de diseño, instalación, configuración y operación.

Como se ve el avance de las aplicaciones de IOT en la vida cotidiana de las personas y en el desarrollo de las organizaciones cada día es más influyente, por tanto, la seguridad en IOT se le debe dar igual o mayor importancia que a cualquier dispositivo de la red TI, dado que al no estar estandarizado ni regulado, cuenta con una mayor exposición a ataques, es por esta razón que se deben aplicar controles como a cualquier dispositivo de red, dentro de los cuales se destacan algunos como contraseñas fuertes, claves de certificados, identificadores y nombres de dispositivos o host difíciles de adivinar, monitoreo y análisis de registros, administración proactiva de usuarios y dispositivos y la implementación de guías y mejores prácticas establecidas por organizaciones como US National Institute of Standards and Tecnology, las cuales cuentan con un mayor conocimiento del uso de esta tecnología.

IOT es una realidad y su uso crece de manera exponencial dados los beneficios que trae, por esta razón es mandatorio que en las organizaciones se contemple la implementación de controles de seguridad desde su diseño, para sacar el mayor provecho de esta tecnología con el menor riesgo.

VI. BIBLIOGRAFÍA

[1] International Telecommunication Union, 15 June 2012. [Online]. Available: www.itu.int/rec/T-REC-Y.2060-201206-I.

[2] ETSI, «Standards for an Internet of Things,» 3-4 July 2014. [Online]. Available: www.etsi.org/news-events/events/771-2014-etsi-ec-dg-connect-iot.

[3] Chitkara et al, «The Internet of Things, PricewaterhouseCoopers,» May 2015. [Online]. Available: www.pwc.com/gx/en/technology/publications/assets/pwc-iot-semicon-paper-may-2015.pdf.

[4] ORACLE, [Online]. Available: https://www.oracle.com/co/internet-of-things/what-is-iot.html.

[5] ISACA, «ISACA Journal Volume 5,» 2017 . [Online]. Available:https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/anatomy-of-an-iot-ddos-attack-and-potential-policy-responses-spanish.aspx.

[6] ISACA, «ISACA Journal Volume 3,» 2017. [Online]. Available:https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/managing-the-risk-of-iot-spanish.aspx?utm_referrer=.

[7] M. Kranz, Internet of Things: Construye nuevos modelos de negocio, Madrid: LID Editorial, 2017.

[8] ISACA, «Revista ISACA Volumen 2,» 2015. [Online]. Available:https://www.isaca.org/Journal/archives/2015/Volume-2/Pages/internet-of-things-offers-great-opportunities-and-much-risk.aspx.

[9] ISACA, An ISACA Internet of Things Series White Paper, p. 13, 2015.

[10] C. Martin, MediaPost, 26 October 2016. [Online]. Available:www.mediapost.com/publications/article/287614/us-to-issue-iot-principles-after-internet-cybera.html.

[11] K. York, Oracle, 22 October 2016. [Online]. Available: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/.

[12] S. Lawson, ComputerWorld, 19 September 2016. [Online]. Available: www.computerworld.com/article/3122244/internet-of-things/industrial-iot-inches-toward-consensus-on-security.html.

[13] Federal Trade Commission, USA, 4 January 2017. [Online]. Available: www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security.

[14] INCIBE, incibe-cert, 2019 Abril 2019. [Online]. Available:https://www.incibe-cert.es/blog/importancia-seguridad-iot-principales-amenazas.

[15] D. Santos, hubspot, 28 Enero 2019. [Online]. Available: https://blog.hubspot.es/marketing/internet-cosas-iot-como-protegerse.

[16] J. M. Ojeda, ambitojuridico, 15 Agosto 2019. [Online]. Available:https://www.ambitojuridico.com/noticias/especiales/tic/una-vision-del-revolucionario-internet-de-las-cosas-en-colombia.

[17] Comisión de Regulación de Comunicaciones, 8 Agosto 2016. [Online]. Available: https://www.crcom.gov.co/recursos_user/2016/Actividades_regulatorias/PCA_IoT/Informe_6_PCA_IoT.pdf.

[18] ForeScout Technologies, Inc, 2016. [Online]. Available: https://www.forescout.com/wp-content/uploads/2016/10/iot-enterprise-risk-report.pdf.

[19] PORTAFOLIO, 16 Febrero 2019. [Online]. Available: https://www.portafolio.co/innovacion/empresas-colombianas-deben-apostarle-al-internet-de-las-cosas-526259.

[20] expomobile, 19 Feb 2019. [Online]. Available: https://expomobile.co/2019/02/19/las-oportunidades-del-internet-de-las-cosas-iot-para-colombia/.

[21] El espectador, «Telefónica lanzó red de "internet de las cosas" para Colombia,» 18 Septiembre 2019. [Online]. Available:https://www.elespectador.com/tecnologia/telefonica-lanzo-red-de-internet-de-las-cosas-para-colombia-articulo-881669.
[22] MINTIC, 30 octubre 2019. [Online]. Available: https://mintic.gov.co/portal/604/w3-article-106960.html?_noredirect=1.
[23] El Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT), [Online]. Available: http://www.cea-iot.org/lineas-de-trabajo/.
[24] MINTIC, 26 Abril 2016. [Online]. Available: https://www.mintic.gov.co/portal/604/w3-article-15169.html?_noredirect=1.

Autor

Jorge Alberto Molina García
Ingeniero Electrónico
Universidad Autónoma de Colombia
2006