IoT: La Evolución de la Seguridad en el Internet de las Cosas

Virguez Lozano, Jorge Alaberto
jvirguez.83@gmail.com
Universidad Piloto de Colombia

Resumen— La conectividad inteligente de dispositivos físicos conocidos más popularmente como internet of things IoT está aumentando rápidamente la productividad y los niveles de comunicación además permite numerosas funciones a través de organizaciones en todo el mundo. Desafortunadamente, la falta de comprensión por parte de las organizaciones de los requisitos específicos de seguridad de IoT impide su potencial de crecimiento. Como tal, una organización sólo puede cosechar la promesa de los beneficios de IoT si piensa en el elemento de seguridad como un componente vital de la implementación.

Índice de Términos—IoT, ciberseguridad, metodologías de seguridad, DDOS, riesgos, seguridad de la información.

Abstract —The intelligent connectivity of physical devices known more popularly as the Internet of Things IoT is rapidly increasing productivity and levels of communication and enabling numerous functions across organizations worldwide. Unfortunately, organizations' lack of understanding of IoT's specific security requirements hinders its growth potential. As such, an organization can only reap the promise of IoT's benefits if it thinks of the security element as a vital component of implementation.

Keywords— IoT, security, cybersecurity, Security methodologies, ddos, risks, information security.

I. INTRODUCCIÓN

En la actualidad en el mundo que vivimos el internet ocupa un papel fundamental en todo aquello que nos rodea y es claro que desde su creación su crecimiento viene de forma exponencial a lo largo de los años hasta el punto donde nos encontramos en estos momentos en el que hay más teléfonos móviles que personas en el planeta, pero esto también ha traído grandes avances en temas de comunicación y uno de estos avances es el internet de las cosas o IoT el cual es algo cada vez más común entre todos los habitantes ya sea de teléfonos inteligentes, usuarios de pulseras con medidores de posición o medidores de salud, los automóviles aun estos en modelos de gamas más accesibles para el usuario promedio y en el hogar como lo es ahora los hogares inteligentes con estufas, lavadoras, refrigeradores, televisores y cámaras de monitoreo remoto como algunos ejemplos comunes de dónde encontrar dicha tecnología, pero también está presente en los ámbitos empresariales, industriales y hasta en la medicina lo cual busca hacer la vida más fácil pero también es la invitación a personas no deseadas sobre algo muy preciado para toda persona o compañía y no es nada más y nada menos que nuestra información, pero como así que personas no deseadas, pues con el crecimiento continuo en el uso del IoT, se han venido presentado inconvenientes de accesos no autorizados sobre algunos de estos dispositivos y hoy en día el mundo de internet tiene un peligro inminente y que avanza constantemente y es el de los hackers o piratas informáticos, pero no hay que generalizar y decir que toda persona que es hacker por ende es un delincuente pero si hay que reconocer que con el crecimiento del IoT estos piratas informáticos que cada vez son más comunes también hay tener presente que se han encontrado debilidades en la seguridad de esta tecnología y lo cual ha garantizado accesos a diversas plataformas causando problemas algunos reconocidos otros no tan publicitados pero que son un llamados de atención para todos tanto usuarios como desarrolladores y compañías que fabrican dichos dispositivos.

Hoy en día es fácil encontrar y ver tutoriales de cómo obtener acceso sobre un televisor inteligente o smart tv, o vulnerabilidades que pueden ser explotadas sobre el refrigerador de última tecnología que está conectado a internet, es por eso que el papel de la seguridad informática y de la información ha tomado un papel vital importancia y es porque esta tecnología que es tan versátil y útil no es la excepción en temas de seguridad.

II. HISTORIA DE IoT

El termino Internet de las Cosas IoT, es un concepto que se refiere a la interconexión digital de objetos dispositivos con el Internet, pero para algunas fuentes[1] comienza desde la invención del telégrafo electromagnético por el Baron Pavel L'vovitch Schilling en Rusia, pero mucho antes el famoso Nicola Tesla nos dejó lo siguiente: "cuando la comunicación inalámbrica esté totalmente implantada en toda la tierra se convertirá en un enorme cerebro, que de hecho lo es, todas las cosas son partículas de un real y rítmico conjunto. Vamos a ser capaces de comunicarnos el uno con el otro al instante, independientemente de la distancia, no solo esto, sino que a través de la televisión y la telefonía vamos a ver y oír a otro perfectamente como si estuviéramos cara a cara, a pesar de las distancias de miles de kilómetros, y los instrumentos a través de los cuales vamos a ser capaces de hacerlos, serán asombrosamente simples en comparación con nuestro actual teléfono un hombre será capaz de llevar uno de estos en el bolsillo de su chaleco" y no estaba nada equivocado hablando a 2016 donde con casi cada individuo del plante posee un teléfono móvil y por el cual podemos estar en contacto y casi en tiempo real gracias a una conexión de internet pero regresando a la cronología del internet de las cosas este nombre se utilizó por primera vez en 1999 por Kevin Ashton, fue cofundador y director ejecutivo del centro de auto-id, en una conferencia que se encontraba dictando, pero su nacimiento lo dan sobre los años 2008-2009 donde Según Cisco Internet business solutions group (ibsg), simplemente el momento en el que más "cosas u objetos" estaban conectados a Internet que las personas.

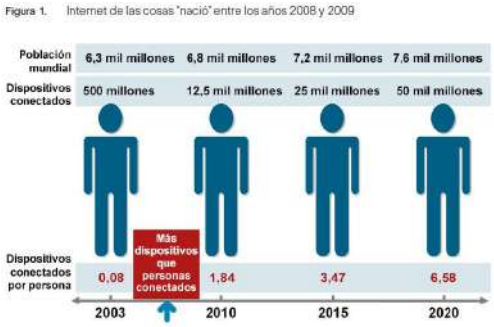

Fig. 1. Nacimiento del internet de las cosas sobre 2008 -2009 [2]

Continuando con la revisión cronológica del IoT en 2011 hay un hecho importante el cual es determinante para la cantidad de aparatos conectados hoy en día se realiza el lanzamiento del protocolo ipv6 este nuevo protocolo permitirá 340 undecillones de nuevas direcciones ip, para el 2014 y los años siguientes Gartner situó al IoT en el pico de expectativas infladas.

Fig. 2. IoT en el pico de expectativas según Gartner [3]

Con respecto avanzan los años también crecen y maduran las comunidades del internet de las cosas así como las redes sociales como linkedin o el consejo de tecnología y estrategia del Reino Unido con su plataforma social_connect, asi como el Reino Unido demuestra interés sobre el IoT también lo hace el resto de Europa apoyando a esta tecnología con su grupo de trabajo ICT (information and comunication thecnologies) o dg-connect el cual trabaja para desarrollar un mercado único digital con el fin de generar un crecimiento inteligente, sostenible e integrador en Europa, también la creación de "the global standards Initiative on internet of things (IoT-gsi)" ayuda promoviendo un enfoque unificado para el desarrollo de normas y técnicas para una escala global. Para el 2015 Garnert también nos muestra una estadista con proyección a futuro del IoT.

Table 1: Internet of Things Units Installed Base by Category (Millions of Units)

Category	2014	2015	2016	2020
Consumer	2,277	3,023	4,024	13,509
Business: Cross-Industry	632	815	1,092	4,408
Business: Vertical-Specific	898	1,065	1,276	2,880
Grand Total	3,807	4,902	6,392	20,797

Source: Gartner (November 2015)

Fig. 3. Unidades instaladas de IoT basados en categorías según Gartner [4]

También nos da claridad que, en términos de inversión en hardware, el consumo en aplicaciones ascenderá a $ 546 mil millones en 2016, mientras que el uso de cosas conectadas en la empresa impulsará $ 868 mil millones en 2016.

Table 2: Internet of Things Endpoint Spending by Category (Billions of Dollars)

Category	2014	2015	2016	2020
Consumer	267	416	546	1,534
Business: Cross-Industry	115	155	201	566
Business: Vertical-Specific	557	612	667	911
Grand Total	**939**	**1,183**	**1,414**	**3,010**

Source: Gartner (November 2015)

Fig. 4. Unidades instaladas de IoT como endpoint basados en categorías según Gartner [5]

Lo que todas estas cifras dejan en claridad es el aumento tanto de unidades como de hardware a los próximos años para el IoT lo cual también trae consigo múltiples inquietudes a muchos sectores y es la ciberseguridad para estos dispositivos y el cómo los principios de la seguridad no se vean afectados por su crecimiento descomunal.

III. BRECHAS DE SEGURIDDAD EN IoT

En la actualidad no existe seguridad perfecta, pero si métodos para lograr hacerla más eficiente y es lo que se debe tener en cuenta en todo momento, pero estas recomendaciones o en algunos casos las buenas practicas no siempre son aplicadas por las compañías ni en los hogares ya sea por temas de recursos económicos o de personal o simplemente por desconocimiento de ellas, la seguridad en IoT se ha vuelto un tema de suma importancia debido a recientes acontecimientos[6] donde se ha visto comprometida lo cual hace necesario evaluar todo el entorno para encontrar posibles nuevos puntos de accesos y vulnerabilidades no tenidas en cuenta anteriormente pero también se debe hacer referencia a una mala metodología al momento de diseño, desarrollo y posterior implementación donde la seguridad se dejó en un segundo plano, en cuanto a brechas causados por dispositivos del internet de las cosas se tomara como referencia al más famoso y también el más grande hasta el momento y el cual ocurrió el pasado 21 de Octubre de 2016 donde en un ataque de denegación de servicio distribuido (ddos) causo una interrupción generalizada de internet en los Estados Unidos, el ataque se vio dirigido al sistema de resolución de nombres (dns) y este es quien se encarga de asegurar que todas las peticiones que se realicen a través de internet sean entregadas correctamente a la dirección ip que les corresponda, pero cómo fue posible este ataque y cuál fue la responsabilidad que tubo IoT, pues en primera medida todo fue posible a la gran cantidad de dispositivos digitales conectados a internet y los cuales está sin protección como lo son routers domésticos, y cámaras de vigilancia los atacantes hicieron usos de estos miles de dispositivos previamente infectados con código malicioso para lograr su cometido, pero como identificar dichos dispositivos que no contaban con protección todo esto fue posible con un software que se encuentra de manera gratuita en la red, también se podrían preguntar como cámaras de vigilancia o un router domestico equipos que a simple vista no son muy potentes comparándolos con grandes computadoras pero que si son capaces de generar grandes cantidades de tráfico y si se utiliza un gran número de estos dispositivos logran causar el desbordamiento de un servidor especifico, pero donde radica el problema mencionado anteriormente que dichos dispositivos no contaban con seguridad y cómo fue que lograron el accesos a dichos equipos pues todo se debe a que muchos de los equipos se encontraban aun con las contraseñas por defecto y que estas en su gran mayoría son de conocimiento público en internet y por esto fue que se hizo posible la infección de dichos equipos por lo que habría que pensar si podemos convertirnos en un punto de ataque desde nuestros hogares ya que cuantos de los usuarios promedio cambia la contraseña por defecto en su router, son premisas que hay que hacerse en cada momento y hacer entender al ciudadano del común.

La ciberseguridad es algo que afecta a todos en general, para poder disminuir el riegos de ataques como los presentados el 21 de Octubre y es que en estudios recientes la compañía eset da a entender que al menos el 15% de los routers domésticos no están protegidos y puede que esa estadística no sea muy llamativa a simple visto pero hay que tener en cuenta que ese 15% podría equivaler a cientos de millones de equipos, pero como lograr disminuir este tipo de ataques, estas son algunas recomendaciones realizadas por us cert a raíz de los últimos ataques:

- Comprobar que todas las contraseñas predeterminadas se hayan cambiado por contraseñas fuertes. Es muy fácil encontrar en Internet los nombres de usuario y las contraseñas por defecto para la mayoría de los dispositivos, por lo que, si se dejan, son extremadamente vulnerables.
- Actualizar los dispositivos de la IoT con los parches de seguridad correspondientes apenas se encuentren disponibles.
- Desactivar la configuración automática universal plug and play (upnp) en los routers al menos que sea absolutamente necesaria.
- Comprar los dispositivos de la IoT en empresas conocidas, que tengan una reputación de ofrecer dispositivos seguros.

La infección de equipos con código malicioso no son temas nuevos en el mundo de la seguridad en internet, así como los ataques de ddos ya que este tipos de ataques datan de hace muchos atrás lo realmente increíble es que en 2014 en we live security se destacó el descubrimiento de 73.000 equipos en este caso cámaras de seguridad que aun usaban las contraseñas por defecto lo que da a entender el descuido en seguridad para estos dispositivos y que solo cuando grandes plataformas son afectadas se empieza a tener la debida atención y donde se visualizan la falta de controles para intentar mitigar ataques como los presentados el 21 de Octubre, pero no solo se puede hablar de controles también debe tenerse en cuenta metodologías y análisis de impacto al momento de implementar nuevas tecnologías en ambientes productivos críticos.

IV. ARQUITERCTURA DE SEGURIDAD EN IoT

Existen diversos enfoques hacia la arquitectura en IoT[7], sobre este documento se tocara el que la compañía Microsoft utiliza para su arquitectura de IoT, pero antes de comenzar a hablar de la arquitectura hay que hablar del modelado de riesgos y es que el objetivo del modelado de riesgos es conocer la forma en que un atacante puede poner en peligro y luego tomar las precauciones necesarias para evitarlo, esto va en concordancia con el personal de diseño ya que las posibles mitigaciones consideradas durante esta etapa causaran un menor impacto sobre el desarrollo del sistemas que si son consideradas en la etapa de implementación adicionalmente que alguna actualización de las defensas para un gran número de dispositivos en producción puede ser inviable para una compañía es decir el modelado de riesgos tendrá su máximo valor si es incorporado desde la fase de diseño pero que modelos de riesgos debe crearse en su documento Microsoft referencia a la creación de un modelo de riesgos para la solución en conjunto, pero también incluir y centrarse en la siguientes áreas las características de privacidad y seguridad, las características cuyos errores son pertinentes para la seguridad y las características que tocan un límite de confianza, el modelado constara de cuatro pasos que son:

- Modelar la aplicación
- Enumerar las amenazas.
- Mitigar las amenazas.
- Validad las mitigaciones.

También es necesario tener presente las siguientes recomendaciones, crear un diagrama con la arquitectura de referencia, obtener información general y pensar en el sistema como un todo, antes de realizar una búsqueda en profundidad en los lugares pertinentes y por ultimo manejar el proceso si hay algún tipo de problema en la fase de modelado y se desea explorar se puede hacer estas recomendaciones no es necesario seguirlas al pie de la letra.

En cuanto a las amenazas también se tienen ciertos elementos principales dentro del modelado de riesgos que son:

- Procesos o servicios ya sean (web, win32, demonios, nix, etc.).
- Almacenes de datos (data centers).
- Flujo de datos donde los datos son movidos dentro de una aplicación o hacia otra.
- Entidades externas pueden ser los usuarios finales,

Todos los elementos del diagrama de arquitectura se encuentran expuestos a amenazas, Microsoft utiliza el mnemotécnico stride (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege) o modelado de riesgos otra vez, stride, los procesos estarán sujetos a stride, los flujos de datos estarán sujetos a “tid”, los almacenes de datos a “tid” y a “r” si son archivos de registro y las entidades estarán sujetas a “srd”, la solución de

arquitectura que Microsoft propone en el informe es para su servicio de cloud computing.

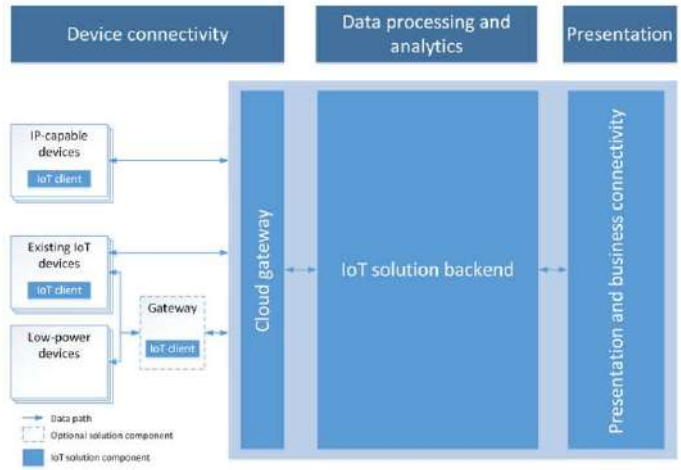

Fig. 5. Diagrama simplificado de la arquitectura de IoT según Microsoft [8]

V. ASPECTOS DE SEGURIDAD EN IoT

Los dispositivos que se encuentran conectados y que son de uso especial tienen un amplio número de posibles áreas de interacción y posibles patrones de interacción y todos deben considerarse al momento de brindar un marco para ser que sea protegido el acceso digital, al momento de realizar la exploración de patrones de interacción, Microsoft seguiré examinar el control del dispositivo y los datos del dispositivo con el mismo grado de atención, el control es posible clasificarlo como toda información que cualquiera de las parte le proporcione al dispositivo con el objetivo de modificar o influir en su comportamiento, en lo relacionado con su estado o el estado de su entorno, los datos los clasifican como toda información que transmite un dispositivo a cualquier otra parte acerca de su estado y el estado que se percibe de su entorno. Se aconseja dividir las arquitecturas de IoT típicas en varias zonas como parte del modelado de riesgos, estas zonas son descritas de la siguiente forma:

- Dispositivo.
- Puerta de enlace de campo.
- Puerta de enlace en la nube.
- Servicios

Estas zonas son una forma de segmentación para la solución y cada una de ellas tendrá sus propios datos, requisitos de autenticación y autorización, también pueden ser usadas para aislar daños y así disminuir el impacto en casos de fallas, casada zona está delimitada por un límite de confianza el cual se indica con la línea puntea el cual representa una transición de datos o información que va de un origen a otro y en donde los datos durante dicha transición pueden verse comprometidos por medio de suplantación de identidad, manipulación, rechazo, divulgación de información, denegaciones de servicio y elevaciones de privilegios o como anteriormente se denominó stride.

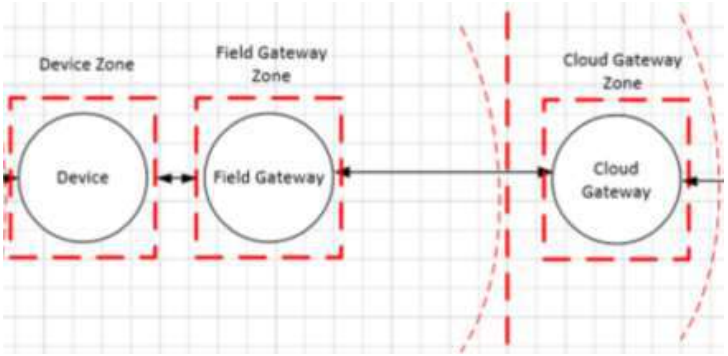

Fig. 6. Diagrama de zonas para la arquitectura de IoT del servicio azure según Microsoft [9]

Todos los componentes que se encuentran dentro de cada limite también serán sometidos al stride lo cual permitirá una mejor perspectiva de todo el modelado de riesgos a continuación se hablara un poco de cada una de las zonas y como se ha señalado anteriormente se tomara como referencia a Microsoft.

a. La zona del dispositivo

Hace referencia al entorno es el espacio físico más próximo que rodea al dispositivo, donde el acceso digital o físico de punto a punto de la red local al dispositivo. Se asume que la red local es única y se encontrara asilada de internet pero podría conectarse de ser necesario además incluye las diferentes tecnologías de conexión ya sean de tipo inalámbrico de largo o corto alcance para así permitir la comunicación entre dispositivos, en esta zona no se incluyen redes virtualizadas ni tampoco redes de operadores públicos que requieran de dos dispositivos o más para comunicarse a través de un espacio de la red pública si se llegase a establecer una comunicación de punto a punto.

b. La zona de puerta de enlace de campo

Hace referencia a un dispositivo o software el cual cumple como principal función ser habilitador de las comunicaciones y potencialmente como sistema de

control de los dispositivos además de ser centro de procesamiento de datos de los dispositivos conectados a esta zona, al ser la puerta de enlace esta se pude estar sujeta a intrusiones física además de tener poca redundancia operativa, la zona de enlace de campo se diferencia de un router en que esta tiene un rol activo en la administración del acceso y del flujo de información, lo cual hace referencia que es una entidad y terminal de sesiones o también terminal de conexiones dirigidas a aplicaciones, también se diferencias de los dispositivos nat o firewalls en que estos dispositivos funcionan como enrutadores de tráfico y permiten o bloquean peticiones o sesiones que son realizadas a través de ellos, la zona de puerta de enlace de campo tiene claramente dos áreas expuestas y se encuentran definidas de la siguiente forma, una zona interna que dice de los dispositivos que conectan a ella y hacen parte del interior de la zona, y una zona externa y hace referencia al borde de la zona.

c. La zona de puerta de enlace en la nube

Permite la interconexión remota desde y hacia los dispositivos o puertas de enlace de campo de varios sitios a través de un espacio en la red pública, una puerta de enlace en la nube puede utilizarse de forma virtualizada para así aislar todas las puertas de enlace como sus dispositivos o puertas de enlace de campo del resto del tráfico de la red, esta zona no es un sistema de control de dispositivos ni almacenamiento o procesamiento de los datos del dispositivo.

d. La zona de servicios

Un servicio según Microsoft se cataloga como cualquier componente de software o modulo que interactúa con dispositivos a través de las puertas de enlace de zona o de la nube para la recopilación y el análisis de datos asi como también el control los servicios se mueven por las otras zonas y subsistemas almacenando y analizando datos.

VI. LA SEGURIDAD EL ELEMENTO VITAL EN IoT

La implementación de IoT en las compañías se encuentra en auge y continuo crecimiento durante los próximos años de acuerdo a fuentes especializadas [9], las cuales señalan 4 aspectos fundamentales para toda compañía al momento de considerar e implementar IoT.

- Que tipos de aplicaciones y dispositivos IoT se están implementando.
- Qué tipo de tecnologías están siendo utilizadas por las compañías.
- Que tipos de eventos de seguridad enfrentan las organizaciones al momento de implementar una solución IoT.
- Comprender como los riesgos asociados a IoT avanzarán o aumentarán en los próximos años.

Dichas fuentes realizaron su evaluación sobre diversas compañías y áreas responsables en la decisión de implementar IoT en sus respectivos negocios, también se tuvieron consideraciones en diversos campos y aplicaciones de IoT como los son: el cuidado de la salud, el campo energético, petróleo, gobierno, utilidades y transporte como algunos ejemplos.

La seguridad sobre IoT es algo que las organizaciones deben afrontar en un futuro ya cada vez más cercano y en algunas ya es una realidad es por eso que el uso de una metodología previa a la implementación como se vio en anterioridad en este documento ayudara a mitigar riesgos antes de una salida a producción prematura de un producto, y es el valor que IoT puede generar para diversas compañías en sus diversos campos de acción lo cual implicaría innovaciones en sus procesos pero también trae consigo temores por las brechas de seguridad que en muchos casos son detectadas cuando una aplicación ya se encuentra en producción lo cual deja en evidencia que muchas compañías no toman las suficientes medias en cuanto a la seguridad en IoT, lo cual también genera demanda cada vez más en compañías especializada en este campo de la seguridad de IoT.

Está claro que muchas compañías se encuentran implementado o están en la planeación de una futura implementación de IoT por su gran variedad de funciones es decir entre el 29% y el 38% de las compañías ya han implementado o piensan expandir IoT en áreas específicas como transporte, salud, monitoreo ambiental, aplicaciones industriales, manejo y administración energética y administración de infraestructura entre el 37% y el 47% planean el despliegue de estas funciones de IoT durante los próximos 5 años según las firmas encuestadas por las diferentes fuentes especializadas

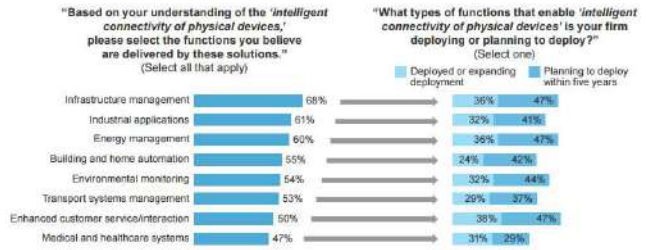

Fig. 7. Variedad de tecnologías de IoT implementadas por las compañías según Cisco [10]

Adicionalmente ya después de que la decisión de la implementación y el despliegue de IoT están tomadas se debe evaluar el tipo de tecnología con que cuenta la compañía y si es viable para la instalación de dispositivos IoT o de ser necesario la adición de una nueva tecnología como por ejemplo wi-fi es la más común entre las tecnologías utilizadas por IoT, otras tecnologías identificadas como necesarias fueron los sensores de localización y seguimiento.

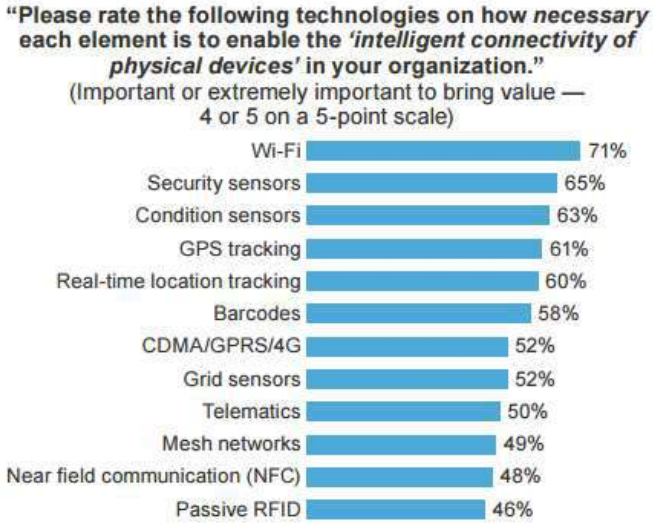

Fig. 8. Tecnologías necesarias para la implementación de IoT en las compañías según Cisco [11]

Así como las nuevas necesidades de infraestructuras se hacen necesarias también lo son las consideraciones en cuanto los peligros y riesgos mencionados anteriormente en este documento, pero los cuales son los más comunes hoy en día como los ataques informáticos a redes, malware, software malicioso y los hackers (ver figura #) del 28% al 47% de las organizaciones han experimentado brechas en seguridad sobre dispositivos IoT pero dichas brechas aun no superan la cantidad de ataques sobre las redes comunes de comunicaciones

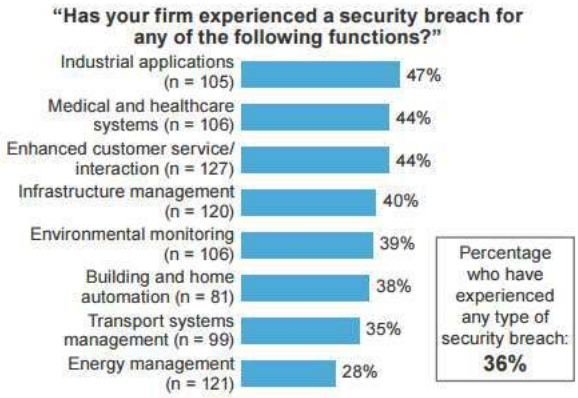

Fig. 9. Áreas de aplicación de IoT con más brechas o incidentes de seguridad en las compañías según Cisco [12]

Los riesgos sobre IoT continuaran creciendo a medida que la misma tecnología avance, pero a su vez la preocupación en las compañías acerca de la seguridad debe tener un crecimiento si no igual al menos considerable en cuando a la concientización de las altas directivas en este aspecto.

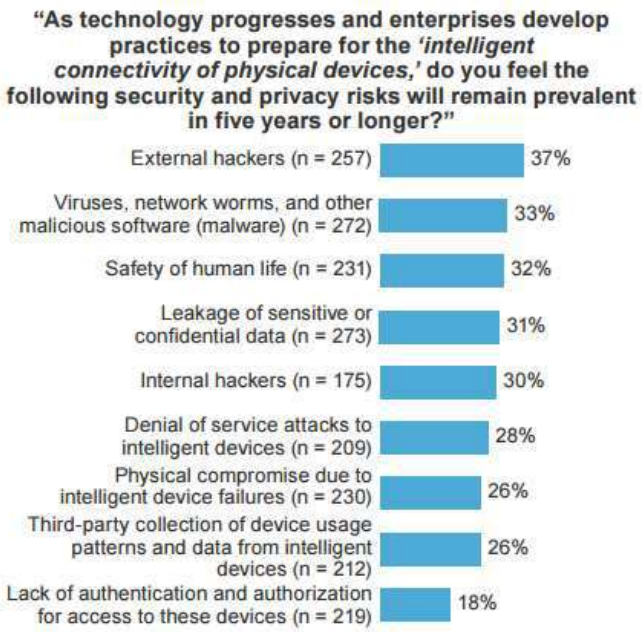

Fig. 10. Riesgos internos y externos que según las compañías seguirán presentes a través del tiempo en IoT según Cisco [13]

Los temores continuarán en las compañías ya que no todos los peligros a los que está expuesto IoT serán mitigados completamente en los próximos años lo cual hace que mantener la privacidad de la información sea la prioridad para IoT ya que la mayoría de estos dispositivos de conexión se encuentran recolectando datos lo cual hace que los riesgos de una violación de seguridad crezcan y si a esto se le agrega la falta de experiencia y de

conocimiento por parte de las organizaciones en una implementación segura de IoT, más se ve necesario de las altas directivas para dar una solución viable y duradera para cada compañía, y es que en muchas ocasiones las compañías en su afán de reducir costos en TI solo se quedan con cierta solución de los proveedores de tecnologías IoT que en la mayoría son parches de seguridad y no se evalúa la seguridad de IoT como un todo ya que no siempre se podrá implementar la solución actual de seguridad que posee la compañía a dichas tecnologías sino que se tendrán que tener consideraciones adicionales así como infraestructura y equipos no contemplados anteriormente lo que incurriría en gastos extras para la compañía como lo son buscar terceros especializados en seguridad para llenar los vacíos que se puedan tener o también buscar el asesoramiento de proveedores de infraestructura de TI.

VII. ESTANDARES DE SEGURIDAD EN IoT

Los grupos de estándares para IoT están surgiendo para resolver problemas de interoperabilidad, protocolos y seguridad [14].

La meta para los estándares de seguridad para los dispositivos IoT al final del dia deben ser la de ayudar a todo tipo de clientes para que estos puedan evaluar la seguridad en sus dispositivos IoT y a medida que dichos estándares se deben mantener enfocados en la seguridad de la información en todo momento.

Esta será una labor que tomará tiempo y es que el objetivo de dichos estándares sean el equivalente cibernético como por ejemplo de underwriters laboratorios (ul) o (ce) safety ratings lo cual garantice que sea algo mesurable para los especialista o consumidores que dado el escenario por medio de estos estándares un futuro usuario de un dispositivo IoT tenga la seguridad que dicho dispositivo cuenta con unos mínimos de seguridad lo cual generara confianza al momento de la compra o también en dado caso una compañía de seguros podría evaluar ciertos tipos de reclamaciones referentes a crímenes cibernéticos relacionados con dispositivos IoT y dependiendo del calificativo que tenga a nivel de seguridad dicho dispositivo, otro ejemplo del cómo deberían ser estos estándares son los relacionados con el sector energético y la automatización industrial los cuales cuentan con estándares de seguridad y que definen los mínimos requisitos a cumplir por como lo es nerc-cip que define los requisitos de seguridad para que operan en la red eléctrica de norte américa otro claro ejemplo es el iec-63443 que se utiliza ampliamente en la automatización industrial y sistemas de control y que a través del cual crean una línea base para todos los fabricantes de dispositivos , la cual deben acatar a cabalidad al momento de desarrollar los respectivos dispositivos es decir si algún dispositivo no cumple con la línea base impuesta en el estándar sencillamente esa pieza de hardware no podrá ser usado.

Dejando a un lado los ejemplos el tema de la seguridad o ciberseguridad para IoT es un reto complejo y sería muy atrevido afirmar que la creación de un estándar para IoT eliminará todas las amenazas de ataques en un corto lapso de tiempo, pero si hay medidas que tomar y marcos que seguir mientras un estándar completo y en su medida efectivo se implementa, pero se podría decir que un estándar de seguridad exitoso proveerá:

- Protección para los dispositivos garantizando que solo código autentico y de una fuente de confianza se ejecuta en los dispositivos.
- Protección de datos proporcionando comunicaciones seguras, protección a los datos que están inactivos y el retiro de forma segura de los dispositivos.
- Conciencia de los ataques incluyendo el monitoreo, la detección de intrusos por medio de la integración de sistemas de administración.
- Gestión de la seguridad actualizando las políticas de seguridad en respuesta a amenazas existentes o futuras dado el caso de ser necesario.
- Autenticación maquina a máquina garantizando que los dispositivos IoT solo se comunican con otros equipos conocidos y de confianza.

Los estándares de seguridad son un mercado emergente como se mencionó anteriormente dado que la seguridad continúa evolucionando para los dispositivos IoT, así como las amenazas, pero algunos de los estándares existentes de seguridad se enfocan en ciertos sectores o industrias específicas como puede ser el estándar de ciberseguridad de la NIST que aplica a los sectores financiero, energético, cuidado de la salud y algunos otros pero para los que se diseñó este estándar es en ayudar a dichos sectores en mejorar

la protección de la información así como de sus activos físicos contra ciberataques es por tal motivo que los estándares de seguridad para los dispositivos de IoT empezaron a emerger para unificar las medidas de control o de buenas prácticas algunas de estas mencionadas en este documento como lo es el modelado de riesgos, desarrollo de software seguro pero que también toca el tema de pruebas a la robustez de la seguridad para dispositivos IoT para así ayudar a disminuir los peligros a los que muchos de esto hoy en día están expuestos y que muchas compañías y personas no están expuestos y por eso habrá que esperar un poco más y que continúen evolucionando para garantizar tranquilidad en un tema en cual la sensibilización tanto en compañías como en usuarios del común viene creciendo día a día.

VIII. CONCLUSIONES

El constante crecimiento de internet hace que las nuevas tecnologías y servicios disponibles para que todo tipo de compañías tengan acceso y puedan mejorar sus servicios y rentabilidad también se ha convertido la puerta trasera para que las amenazas externas puedan obtener accesos a información confidencial o la realización de ataques de denegación de servicio y todo esto por una mala planeación o concepción al momento de implementar una nueva tecnología en este caso IoT.

Los estándares de seguridad para IoT están emergiendo aceleradamente dado los recientes reportes de brechas de seguridad en dispositivos de IoT lo cual hace que las compañías corran contra el reloj para proteger sus activos de información de las intrusiones externas e internas, pero también estos estándares metodologías recomendaciones y marcos de endurecimiento para nuevas compañías que están en el proceso de implementación son de gran ayuda para ayudar a mitigar los riesgos de seguridad en IoT.

REFERENCIAS

[1] Gotay, A. (2015, Marzo). Una breve historia del Internet de las cosas [Online]. Disponible en: http://www.tecnopr.com/una-breve-historia-del-internet-de-las-cosas/

[2] Cisco. (2011, abril). INTERNET DE LAS COASAS COMO LA PROXIMA EVOLUCION DE INTERNET LO CAMBIA TODO [Online]. Disponible en: http://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

[3] Gotay, A. (2015, Marzo). Una breve historia del Internet de las cosas [Online]. Disponible en: http://www.tecnopr.com/una-breve-historia-del-internet-de-las-cosas/

[4] Gartner. (2015, Noviembre). Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. 2015 PRESS RELEASE [Online]. Disponible en: http://www.gartner.com/newsroom/id/3165317

[5] Gartner. (2015, Noviembre). Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. 2015 PRESS RELEASE [Online]. Disponible en: http://www.gartner.com/newsroom/id/3165317

[6] Cobb, S. (2016, Octubre). 10 cosas que debes saber sobre los ataques DDoS a la IoT del 21 de octubre [Online]. Disponible en: http://www.welivesecurity.com/la-es/2016/10/26/ataques-ddos-a-la-iot-octubre/

[7] Microsoft. (2016, Noviembre). ARQUITECTURA DE SEGURIDAD DE INTERNET DE LAS COSAS [Online]. Disponible en: https://docs.microsoft.com/es-es/azure/iot-suite/iot-security-architecture

[8] Microsoft. (2016, Noviembre). ARQUITECTURA DE SEGURIDAD DE INTERNET DE LAS COSAS [Online]. Disponible en: https://docs.microsoft.com/es-es/azure/iot-suite/iot-security-architecture

[9] Microsoft. (2016, Noviembre). ARQUITECTURA DE SEGURIDAD DE INTERNET DE LAS COSAS [Online]. Disponible en: https://docs.microsoft.com/es-es/azure/iot-suite/iot-security-architecture

[10] Cisco. (2015, Marzo). SECURITY: THE VITAL ELEMENT OF THE INTERNET OF THINGS CONSULTING REPORT [Online]. Disponible en: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/vital-element.pdf

[11] Cisco. (2015, Marzo). SECURITY: THE VITAL ELEMENT OF THE INTERNET OF THINGS CONSULTING REPORT [Online]. Disponible en: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/vital-element.pdf

[12] Cisco. (2015, Marzo). SECURITY: THE VITAL ELEMENT OF THE INTERNET OF THINGS CONSULTING REPORT [Online]. Disponible en: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/vital-element.pdf

[13] Cisco. (2015, Marzo). SECURITY: THE VITAL ELEMENT OF THE INTERNET OF THINGS CONSULTING REPORT [Online]. Disponible en: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/vital-element.pdf

[14] Grau, A. (2016, Febrero). IOT SECURITY STANDARDS – PAVING THE WAY FOR CUSTOMER CONFIDENCE [Online]. Disponible en: http://www.standardsuniversity.org/e-magazine/march-2016/iot-security-standards-paving-the-way-for-customer-confidence//

Virguez Lozano, Jorge Alberto. Ingeniero Electrónico de la Universidad de San Buenaventura, con conocimientos y certificaciones en diversos ámbitos de Redes y Seguridad, como Cisco, Fortinet y Checkpoint.

Desde 2013 ha tenido experiencia en áreas de soluciones de redes y seguridad