EL ESTADO DEL ARTE SOBRE EL INTERNET DE LAS COSAS. AMENAZAS Y VULNERABILIDADES DE SEGURIDAD INFORMÁTICA EVIDENCIADAS DESDE LA DOMOTICA.

ING. CESAR MAURICIO ACOSTA MOLINA

Escuela de Ciencias Básicas, Ingeniería, Tecnología e Ingeniería – ECBTI,
Especialización en Seguridad Informática,

Bogotá, Colombia.

2019.

EL ESTADO DEL ARTE SOBRE EL INTERNET DE LAS COSAS. AMENAZAS Y VULNERABILIDADES DE SEGURIDAD INFORMÁTICA EVIDENCIADAS DESDE LA DOMOTICA.

Trabajo de Monografía como requisito de grado para optar el título de:

Especialista en Seguridad Informática.

Yolima Esther Mercado Palencia

Director.

Escuela de Ciencias Básicas, Ingeniería, Tecnología e Ingeniería – ECBTI,
Especialización en Seguridad Informática,

Bogotá, Colombia.

2019.

Nota de aceptación:

Firma del presidente del jurado

Firma del presidente del jurado

Firma del presidente del jurado

Bogotá D.C., Fecha (día, mes, año)

Buscando el camino de la decisión, determinación y disciplina encontrare el camino adecuado a cualquier cosa que me proponga en la vida.

Dedicado a la disciplina, constancia, el esfuerzo diario por querer salir adelante para ser una mejor persona, que quiere ayudar a su familia, amigos y sociedad en general.

“El allá es un espejo en negativo. El viajero reconoce lo poco que es suyo al descubrir lo mucho que no ha tenido y no tendrá."

Italo Calvino.

CONTENIDO

LISTA DE FIGURAS.

GLOSARIO:

IoT: *Internet of Things* “Internet de las cosas”.

TLS: Seguridad de la capa de transporte.

C: Computación en la nube La computación en la nube es una característica muy utilizada de Internet de las cosas, en la que varias aplicaciones y servicios se alojan y entregan a través de Internet en lugar de requerir nueva infraestructura, personal o software en el terreno.

D: Domótica como término indica las confluencias de "doméstica" y "robótica" y forma la base de muchas innovaciones de Internet of Things. Estos incluyen sistemas de domótica, robots de servicio autónomo como el Roomba vacuum y sistemas de seguridad en red. En el Internet de las cosas, estos dispositivos a menudo tienen capacidades de comunicación de máquina a máquina.

IDS/IPS: Sistema de Detección de Intrusos/ Sistema de Prevención de Intrusos.

M: máquina a máquina (M2M): La tecnología de máquina a máquina (M2M) se refiere a la comunicación automática entre dispositivos sin intervención humana. PC Magazine señala que esto se puede lograr a través de un sistema de sensores remotos que transmite continuamente datos a otro sistema centralizado (como sistemas de detección meteorológica, etiquetas RFID y lecturas automáticas de medidores).

M2P: Maquina a Persona.

RFID: Identificación de Radio Frecuencia.

SSL: Capa de conexión segura.

SQL: Lenguaje de Consulta Estructurado.

SSH: Interprete de Órdenes Seguras.

Computación ubicua. La informática ubicua está siempre presente y siempre encendida. En el Internet de las cosas, los microprocesadores están integrados en los dispositivos cotidianos, lo que les permite conectarse constantemente a una red y recopilar y transmitir información.

UHF: Frecuencia Ultra alta.

VPN: Red Privada Virtual.

WEP: Privacidad Equivalente a Cableado.

WPA/WPA2: Acceso Wi-Fi Protegido / Acceso Wi-Fi Protegido versión 2

INTRODUCCION

Internet de las cosas o sus siglas en inglés (IoT). Integra dispositivos de *hardware*, software, nanotecnología, inteligencia artificial, identificadores de radio frecuencia (RFID), Con la capacidad compartir información a través de la red automatizándose sin la necesidad del talento humano.

Teniendo en cuenta la evolución de las comunicaciones, tecnología, El internet de las cosas es una tecnología que está en auge, pero sin embargo los usuarios se basan más en la funcionalidad, descuidando la seguridad de sus dispositivos ya que, de forma paralela, alguien le esté robando su información.

Por este motivo, a través de la monografía se hace un análisis que puede identificar claramente las vulnerabilidades y las posibles amenazas y luego de este análisis plantear posibles acciones que logren mitigar o de ser posible eliminar el riesgo para así poder disfrutar esta tecnología de una manera más segura aplicando buenas prácticas y los mejores mecanismos de protección.

Este documento, tiene como propósito generar conciencia, una visión clara a los consumidores acerca del conjunto de problemas al usar esta tecnología, por ejemplo; la seguridad de los datos, seguridad física, seguridad lógica, ataques como, *Botnets* y ataques DDoS, *spam*, *Ransonware*, intrusiones en el hogar, comunicación con niños, ataques personales, Grabación remota, se realiza una serie de recomendaciones acerca del uso adecuado de la red, sea cableada o *wifi*, evidenciando algunos métodos de seguridad y criptografía.

Dentro de esta nueva tecnología de los dispositivos inteligentes IoT, en las viviendas y edificios inteligentes, es de vital importancia de conocer sus usos, beneficios que trae, facilita la tarea, reduce tiempos, permite controlar todo desde el celular, las luces, cerraduras, cámaras, audio doméstico, puerta de garaje, persianas de las ventanas, y cualquier cosa con un enchufe. Estos nuevos dispositivos son geniales, pero es bueno conocer todos los riesgos asociados al implementar esta tecnología.

DEFINICIÓN DEL PROBLEMA.

La seguridad es una preocupación primordial cuando se implementa los dispositivos IoT. Incluso sin darse cuenta puede ser parte de una *botnet,* y estar siendo comprometido con delincuentes informáticos.

La seguridad en los dispositivos IoT, es un compromiso de los fabricantes, consumidores, y gobiernos, a medida que implementan aplicaciones y soluciones de IoT, debe abordar importantes cambios de paradigma, así como desafíos operativos, estratégicos y comerciales. Con ellos enfrentar diversos problemas de seguridad interna y externa como ataques de red, *malware, software* malicioso y piratas informáticos, hackers maliciosos que amenazas a la seguridad de la vida humana.[1] Los atacantes de una *botnet* alimentada con IoT en 2016 cuando la *botnet Mirai* derribó sitios web importantes como *Reddit, Twitter* y GitHub. A pesar de los daños, no se produjeron cambios significativos en la industria de la IoT. De hecho, los consumidores continúan comprando e implementando dispositivos IoT con poco cuidado fuera de la garantía de que el dispositivo funciona y el precio es bajo. Los fabricantes continúan bombeando nuevos dispositivos IoT a un ritmo rápido, a menudo intercambiando seguridad por usabilidad y asequibilidad.

0.1 ***Antecedentes del problema.***

Desde el punto de vista de la seguridad IoT, los fabricantes de dispositivos no están pensando y contemplado los riesgos y vulnerabilidades asociados al utilizar esta tecnología, la seguridad está en un proceso de transición y el consumidor no están dispuesto a pagar tanto, ya que los dispositivos inteligentes IOT, en las viviendas y edificios inteligentes tienen ciclos de remplazo corto, como por ejemplo, la seguridad de los datos ya qué diariamente los dispositivos están enviando y recibiendo información de diferentes partes. También lo que tiene que ver con la Seguridad en el software, hardware, red, nube, servidores configuración, funcionalidad, infraestructuras, consumidores y ataques reales que se pueden llegar a materializar, debido al aumento de los ciberdelincuentes, y a la falta de a actualizaciones para parchar vulnerabilidades, también por desconocimiento de los usuarios dejando puertas traseras y facilitando el trabajo a los delincuentes informáticos.

[1] CISCO. The Vital Element Of The Internet Of Things {En Línea}. 2015. {11 de Marzo de 2018}. Disponible en: https://www.cisco.com/c/dam/en_us/.../iot/vital-element.pdf

0.2 ***Formulación del problema.***

¿Qué beneficios o inconvenientes de seguridad informática, puede causar el uso del internet de las cosas, evidenciado desde la Domótica?

Trae a los hogares, viviendas edificios inteligentes miles de beneficios, ayuda a optimizar el tiempo en las actividades, minimizando los tiempos de respuesta en base a las necesidades, ya que esta tecnología cuenta con dispositivos inteligentes dotados con sensores, actuadores, controladores, y transductores con el fin de ayudar a mejorar la calidad de vida y la seguridad de las personas, en los hogares, industria y sociedad en general.

EL uso de la IoT, presentan muchas soluciones ya sea para tareas cotidianas, sencillas, complicadas, técnicas, especificas, este avance tecnológico aporta a la sociedad, empleo y una mejor forma para la vida, ya que son capaces de analizar, diagnosticar y ejecutar funciones eliminando posibles errores humanos.

Toda esta tecnología de dispositivos del IoT está dirigida, a una interacción con capacidad de aportar a la sociedad, aplicaciones para negocios, la salud, industria, agricultura, multimedia, ambiente, aeronáutica, militar y ciudades inteligentes.

El Internet de las cosas contribuye en la protección en seguridad en el hogar, viviendas edificios inteligentes, brinda la posibilidad de estar conectado en línea otorga vigilancia y seguridad física, brinda tranquilidad y permite por medio de la aplicación en el móvil ver la casa, desde cualquier lugar, verificando todos sus entornos, sistemas de detección de intrusos, termostatos cuando no estén en ella.[2]

El Internet ha dejado de ser utilizado solo para las personas, con el avance de la ciencia, las evoluciones tecnológicas, está integrando dispositivos inteligentes la vida cotidiana. Cambiando la forma de interactuar de las personas, la conectividad de los dispositivos inteligentes ha evolucionado tanto en los hogares que ya todo

[2] WAUGH, Rob. Seguridad en Internet de las Cosas: cómo proteger ... – WeLiveSecurit. {En Línea}. 2014. {11 de mayo de 2018}. Disponible en: https://www.welivesecurity.com/la-es/2014/11/25/seguridad-internet-de-las-cosas

puede ser inteligente. Desde la ropa hasta la puerta del garaje, todo puede ser inteligente. [3]

Para las viviendas, edificios y hogares el uso del internet de las cosas, es de vital importancia ya que cuenta con dispositivos conectados a la red y que son capaces transmitir datos información de los dispositivos IoT, conectados interactuando con los usuarios. Cuenta con sistema de iluminación inteligente, para el ahorro de energía eléctrica, puertas inteligentes, con sensores de presencia que censan y se abren automáticamente, sensores detectores de intrusos que emiten señales de alarma luminosas, ruido, sensores de temperatura para mantener la temperatura deseada.[4]

0.3 ***Descripción del problema.***

Los ataques dirigidos a los dispositivos inteligentes IoT, la seguridad y privacidad de los datos generados y transmitidos por los dispositivos inteligentes IoT, pueden caer a manos de terceros, es un tema candente a nivel mundial, debido al aumento de la ciberdelincuencia en todos los ámbitos, robo, secuestro de datos, modificación de datos, espionaje industrial, entré gobiernos a nivel general todos los dispositivos IoT, son vulnerables a todo tipo de ataques ya sean físicos, o por medio de tecnologías inalámbricas, se contempla falta de estándares globales aceptados, seguridad lógica, aplicación de barreras para resguardar los datos, falta de conciencia dirigida a la seguridad de los miles de dispositivos conectados en el mundo, se convierte en una problemática actual para mejorar. En la actualidad la mayoría de dispositivos IoT están conectados a la red de redes, estos dispositivos inteligentes IoT, cómo: teléfonos inteligentes, tabletas, PC, consolas de juegos, cámaras de seguridad, Smart, estufas neveras, puertas inteligentes, etc. están conectados en línea y se accede a ellos remotamente por medio de una aplicación que los controla por medio del celular, debido a toda esta interconectividad cada día se hacen más vulnerables los usuarios, viviendas, edificios inteligentes, empresas y sociedad en general, esta tecnología hecha con el fin de quitar las tareas monótonas repetitivas, con la intención de facilitar la vida a los usuarios, llegara el día que se convertirán en un riesgo, amenaza que se puede llegar a materializar en arma de doble filo para la seguridad, ya que por medio de ingeniería

[3] REDACCIÓN GESTIÓN. El impacto de Internet de las cosas en la vida cotidiana | Tecnología... {En Línea}. 2014. {11 de Febrero de 2018}. Disponible en: https://gestion.pe/tecnologia/impacto-internet-cosas-vida-cotidiana-58481

[4] LONDOÑO ORTIZ, Roby Nelson. internet de las cosas. Manizales 2016, monografía presentada como requisito parcial para optar el título de tecnólogo en sistemas, universidad de Manizales.

inversa van a explorar todas las vulnerabilidades, llegara el momento en el cual se pierdan los privilegios de acceso, *hackean* el dispositivo y cobren recompensa para devolverlos, como ya pasa *Ransomware* cobrando por la información.

A partir de toda la información revisada y recolectada, de las referencias bibliográficas, encontraran algunas posibles contribuciones de medidas de protección en seguridad evidenciados desde la Domótica, para los dispositivos que estén conectados a Internet y concienciar en la necesidad de protegerlos.

0.4 ***Justificación.***

Este trabajo referente a determinar el estado del arte sobre la seguridad del internet de las cosas. Amenazas y vulnerabilidades de seguridad informática evidenciadas desde la domótica, busca dar a conocer el panorama poco alentador, acerca de las amenazas, vulnerabilidades y riesgos para los dispositivos del internet de las cosas, ya que con la integración de las nuevas tecnologías el mercado es muy amplio y presenta servicios que uno no se imagina ya que este tema Internet de Todo está aumentando masivamente, en la industria en el hogar, y en las (*Smartcitys*). Mirando a futuro, el mercado ofrecerá cantidades de dispositivos inteligentes para las diferentes clases de compradores, clases sociales. El mundo contara con millones de dispositivos conectados en línea compartiendo contenido en tiempo real remotamente censando, monitoreando, midiendo y valorando el estado de los hogares de los dispositivos conectados a la red, a través utilizando las redes publica o privadas.[5]

Internet de las cosas es una innovación tecnológica que permite transformar el entorno, gracias a la revolución industrial, revolución informática, avances y expansión de las redes de comunicaciones, la evolución rápida de la microelectrónica se convertido en la principal tendencia tecnológica en el siglo XXI, transformando lo que era una red global de personas en una “red global de todas las cosas conectadas” han permitido y facilitado que cada día todo este más conectado, permitiendo que los objetos cotidianos cobren vida y hagan parte de la vida diaria, con sensores y etiquetas RFID, a raíz de esta tecnología el mundo se encuentra más interconectado y gracias al gran impacto en la sociedad y los negocios, se abren mucha puertas para la economía, el trabajo, en la parte del software, hardware, comunicaciones, criptografía, seguridad informática, redes

[5] OPENMIND .El Internet de Todo - BBVA {En Línea}. 2016. {11 de Marzo de 2018}. Disponible en: https://www.bbvaopenmind.com/el-internet-de-todo/

cableado, programación, nanotecnología, Big data, donde se posibilita el interactuar entre maquinas, dispositivos IoT, personas, traspasando las barreras de tiempo y espacio.

Esta tecnología busca beneficiar a los usuarios, pero siempre se deben realizar los procedimientos de seguridad, conciencia, buenas prácticas, y políticas que permitan minimizas los riesgos, en área de la seguridad del internet de las cosas, trabajar en la prevención control de acceso, prácticas de codificación seguras, permitiendo a los consumidores comprar de forma masiva los diferentes dispositivos, y utilizar para mejorar la calidad de vida de la sociedad en general.

Busca mediante de una lectura bibliográfica, diferentes alternativas para prevenir ataques, dando a conocer medidas preventivas, referente al internet de las cosas, para seguir mejorando esta tecnología. “El IoT ha podido evolucionar principalmente a factores como el abaratamiento del hardware, las mejoras en miniaturización de componentes y un mejor acceso de cara al público a las tecnologías móviles”.

0.5 ***OBJETIVOS.***

0.6 ***Objetivo general.***

Realizar un estudio que determine el estado del arte sobre el internet de las cosas. Amenazas y vulnerabilidades de seguridad informática evidenciados desde la domótica.

0.7 ***Objetivos específicos.***

1 Realizar revisión bibliográfica, documentando acerca del estado del arte sobre el internet de las cosas desde sus inicios, actualidad y futuro.

2 Conocer los ataques actuales a los que se encuentra expuesto, acerca de las amenazas y vulnerabilidades de seguridad informática evidenciados desde la domótica.

3 Identificar y determinar las mejoras de seguridad mediante controles, procedimientos y medidas preventivas buscando la conciencia por parte de los usuarios en los diferentes dispositivos inteligentes del internet de las cosas.

4 Documentar acerca de las buenas prácticas, políticas de seguridad, aspectos físicos y uso seguro IoT, compartiendo medidas preventivas para identificar los riesgos a los cuales están expuestos los usuarios en los diferentes dispositivos inteligentes del internet de las cosas.

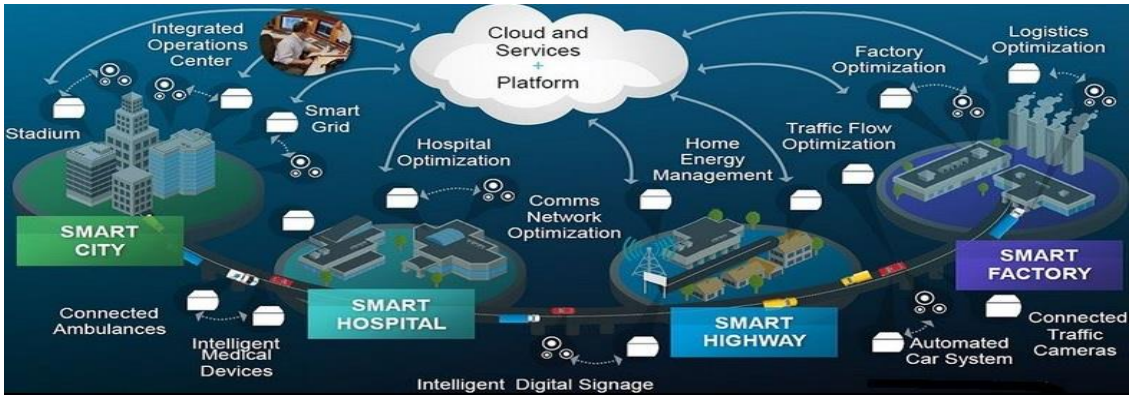
0.8 ***MARCO REFERENCIAL.***

Marco Teórico. Internet de las cosas hace referencia a un conjunto de objetos cotidianos conectados digitalmente a internet, entre los que debe existir algún tipo de intercambio de información para que estos objetos representados por la palabra (cosas) trabajen en el mundo de los datos.

0.9 ***Que es el internet de las cosas.***

6 En la Ilustración 1, se indica cómo trabajan los diferentes elementos del IoT, mostrando su relación entre clientes y servidores.

Ilustración 1 Funcionamiento del internet de las cosas.



Fuente: isp oligopoly 2017. [En Línea]. Disponible en Internet:http://drrajivdesaimd.com/wp-content/uploads/2016/07/iot-smart-1.jpg.

[6] BARRIGA DOMINGEA. Ana. Nuevos retos para la protección de datos personales. En la Era del..Madrid (2004) P29

El Internet de las cosas combina mundos físicos, digitales y virtuales, creando entornos inteligentes. Es un conjunto de objetos cotidianos conectados digitalmente a internet, la red entre los que debe existir sensores, actuadores, controladores, transductores y algún "tipo de intercambio de información para que estos objetos representados por la palabra (cosas) trabajen en el mundo de los datos."

0.10 ***Evolución IoT.***

En sus inicios los inventos el telégrafo, teléfono, radio y el computador abren las puertas para el avance tecnológico del Internet integrando las diferentes ventajas de los medios de comunicación, informáticos existentes para generar esa gran evolución de internet de las cosas, dispositivos inteligentes que logran la interacción comunicación redes, infraestructura e informática compartiendo información en todas partes del planeta.[7] La gran evolución en las grandes ciudades y la integración de las tecnologías de la información, y las comunicaciones, (TIC) y que convierte en el concepto de casa inteligentes (*Smartcitys*)".[8] Ha evolucionado en otros aspectos, en la medicina, industria, Aeronáutica, Domótica.

0.11 ***Arquitectura IoT.***

Contemplando su arquitectura de los objetos inteligentes IoT, el hardware, infraestructura y software, dotándolos de inteligencia para que actúen de manera física en los entornos, ciudades, viviendas, edificios y sociedad en general. Permitiendo la comunicación entre sensores, actuadores, maquinas computación en la nube, compartiendo el análisis de la información, su convergencia dará lugar al aprendizaje autónomos de los dispositivos inteligentes que aprenderán adaptarse y optimizarse por sí solos. [9]

---

[7] GARCIA, Luis. Estudio del impacto técnico y económico de la transición de internet al internet de las cosas (iot) para el caso colombiano.Colombia, 2015, p18, Trabajo de investigación (Magister en Ingeniería de Telecomunicaciones) Universidad Nacional de Colombia, Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial.

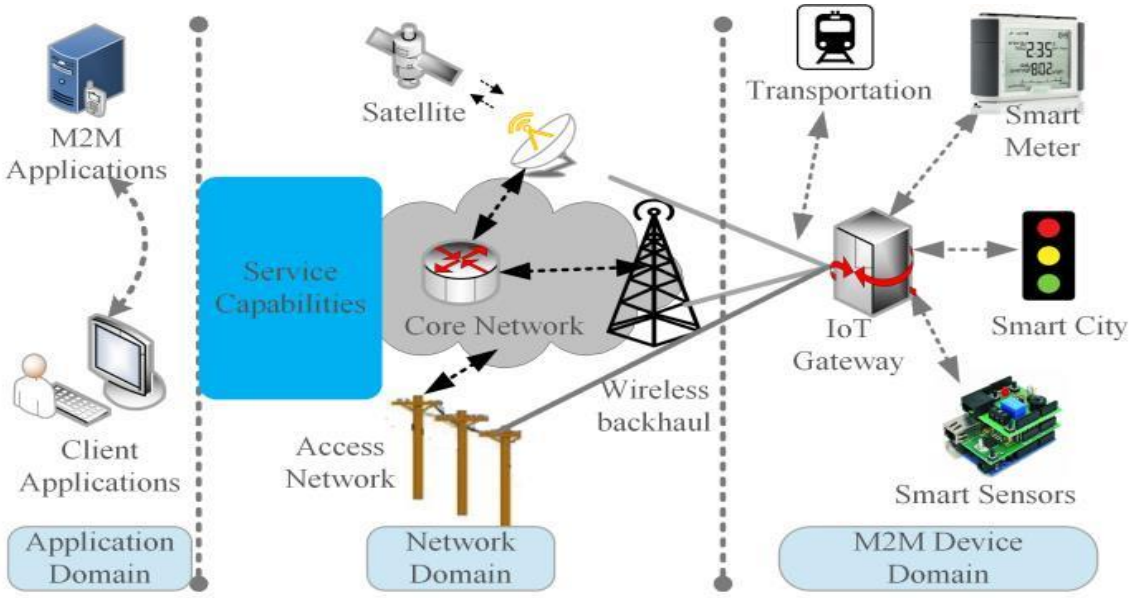
[8] TELEFÓNICA, F. Smart Cities: un primer paso hacia la Internet de las Cosas. Fundación Telefónica. {En Línea}. 2011. {11 deOctubre de 2017}. Disponible en: https://www.socinfo.es/.../1404smartcities6/01-TelefonicaSMART_CITIES-2011.pdf

[9] OCDE. sobre la economía digital. Microsoft, México. 2015 - Página 69

Arquitectura para Internet de las Cosas. Cuenta con la capa de aplicaciones que permite interactuar con los diferentes dispositivos inteligentes realizando los procedimientos de integración, las capas de gestión y seguridad en cargadas del correcto funcionamiento y la protección de los recursos de los diferentes dispositivos inteligentes.

En la ilustración 2 muestra una arquitectura de alto nivel de los sistemas de IoT, que se compone de tres dominios: el dominio de dispositivo, el dominio de red y el dominio de aplicación. En el dominio del dispositivo, el dispositivo proporciona conectividad directa al dominio de la red a través de redes de acceso, que pueden incluir tecnologías PAN de rango limitado, como Bluetooth, ZigBee, etc., o a través de una puerta de enlace que actúa como un proxy de red para el dominio de la red.

Ilustración 2 arquitectura de alto nivel de los sistemas de IoT.



FUENTE 2019 [En Línea]. Disponible en Internet https://www.researchgate.net/figure/High-level-IoT-architecture_fig1_281896657

0.12 ***Impacto IoT.***

El impacto de los diferentes dispositivos inteligentes conectados a internet como: teléfonos, pc, video juegos, electrodomésticos, cámaras, coches, medicina, juguetes, etc. Personas malintencionadas podría utilizar un dispositivo IoT con fines causar daño (robo, modificación, causar accidentes.) se destaca la vigilancia ilegal,

invasión a la privacidad. El estar conectado a la red tiene riesgo para los diferentes dispositivos inteligentes conectados, los cibercriminales pueden aprovechar la vulnerabilidades, puertas traseras para por ejemplo realizar un ataque de denegación de servicios (DoS), bloquear la puertas para que no se pueda ingresar a los hogares.[10]

0.13 ***IoT en los diferentes sectores.***

- Hogares. Permite automatizar el entorno, habitaciones, garaje, cocinas, sala, por medió de los dispositivos inteligentes IoT, permite la monitorización y control de forma remota por medio de app desde el teléfono.

- Ciudades; Lo podemos aplicar en el control y monitorización del tráfico, inspeccionar las casas, edificios, estructuras, puentes, por medio de sensores que nos muestres grietas.

- Automotores: En este campo se puede monitorear, mediante de los sensores que controlan, la gasolina, aceite, nivel del aire de las llantas, lo remite al computador del carro, podemos controlar su mantenimiento de esta manera.

- Salud; Se puede realizar por medio de Biosensores que nos ayudaran a prevenir enfermedades y a llevar una vida más sana. Ayudar a las personas mayores, a realizar con mayor eficiencia los tratamientos ya que los podemos monitorear.

- Agricultura y Ganadería; En el campo estas herramientas térmicas, como sensores se puede ayudar a monitorear el suelo, su nivel de humedad, temperatura, ayudando también a monitorear de forma individual el estado de cada planta, animales revisando su crecimiento y estado de salud.

[10] BALLESTIN PEREZ, Alberto. Internet de las cosas, España. 2015, p5, Trabajo de investigación (Grado en Ingeniería Informática) Universidad Politécnica de Valencia, Facultad Ciencias e Ingeniería.

- Medio ambiente; Sensores conectados, nos ayudan a recopilar información, acerca del suelo/aire/agua donde nos indican sus niveles de contaminación y polución.

0.14 ***Actualidad IoT.***

La actualidad de los dispositivos inteligentes IoT. ha impactado los entornos globales, de la forma como viven, piensan, la forma del conocimiento y actualidad humana, depende de las necesidades y usó por parte de los consumidores.

"Permite controlar remotamente el tráfico inteligentemente, que reúna los datos proporcionados por sensores, cámaras y semáforos en las calles de la ciudad, así como de los propios automotores en circulación. Para determinar la duración de las luces de los semáforos individualmente en tiempo real, y realizar los desvíos más conveniente de modo a evitar los atascos y reducir los tiempos de espera de los conductores" [11]

El estándar IEEE 802.15.4 está conformada por objetos que contienen sensores y transmisores embebidos, con capacidad para monitorizar y reaccionar en el ambiente donde operan. La lógica embebida también permite el control remoto y la monitorización, y proporciona la oportunidad para vigilar y analizar fuentes de datos con información constante, lo cual repercute en el manejo y búsqueda de datos en tiempo real.[12]

0.15 ***Marco conceptual.***

El Internet de las cosas (IoT) Comparte mucho en común con la tecnología de la Visión artificial mediante la diferentes aplicaciones innovadoras, permite el procesamiento en tiempo real de imágenes y videos para su visualización en la red, con la recolección de esta cantidad de datos el Big Date, se pueden generar dispositivos inteligentes para, edificios inteligentes, sistemas de vigilancia de personas y vehículos, entre otros 13 Orientada a mejorar el tráfico en las ciudades y permitir contar con ciudades inteligentes. Cualquier objeto es susceptible de ser

[11] ALCARAZI, Marcelo. "Internet de las Cosas" {En Línea}. 2014. {112 Junio de 2017}. Disponible en: http://jeuazarru.com/wp-content/uploads/2014/10/Internet-of-Things.pdf.

[12] Pinto, A. C., De la Hoz Franco, E., & Pinto, D. C. (2012). Las redes de sensores inalámbricos y el internet de las cosas. Inge Cuc, 8(1), 163-172.

[13]Alvear-Puertas, V., Rosero-Montalvo, P., Peluffo-Ordóñez, D., & Pijal-Rojas, J. (2017). Internet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones: Revisión de Literatura. Enfoque UTE, 8(1), pp. 244 - 256. https://doi.org/https://doi.org/10.29019/enfoqueute.v8n1.121

conectado, instrumentándolo para transformar nuestra forma de trabajar, vivir y hacer las cosas, en la actualidad traspasando las barreras de tiempo y espacio.

0.16 ***Domótica – IoT (Internet de las cosas)***

La domótica es un conjunto de tecnología integrada, que permiten dotar de inteligencia a los edificios y hogares.

Seguridad y Alarmas. Accesos con tarjeta, con tags, utilizando las huellas y/o con reconocimiento facial. Gestión eficiente del uso de energía Manejo automático de luces. Control de temperatura en los ambientes. Música centralizada en todos los ambientes. Centros de entretenimiento. (Cine - TV) 14 relojes, altavoces, luces, timbres, cámaras, ventanas, persianas, calentadores de agua, electrodomésticos, utensilios de cocina, lo que sea. Permiten enviarte información es el Internet de las cosas (IoT), y es un componente clave de las viviendas y las casas inteligentes.

Con estos dispositivos inteligentes prácticamente podemos automatizar la casa, desde cortinas de ventanas, luces, temperatura, cerradura hasta comederos para mascotas, con solo presionar un botón (o un comando de voz). Algunas actividades, como configurar una lámpara para encender y apagar a medida de las necesidades.

[14]BUREAUCORP, Domótica. IoT.(Internet of Things , Internet de las cosas) - {En Línea}. {11 de Marzo de 2018}. Disponible en: www.bureaucorp.net/domotica-iot/

En la ilustración 3 podemos mirar la conexión por medio de un multicable opcional, se hace posible la conexión de sistemas domóticos en *Trimline gasfire* y se pueden controlar las funciones básicas: Encendido apagado Fijación de llamas alta / baja Control de doble quemador DB Esperar.

Ilustración 3

Fuente: .thermocet 2019. [En Línea]. Disponible en Internet: https://www.thermocet.nl/en/products/trimline-optionals/198-domotica-connection.

Ventajas.

Ahorro de energía, al programar los dispositivos inteligentes IoT, bombillos, aire acondicionado, electrodomésticos para que prendan y apaguen cuando sea necesario con esto podemos ahorrar energía, ahorrar dinero, y contribuir con el medio ambiente.

Ventajas en cuanto a la seguridad en las viviendas y edificios, con los sensores de detección de intrusos prevenimos que personas no gratas entren a las casas, con

los sensores de incendio, de gas, agua nos protegemos de accidentes también por medió de las cámaras podemos vigilar las viviendas y edificios por medió de las aplicaciones instaladas en los *Smartphone*, verificando la seguridad de su casa, y la comodidad de controlar todos los dispositivos inteligentes IoT conectados en una sola app en su celular a Tablet desde un solo lugar.

Desventajas.

Precio elevado al momento de implementar los dispositivos inteligentes IoT en sus viviendas y edificios.

Una caída del sistema en la red, puede bloquear dejándolo sin la capacidad de censar y controlar y uso o fin de cada dispositivo inteligente IoT, para lo que fue diseñado.

Velocidad de transmisión de datos a los que se ve expuesta la red puede llegar a relentalizar el servidor y por ende los dispositivos inteligentes IoT.

Falsos positivos o des configuración del sensor de detección temprana de Sismo, en una vivienda o edificio, active la alarma, imagínense el caos y el temor que podría generar entre las personas.

0.17 ***Ciudad inteligente.***

En una ciudad inteligente, los sistemas y dispositivos múltiples están conectados entre sí. Comparten información para mejorar procesos como detectar luces de la ciudad, mejorar los flujos de tráfico, ahorrar energía y proporcionar información. Facilitando la interactividad con los ciudadanos.

Entre ellos encontramos.

- **Energía**: Servicios públicos y la red inteligente: Permiten a las empresas eléctricas prosperar en la actualidad, monetizar la red y garantizar la agilidad

para el futuro. Mejora la seguridad reduciendo el riesgo, mejora la seguridad de red, industrial y de IoT. Y hágalo mientras aumenta la seguridad, la excelencia operativa y el cumplimiento.

- **Petróleo y gas**: Mejora la prevención de incidentes, la seguridad de los trabajadores, la seguridad de la IO industrial, la integridad de la cadena de suministro y el cumplimiento normativo.

- **Transporte. Aviación**: Ofrezca nuevos servicios a pasajeros, trabajadores y arrendatarios para una mayor movilidad y colaboración.

- **Marítimo**. Ofrece una gestión de tráfico eficiente, enrutamiento de carga y seguridad para los puertos del mundo.

- **Ferroviaria.** Mejora la eficiencia operativa, simplifique el mantenimiento y proporcione Wi-Fi a bordo de los trenes, en la vía y en las estaciones.

- **Carreteras.** Ayuda a reducir la congestión del tráfico y ayude a salvar vidas proporcionando actualizaciones de seguridad y reencaminamiento dinámico para los viajeros. Vehículos Mejora las comunicaciones entre vehículos y vehículos a la infraestructura circundante, como las señales de tráfico.[15]

0.18 ***Futuro IoT.***

Contemplando el futuro IoT, busca el control del espacio de nombres de dominio y la forma de las próximas direcciones IP que se generan, por otra parte, la industria busca generar mayores ingresos para invertir en mejorar las para el crecimiento futuro del internet de las cosas.

- Los gobiernos opondrán resistencia al uso masivo de esta tecnología, ya que con los dispositivos IoT, podrían ser utilizados para espionaje. Por falta de

[15]CISCO. Internet de las cosas (IoT) - {En Línea}. {11 de Agosto de 2017}. Disponible en: https://www.cisco.com/c/es_co/solutions/internet-of-things/overview.html

estándares globales presentando preocupación por la seguridad y privacidad.

- Infraestructuras insuficientes, lentas con capacidad de conexión insuficiente, falta de modelos de negocios claros, falta de conocimiento de los usuarios.

- Desarrollo lento dé las nuevas aplicaciones tamaño de los sensores, consumo energético, regulación política lenta.

0.19 ***Marco Institucional IoT.***

Fabricantes, selecciono cisco entre muchos ya que nos brinda Herramientas para mejorar los procesos de negocio con una infraestructura de red inteligente. Aumentar la seguridad y la protección. Obtener información muy valiosa para los datos con el fin de optimizar la automatización.

0.20 ***Normativa.***

En Colombia el encargado de las normativas es el Ministerio de Tecnologías de la Información y las Comunicaciones que. Por medio de la Ley 1341 de 2009 "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"[16]

0.21 ***Fuentes:***

Documentos científicos (tesis de maestría, tesis doctorales, libros, publicaciones científicas y sitios de seguridad de la información confiables).

[16]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y. COMUNICACIONES, Internet de las cosas -… {En Línea}. {11 de Octubre de 2017}. Disponible en: www.mintic.gov.co/portal/604

EL ESTADO DEL ARTE SOBRE EL INTERNET DE LAS COSAS.

El Internet de las Cosas, conocido por (IoT), fue descrito por primera vez por el Instituto de Tecnología de *Massachusetts o Massachusetts Institute of Technology* (MIT), en el año 1999 comenzó a diseñar infraestructuras RFID identificadores de radio frecuencia (*Radio Frequency Identification*). En el 2002, su cofundador, Kevin Ashton, citaba en la revista Forbes: "Necesitamos un Internet de las Cosas, una forma estandarizada para que los ordenadores puedan entender el mundo real". Después en el artículo "El Internet de las Cosas" el primer archivo escrito y documentado. También en 1999 Neil Gershenfeld del MIT plasmo la misma idea en su libro "Cuando las cosas empiezan a pensar", cuando escribió: "parece que el rápido crecimiento de la *World Wide Web,* con esa idea clara fueron creándose entornos relacionados, para el uso de los dispositivos inteligentes IoT, conectados en línea, realizando en estos tiempos labores impensables, cambiando la forma de vivir" [17]

Internet of Things (IoT) es un nuevo paradigma que combina aspectos y tecnologías provenientes de diferentes enfoques. La computación ubicua, la informática ubicua, el protocolo de Internet, las tecnologías de detección, las tecnologías de comunicación y los dispositivos integrados se fusionan para formar un sistema en el que los mundos real y digital se encuentran y están continuamente en interacción simbiótica. El objeto inteligente es el componente básico de la visión IoT. Al colocar inteligencia en los objetos cotidianos, se convierten en objetos inteligentes capaces no solo de recopilar información del entorno e interactuar/controlar el mundo físico, sino también de estar interconectados entre sí a través de Internet para intercambiar datos e información.

Tecnologías sistema informático integrado. Permite el procesamiento de datos de los dispositivos, microcontroladores, algunas plataformas populares como Arduino, *Raspberry*. Fáciles de usar que permite armar su casa inteligente.[18] .

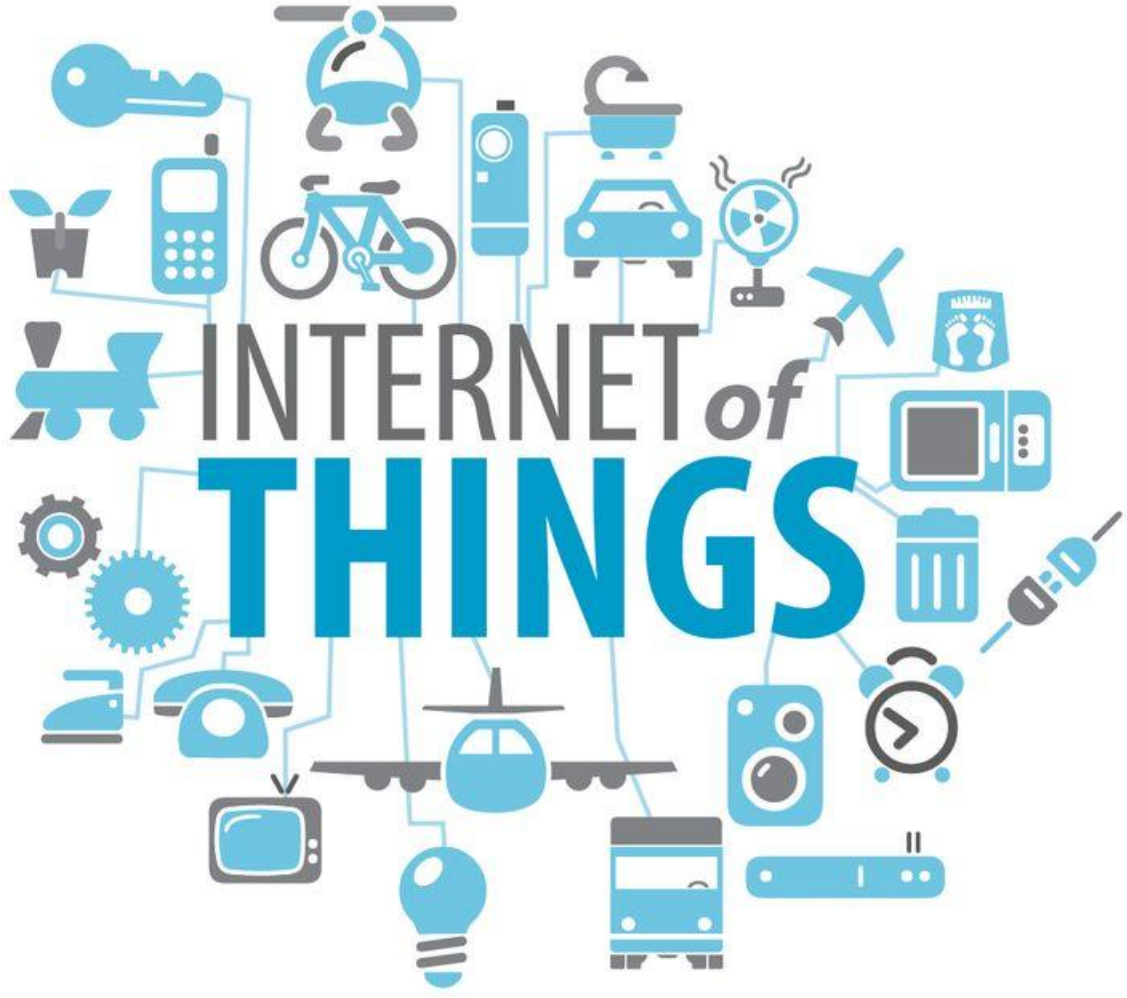
En la ilustración 4 encontramos que el Internet de las cosas ha evolucionado debido a la convergencia de múltiples tecnologías, análisis en tiempo real, aprendizaje automático, sensores de productos básicos y sistemas integrados, en los campos tradicionales de sistemas integrados, redes de sensores inalámbricos, sistemas de

[17] MATTERN. Friedemann, FLOERKEMEIEr, Christian. "From the Internet of Computers to the Internet of Things". Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich, Jul 2010.

[18] WEISER M. The Computer for the 21st Century. Sci. A.m. 1991; 265 : 94-104. doi: 10.1038 / scientificamerican0991-94

control, automatización (incluida la automatización de viviendas y edificios denominado DOMOTICA.) y otros contribuyen a habilitar el Internet de las cosas.

Ilustración 4 evolución IoT, integración de múltiples tecnologías.



Fuente insuredsoftware 2017 [En línea] Disponible en: http://insuredsoftware.net/internet-of-things/

0.22 ***Tecnologías relacionadas IOT.***

Se relacionada con nanotecnología, *Big data, RFID, NFC, EPC, M2M*, Computación Ubicua, identificación, localización y tecnologías de nube, procesadores, Arduino *Raspberry,* Inteligencia Artificial, se ha extendido a varios dominios o según el uso previsto de la tecnología.

0.23 ***Características.***

Un dispositivo IoT se caracteriza, por tener IP propia, tiene la capacidad de conectarse a la red ya sea cableada o inalámbrica deben ser, compatibles con otras plataformas, integra sensores, actuadores, receptores, controladores, Etiquetas RFID, nanoelectrónica, *software, hardware*, algoritmos, inteligencia artificial, para programar los dispositivos IoT, para permitir dotarlos con la capacidad de comunicarse mediante internet, proporcionando información de todo lo que sea posible medir. Capaces de analizar, diagnosticar y ejecutar funciones tecnológicas avanzadas desde cualquier sitio en cualquier lugar, y momento, dando vida a objetos cotidianos que nos rodean, y que hacen parte de la vida diaria.

0.24 ***Diferentes usos IoT.***

Entre los diferentes usos IoT, encontramos las Ciudades inteligentes la cual integra.

Estacionamiento inteligente, Salud estructural, Detección de Smartphone; Detectar *Phone* y dispositivos Android y en general cualquier dispositivo que funciona con *WiFi* o Bluetooth interfaces. Congestión del tráfico, Monitoreo de vehículos y peatones a optimizar rutas de conducción y a pie. Iluminación inteligente, Carreteras inteligentes, Contaminación del aire, Prevención de avalancha y deslizamientos. Detección temprana de los terremotos.

0.25 ***Domótica y automatización del hogar.***

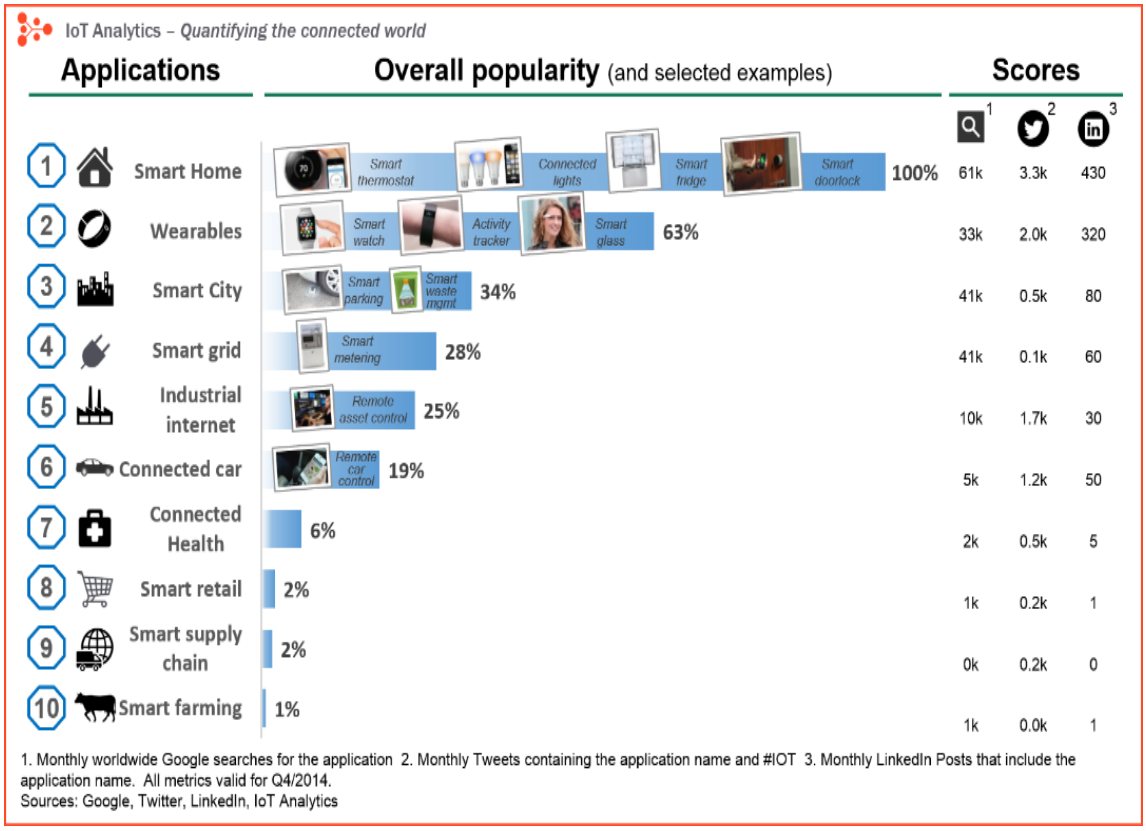
- Ahorro de energía y uso del agua, aparatos de control remoto, sistemas de detección de intrusos,

2.4.1 Salud. Detección de caída. refrigeradores médicos, cuidado de los deportistas. Vigilancia de pacientes. Monitoreo de las condiciones de los pacientes dentro de hospitales y el hogar de personas de la tercera edad.[19]

[19] LIBELIUM. Top 50 Internet of Things Applications - Ranking | … {En Línea}. {11 de Marzo de 2018}. Disponible en: www.libelium.com/resources/top_50_iot_sensor_applications_ranking

- En la ilustración 5 muestra el hogar inteligente como la aplicación del Internet de las Cosas más popular en este momento. Según un estudio del 2016 IoT, *Analytics.*

Ilustración 5 estudio IoT, Analytics aplicaciones más populares.



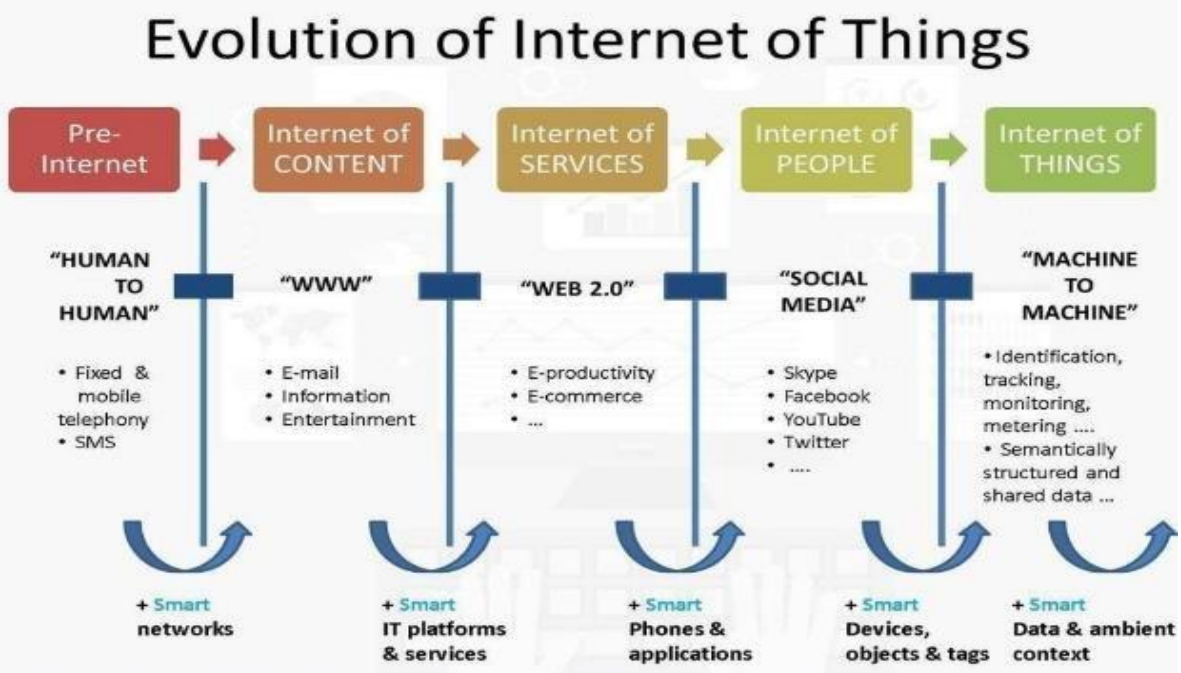
Fuente IoT, Analitys 2016 [en línea] Disponible en, https://iot-analytics.com/10-internet-of-things-applications/

0.26 ***Evolución de IOT.***

La evolución integrada desde el pre internet, después se crea el internet de contenidos como plataformas, siguiendo se ve el internet de los servicios con la integración aplicaciones más adelante encontramos el internet de las personas con la integración de las redes sociales, dispositivos y objetos conectados, y por último se evidencia el internet de las cosas que integra las maquinas interactuando identificando monitoreando todo lo que podemos tener conectado en línea transmitiéndolo, para poder controlar desde la comodidad de nuestro hogar o en el sitio donde deseemos.

En la ilustración 6, se ve la evolución IoT, desde el pre internet hasta el momento el internet de las cosas.

Ilustración 6 evolución of Internet of things.



FUENTE researchgate.net. 2016 [en línea] Disponible en: https://www.researchgate.net/figure/Evolution-of-IoT-https-twittercom-fisher85m-status-926360908900773889-II-IOT_fig1_329936193

1961 LA PRIMERA COMPUTADORA PORTÁTIL El matemático estadounidense Edward O. Thorpe, junto con el matemático Claude Shannon, inventaron la primera computadora portátil del mundo. El dispositivo del tamaño de un paquete de cigarrillos fue creado para predecir el movimiento de las ruedas de la ruleta.

1961 21 de noviembre de EL PRIMER ENLACE PERMANENTE "INTERNET" ESTABLECIDO Las universidades estadounidenses *UCLA y Stanford Research Institute* se conectaron con el primer enlace permanente de *ARPANET*, el precursor de Internet. Aproximadamente un mes antes, el 29 de octubre de 1969, el primer mensaje fue enviado: una comunicación de "nodo a nodo" desde UCLA a Stanford a través de computadoras por el programador estudiantil de UCLA; cada una tenía el tamaño de una casa pequeña). El mensaje, "INICIAR SESIÓN", fue breve y simple, pero de todos modos se estrelló en la red ARPA.: La computadora de Stanford solo recibió las dos primeras letras de la nota.

1962 LOS ORÍGENES DE LA COMPUTACIÓN EN LA NUBE. El psicólogo estadounidense y científico informático Dr. *Joseph Carl Robnett Licklider* escribió una serie de memorandos que exploran su idea de una "red informática intergaláctica". Imaginó un sistema de computadoras conectadas entre sí, y un espacio donde todos los datos están disponibles para todos desde cualquier lugar. Esta idea preparó el camino para la creación de interfaces bancarias en línea, bibliotecas digitales y computación en la nube.

1976 LA PRIMERA TARJETA CHIP El inventor francés Philip Moreno demostró que una tarjeta de plástico con un chip de computadora integrado en ella puede usarse para pagos electrónicos. A Moreno generalmente se le atribuye haber inventado la tarjeta inteligente, a la que llamó ("la carta de las pulgas"). La tarjeta tardó ocho años en hacerse popular en Francia, e incluso más tiempo en generalizarse en otros lugares. Las primeras pruebas de tarjetas bancarias ATM con chips se llevaron a cabo con éxito en 1984.

1979 LA PRIMERA FORMA DE COMPRAS EN LÍNEA El inventor y empresario británico Michael Aldrich demostró el procesamiento de las transacciones en tiempo real conectando un televisor doméstico a una computadora a través de una línea telefónica. Llamó a su invención televenta. Era un sistema en línea bidireccional y centralizada, que transmitía información en tiempo real, similar a cómo se muestran los horarios del aeropuerto hoy en día.

1981 LA PRIMERA COMPUTADORA DE PROPÓSITO GENERAL QUE SE PUEDE USAR investigador estadounidense Steve Mann diseñó y construyó una computadora multimedia portátil con capacidades inalámbricas. La computadora portátil aún no se había inventado, por lo que una computadora que funciona con batería era una novedad. La computadora también tenía capacidades de imagen. Mann llevaba el sistema en una mochila y tenía una pantalla CRT en el casco. Él llevó una lámpara para poder tomar fotos en la oscuridad.

1982 TCP / IP establecido como estándar el Departamento de Defensa de EE. UU. Declaró TCP / IP como el estándar para todas las redes informáticas militares. TCP / IP es un conjunto de protocolos de comunicación utilizados en redes de computadoras, que proporcionan conectividad de extremo a extremo para computadoras.

1983 Tecnología de identificación de frecuencia inventor Charles Walton patentó por primera vez el dispositivo de identificación por radiofrecuencia (RFID). El

dispositivo, que consiste en un pequeño chip y una antena, se utiliza para transferir datos de forma inalámbrica entre los objetos conectados. La tecnología se desarrolló por primera vez para espionaje en 1945.

1990 El primer sistema electrónico para rastrear el movimiento del personal Olivetti inventó un sistema de identificación electrónica para rastrear el movimiento del personal. La insignia transmite señales de infrarrojos, que son captadas por sensores en todo el edificio.

1990 08 de octubre La tostadora de Internet Los informáticos John Romkey y Simon Hackett conectaron una tostadora a Internet, convirtiéndolo en el primer dispositivo controlado a través de Internet. Usando una conexión TCP / IP, la tostadora podría encenderse y apagarse. La oscuridad de la tostada dependía de la duración de la tostadora. Un ser humano todavía tenía que insertar el pan. Un año después, se agregó un brazo robótico para recoger e insertar la rebanada de pan. El brazo también podría controlarse desde Internet.

1993 De Noviembre. La primera webcam del mundo La primera cámara web, transmitiendo el nivel de café de una olla en la Sala de Troya del Laboratorio de Computación de la Universidad de Cambridge, se conectó en línea. La cámara se instaló en 1991 para mostrarles a las personas en una red local que trabajaban en el edificio si había café en la olla individual del laboratorio o no. La transmisión se movió a la *World Wide Web* una vez que los navegadores fueron capaces de

2015 Sistema de ventilación inteligente para el hogar *Ecovent* sale a la venta *Ecoven*t, un sistema de ventilación inteligente que permite el control de la temperatura ambiente por habitación a través de una aplicación de teléfono inteligente sale a la venta. El kit *Ecovent DIY*, funciona con los sistemas existentes al agregar sensores de temperatura y movimiento a las habitaciones y reemplazar los respiraderos viejos por otros que se abren y cierran para regular la temperatura. Los sensores y las ventilas se comunican de forma inalámbrica. La temperatura se puede configurar para cada habitación individualmente. Cuando la habitación está vacía, las ventilaciones dejan de calentarla o enfriarla.

2016 Ropa inteligente para vencer a las pulseras inteligentes La firma de investigación Gartner predice que, para 2016, las prendas inteligentes, actualmente comercializadas solo para atletas, superarán a las pulseras inteligentes. En total, se predice que se venderán 26 millones de prendas inteligentes ese año, superando a las pulseras inteligentes en 7 millones de piezas.

En el 2017 Televisores inteligentes para dominar el mercado televisivo *Business Insider*, predice que para el año 2017, los televisores inteligentes representarán el 73% de los envíos globales de TV de pantalla plana.

2018 Más de la mitad del tráfico de Internet será generado por dispositivos que no sean PC De acuerdo con la predicción hecha por Cisco Visual *Networking Index (VNI),* en 2018 más de la mitad del tráfico de Internet será producido por dispositivos que no sean PC. En 2013, esta cifra se situó en el 33%. El crecimiento del tráfico generado por PC será solo del 10%, mientras que el crecimiento del tráfico para los televisores será del 35%, para las tabletas el 74% para los teléfonos inteligentes el 64%.

2018 Los envíos de dispositivos portátiles tocan más de 100 millones al año. La firma de investigación IDC predice que en 2018 los envíos de dispositivos portátiles ascenderán a 111,9 millones de unidades, diez veces más que en 2013. Los dispositivos de pulsera como los *smartwatches* y las bandas inteligentes seguirán dominando el mercado.

2018 Dispositivos móviles excederá la población mundial en la tierra Cisco predice que para 2018 habrá casi 1,4 dispositivos móviles por habitante. Habrá más de 10 mil millones de dispositivos conectados a dispositivos móviles en 2018, incluidos los módulos de máquina a máquina (M2M). Esto definitivamente excederá la población mundial de 7.6 billones en ese momento.

0.27 ***Las primeras visiones IOT.***

Ashton, por primera vez la frase *Internet of Things* en 1999 como el título de una presentación en la que vinculó el uso de RFID en la cadena de suministro de Procter & Gamble a Internet. Describió una visión en la que las computadoras serían capaces de recopilar datos sin ayuda humana y convertirlos en información útil, lo que sería posible con tecnologías como sensores e identificación por radiofrecuencia (*RFID*) que permiten a las computadoras observar, identificar y comprender el mundo[20]

[20]ASHTON. Kevin .That 'Internet of Things' Thing - 2009-06-22 - Page 1 - RFID Journal {En Línea}. {11 deMarzo de 2018}. Disponible en: www.rfidjournal.com/articles/view?4986

Sarma, Describe un mundo en el que cada dispositivo electrónico está interconectado y cada objeto, electrónico o no, está etiquetado electrónicamente con información relacionada con él[21] Dichas etiquetas permitirían obtener la información de forma remota y sin contacto, estableciendo los objetos como nodos en un mundo físico interconectado, análogo a Internet y considerado como un nuevo "Internet de las cosas". Un elemento clave para esta arquitectura fue el Producto Electrónico. Código (EPC) como un medio para identificar todos los objetos físicos y vincularlos a la red[22] Aquí, la red se entendía como un sistema ininterrumpido, omnipresente y de bajo costo que uniría automáticamente los objetos físicos a la Internet global, adoptando estándares en cooperación con los órganos de gobierno, los consorcios comerciales y los grupos de la industria.

Una propuesta más completa fue la llamada Internet de las cosas (IoT). Los posibles usos y beneficios de conectar objetos cotidianos a una red de datos se ejemplificaron en una serie de exhibiciones mejoradas con computadoras y sensores integrados. La intención con los dispositivos Inteligentes IoT, no era reemplazar la Internet existente, sino proporcionar una capa compatible debajo de ella, donde los dispositivos conectados dependen de los enrutadores, *gateways* y servidores de nombres existentes. Aquí, la idea original de Internet de vincular las redes informáticas en un todo sin fisuras se consideró factible de extender a las redes de todo tipo de dispositivos, un concepto conocido como inter redes. [23]

Una de las primeras contribuciones para definir y comprender el IoT fue el informe *Internet of Things*, de la Unión Internacional de Telecomunicaciones (UIT), publicado en 2005. Perspectiva de dispositivos y todo tipo de cosas convirtiéndose en usuarios activos de Internet en nombre de los seres humanos, con la mayoría del tráfico que fluye entre ellos, y una cantidad de conexiones activas que podrían medirse en términos de decenas o cientos de miles de millones. La conexión de objetos y objetos inanimados a las redes de comunicación, además del despliegue de redes móviles de mayor velocidad que proporcionan una conectividad

[21] SARMA S., BROCK DL, ASHTON K. The Networked Physical World; Centro de autoidentificación, Libro Blanco MIT-AUTOID-WH-001,{EnLínea}.2001.{1 de Marzo de 2018}. Disponible en: http://cocoa.ethz.ch/downloads/2014/06/None_MIT-AUTOID-WH-001.pdf .

[22] BROCK. DL El Código Electrónico de Producto (EPC); Centro de autoidentificación, Libro Blanco MIT-AUTOID-WH-002, {En Línea}.2001 {11 de mayo de 2018}. Disponible en: http://cocoa.ethz.ch/media/documents/2014/06/archive/MIT-AUTOID-WH-002.pdf .

[23] N. Gershenfeld, R. Krikorian, D. Cohen, “The internet of things”, Scientific American, vol. 291, no. 4, pp. 76-81, 2004. {En Línea}.2016. {3 de Marzo de 2018}. Disponible en: www.sciepub.com/reference/146435

permanente, cumpliría la visión de una red verdaderamente ubicua, "en cualquier momento, en cualquier lugar, por cualquier persona y cualquier cosa"

La UIT presenta el IoT como un mundo virtual que mapea el mundo real, donde todo en nuestro entorno físico tiene su propia identidad en el ciberespacio virtual, lo que permite la comunicación y la interacción entre personas y cosas, y entre cosas. Esta visión se basa en la aplicación de habilitadores tecnológicos claves que darían cuenta de una Internet expandida, capaz de detectar y monitorear los cambios en el estado físico de las cosas conectadas en tiempo real[24]

0.28 ***¿Cuál será el futuro del internet de las cosas?***

En el futuro todos los objetos en nuestra vida diaria estarán conectados a Internet. Los teléfonos móviles se usarán como el punto central o el control remoto para todos los objetos en el mundo físico comúnmente llamados IoT.[25] Los usuarios jóvenes usarán masivamente esta tecnología, caso opuesto de los consumidores mayores opondrán resistencia al cambio.

2020 Se esperan más de 900 satélites para su lanzamiento La compañía de investigación de mercado Frost and Sullivan predice que 927 satélites se lanzarán en 2020 para sostener y desarrollar la infraestructura espacial para complementar las necesidades de conectividad de la próxima generación.

2020 Internet de las cosas creando nuevos mercados y soluciones comerciales La investigación de *Gartner, Inc.* predice que habrá 26 mil millones de unidades conectadas al Internet de las cosas en 2020. IoT se expandirá a nuevos horizontes, como nuevos modelos comerciales, dispositivos móviles y micropagos. También permitirá un seguro calculado en base a datos de conducción en tiempo real, una gama más amplia de dispositivos y servicios de salud y estado físico, y así sucesivamente.

---

[24] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT) Internet of Things - ITU Internet Reports. ITU;Ginebra, Suiza: 2005. {En Línea}. {11 de Marzo de 2018}. Disponible en: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

[25] TYAGI, S., DARWISH, A. y KHAN, MY (2014), Gestión de la infraestructura informática para datos de IoT. Avances en Internet of Things, 4, 29-35. {En Línea}. {03 Marzo de 2018}. Disponible en: https://doi.org/10.4236/ait.2014.43005

2020 Internet de las cosas: ¿qué pasa con la Ciberseguridad? *ABI Research* predice que habrá más de 30 mil millones de dispositivos conectados de forma inalámbrica para 2020. Esta firma de investigación está preocupada porque *Internet of Things* se está convirtiendo en la próxima frontera para la ciberseguridad, pero el problema aún no ha ganado relevancia.

2020 India y la política de Internet de las cosas La India planea destinar 20 millones de dólares para cinco proyectos basados en sensores y basados en Internet dentro de su programa de desarrollo "IoT y 100 *Smart Cities* para 2020. Tiene como objetivo facilitar la vida de las comunidades rurales. Estos cinco servicios permitirían el monitoreo digital de la agricultura, el suministro de alimentos y agua y la contaminación ambiental para los agricultores y los trabajadores. El gobierno indio espera involucrar a asociaciones público-privadas en este programa.

2020 Se espera que el Internet de las cosas reduzca la emisión de gases de efecto invernadero en un 19% NGO Carbon *Room* predice que con la ayuda de dispositivos M2M, el Internet de las cosas puede reducir las emisiones mundiales de gases de efecto invernadero en 9.100 millones de toneladas métricas para 2020, equivalentes al 18,6 por ciento de las emisiones mundiales de gases de efecto invernadero en 2011. Esto será posible aumentando el Eficiencia energética de los sistemas de construcción, incluida la calefacción, refrigeración y ventilación, iluminación, electrodomésticos y sistemas de seguridad.

2024 Monitoreo de Gas a través de Internet Cisco estima que los gobiernos podrían ahorrar alrededor de $ 69 mil millones en 10 años mediante la conexión de medidores de gas a una red en línea. Esta red podría ayudar a los proveedores de energía a supervisar el uso de gas en todos los hogares. Reduciría sustancialmente los costos de mano de obra asociados con la lectura de los medidores de gas anualmente en cada hogar.

2024 Mercado global de drones civiles *Business Insider Intelligence* estima que para 2024, el 12% de los $ 98 mil millones estimados en el gasto global acumulado en drones aéreos será con fines comerciales y / o civiles. Se espera que los aviones no tripulados comiencen a asumir roles mucho más grandes para las empresas y algunos consumidores individuales. Pueden ser ampliamente utilizados en sectores como la ingeniería, la venta al por menor, el comercio electrónico, la agricultura, el medio ambiente, la gestión de recursos, el socorro humanitario, etc. Además, la expansión del mercado mundial de drones afectará a las industrias de componentes, como los fabricantes de GPS y sensores, así como al sector de TI.

Los gigantes de Internet, incluidos Facebook, Google y Amazon, también contribuirán a la expansión del mercado mundial de drones comerciales.

2025 Todos los automóviles conectados a Internet en 2025 BMW predice que el 100% de los automóviles estarán conectados en 2025.[26]

0.29 ***Nombre dado a las cosas del IOT.***

En el contexto del Internet de las cosas, una cosa se define como una entidad real /física o digital/virtual que existe y se mueve en el tiempo y el espacio y que puede identificarse.

Un nombre más comúnmente utilizado es el objeto inteligente. Kopetz considera que los objetos inteligentes son la base del IoT y los describe como elementos físicos cotidianos que se potencian con un pequeño dispositivo electrónico para proporcionar inteligencia local y conectividad al ciberespacio establecido por Internet.[27] *Aggarwal.* Vea los objetos inteligentes como ejemplos del *spime*, describiéndolos como computadoras diminutas que tienen sensores o actuadores, y un dispositivo de comunicación.[28] Los objetos inteligentes también se definen por sus características, como objetos que:

- Tener una encarnación física y un conjunto de características físicas asociadas.
- Posee un identificador único.
- Están asociados a al menos un nombre y una dirección.

---

[26] TIKI-TOKI. Internet of Things Timeline,{En Línea}. {10 Octubre de 2017}. Disponible en: www.tiki-toki.com/timeline/entry/.../Internet-of-Things-Timeline

[27] KOPETZ H. Real-Time Systems. Springer; Boston, MA, USA: 2011. Internet of Things; pp. 307–323.

[28] AGGARWAL C.C., ASHISH N., Sheth A. The Internet of Things: A Survey from the Data-Centric Perspective. In: Aggarwal C.C., editor. Managing and Mining Sensor Data. Springer; Boston, MA, USA: 2013. pp. 383–428{En Línea}. {05 Marzo de 2018}. Disponible en: https://link.springer.com/chapter/10.1007%2F978-1-4614-6309-2_12

- Puede detectar y almacenar mediciones hechas por transductores de sensor asociados con ellos.

- Tener un conjunto mínimo de funcionalidades de comunicación que les permita hacer que su identificación, mediciones de sensores y otros atributos estén disponibles para entidades externas, como otros objetos o sistemas inteligentes.

- Puede poseer medios para desencadenar acciones que tengan un efecto sobre la realidad física.

- Posee algunas capacidades básicas de computación que pueden usarse para tomar decisiones sobre sí mismas y sus interacciones con entidades externas.

- Por lo general, las cosas se conocen solo como objetos. Un objeto en el IoT se considera como cualquier máquina, dispositivo, aplicación, computadora, objeto virtual o físico involucrado en una comunicación que podría conectarse a Internet, y podría tener la capacidad de crear, solicitar, consumir, reenviar o tener acceso a información digital. [29]Existen conceptos similares a menudo mencionados en la literatura, como partes inteligentes, artículos inteligentes o productos inteligentes.

0.30 ***Propiedades de las cosas.***

- **Ubicación y seguimiento.**

  A medida que grandes cantidades de objetos se conectan al IoT, y siempre que puedan identificarse de manera única, los objetos individuales serán rastreados, su condición y ubicación comunicadas en tiempo real a un servicio de nivel superior. La forma en que las cosas se conectan al IoT, ya sea por cable o inalámbrica, proporciona una pista de dónde podrían estar en esta clasificación y su necesidad de ser rastreados. El seguimiento de una cosa no solo se refiere a conocer su ubicación física, sino también su historia individual, desde su fabricación hasta el final de su vida útil.

[29] ELKHODR M., SHAHRESTANI S., CHEUNG H. The Internet of Things: Vision & Challenges; Proceedings of the IEEE 2013 Tencon Spring Conference; Sydney, Australia. 17–19 April 2013; pp. 218–222. {En Línea}. {08 Marzo de 2018}. Disponible en: http://ieeexplore.ieee.org/document/6584443/

- **Detección.**

  Esta propiedad se refiere a la capacidad de las cosas para recopilar datos del entorno. La UIT denomina a las cosas equipadas con sensores como "cosas que sienten" y consideran que los sensores complementan los sentidos humanos. El uso de sensores como elemento clave del IoT se introdujo en las primeras visiones propuestas a fines de la década de 1990, aunque las primeras implementaciones del IoT se centraron principalmente en identificar, localizar y rastrear objetos. Con los sensores, las cosas pueden tomar conciencia de sus características, contexto y situación. Esto es, una cosa no solo proporciona información sobre su entorno, sino también sobre su estado.

- **Actuación**.

  Por medio de actuadores, las cosas pueden influir en su entorno. Esta actuación puede basarse en datos detectados y controlarse de forma remota a través de Internet y es fundamental para la automatización de procesos en las industrias, viviendas, edificios inteligentes, *Smartcytis.*

- **Tratamiento de datos**.

  La propiedad de procesar datos y ejecutar comandos se menciona con frecuencia como inteligencia. Implica que a medida que mejoran las capacidades de procesamiento de las cosas, pueden convertirse no solo en proveedores de datos sino también de servicios. Sin embargo, Jazayeri y otros proponen una característica interesante: para que los dispositivos de IoT se puedan enchufar y jugar fácilmente, cada dispositivo de IoT debe ser autodescriptivo e independiente para comunicarse con otros objetos o servicios, de modo que puedan describir y anunciarse a sí mismos y sus capacidades.[30] También implican una necesidad de interoperabilidad, ya que los protocolos de comunicación y la codificación de datos para dispositivos actuales de IoT generalmente son propietarios y diferentes entre sí.

---

[30] JAZAYERI M., LIANG S., HUANG C.-Y. Implementation and Evaluation of Four Interoperable Open Standards for the Internet of Things. Sensors. {En Línea}.2015 {09 Marzo de 2018}. Disponible en: http://www.mdpi.com/1424-8220/15/9/24343

AMENAZAS Y VULNERABILIDADES DE SEGURIDAD INFORMÁTICA EVIDENCIADOS DESDE LA DOMÓTICA.

Amenazas de seguridad existentes en los sistemas de IoT. A medida que más dispositivos inteligentes IoT, se conectan en el mundo se encontraran más vulnerabilidades presentes que se deben trabajar en los dispositivos por ejemplo; autorizar y autenticar los dispositivos, administrar las actualizaciones de los dispositivos, que tengan comunicación segura, asegurar la privacidad e integridad de los datos, aplicaciones Web, móviles y de nube seguras, asegurar alta disponibilidad, predecir y prevenir problemas de seguridad: desde el punto de vista de la seguridad de los dispositivos IoT, se podría implementar un enfoque de seguridad por diseño de múltiples capas, para administrar los dispositivos IoT, datos y aplicaciones , basados en la nube lo más importante es tomar todas las medidas de precaución y conciencia necesarios, ya que el tráfico de información digital se ha elevado, escuchamos, leemos con frecuencia acerca de las violaciones a la seguridad de *Internet of Things* (IoT) WikiLeaks reveló que los televisores conectados a Internet se pueden usar para grabar conversaciones en secreto.

Los fabricantes de dispositivos no están destinado dinero para eliminar las amenazas de los productos, las condiciones se siguen dando para nuevos ataques de *botnet* alimentado de IoT en el 2018. Como los hackers continúan refinando y mejorando su código de *botnet*, predigo que el próximo ataque será incluso más grande que el ataque de DDoS rompiendo récord causado por Mirai y que creará suficiente impacto a gatillo gobierno regulación de IoT.[31]

Los investigadores han descubierto una serie de ataques diseñados de tal manera que dejen de funcionar con eficacia los dispositivos inteligentes IoT, también ocasionan daño en los *routers* y otros dispositivos conectados a Internet. DOP ataque *bots* (diminutivo de "permanente denegación de servicio") buscar el Internet para *routers* basados en Linux, puentes y similares dispositivos conectados a Internet que requieren sólo las contraseñas por defecto de fábrica a otorgar acceso de administrador remoto. Una vez que los *bots* de encuentran un objetivo vulnerable, corren una serie de altamente debilitantes comandos que limpiar todos

[31] LALIBERTE. Marc analista de amenazas de seguridad de la información en WatchGuard Technologies, helpnetsecurity {En Línea}. {11 de Febrero de 2018}. Disponible en: https://www.helpnetsecurity.com/.../11/iot-botnets-security-regulation

los archivos almacenados en el dispositivo, corruptos de almacenamiento del dispositivo y cortar su conexión a Internet. .[32]

Las amenazas provienen de ciberdelincuentes aprovechando la cantidad de dispositivos inteligentes IoT conectados en las viviendas o edificios relacionados con la Domótica, aprovechando sus vulnerabilidades, puertas traseras explotadas por ellos mediante virus, debido al bajo nivel de *password* son fáciles de acceder.

Los fabricantes deben integrar de manera predeterminada, donde las funciones de seguridad estén configuradas en su configuración más segura en todo momento, y que los usuarios con poco conocimiento de seguridad no tengan acceso de como modificarlo y permitiendo mantener la privacidad e integridad de los datos. En la ilustración 7 se observa como un cibercriminal podría ingresar remotamente a los dispositivos inteligentes, y robar o manipular los datos.

Ilustración 7 cibercriminal tratando de ingresar a nuestros dispositivos IoT.

Fuente [en línea] Disponible en : http://www.mercado.com.ar/notas/8019460

[32] GOODIN. Dan, Rash of in-the-wild attacks permanently destroys … {En Línea}. {02 de mayo de 2018}. Disponible en: https://arstechnica.com/information-technology/2017/04/rash-of-in...

Básicamente las amenazas son provocadas por:

- **Personas:**

  Pero la verdad es que no se sabe con seguridad si son, Ciberdelincuentes, hacker, cracker, Intrusos remunerados, el gobierno, actores estatales, activistas, o investigadores.

- **Amenazas lógicas:**

  Software incorrecto, herramientas de seguridad, puertas traseras, bombas lógicas, canales cubiertos, virus, gusanos, caballos de Troya, programas conejo o bacterias.

- **Amenazas físicas:**

- Robos, sabotajes, destrucción de sistemas, cortes, subidas y bajadas bruscas de suministro eléctrico, condiciones atmosféricas adversas, catástrofes (naturales o artificiales como incendios).[33]

0.31 ***Tipos de ataques.***

El cibercrimen está evolucionando rápidamente con ataques cada vez más sofisticados cómo, atacar las plataformas, aplicaciones y los sistemas de mensajería de las red Domótica inteligente, también el Secuestro por medio de *Ransomware* de información almacenada en la nube de los servidores, igual por medio de extorsión a las personas utilizando micrófonos y cámaras, de igual manera por medio de grabaciones, fotos, vídeos, para posteriormente pedir recompensa para que sean devueltos los archivos, y no sean reveladas las fotos o videos. Ataques a dispositivos inteligentes IoT, en las viviendas y edificios Domótica.

[33] COSTAS, SANTOS, Jesús. Seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, {En Línea}. {11 de Mayo de 2018}. Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3228430.

0.32 ***Botnets y ataques DDoS.***

Muchas personas en el público en general se dieron cuenta de las amenazas de seguridad de IoT cuando escucharon sobre el *botnet Mirai* en septiembre de 2016. Según algunas estimaciones, Mirai infectó aproximadamente 2.5 millones de dispositivos IoT, incluyendo impresoras, enrutadores y cámaras conectadas a Internet. Los creadores de *botnets* lo usaron para lanzar ataques de denegación de servicio distribuida (DDoS).

0.33 ***Grabación remota.***

La posibilidad de que los atacantes pudieran piratear los dispositivos de IoT y registrar a los propietarios sin su conocimiento salió a la luz no como resultado del trabajo de los piratas informáticos, sino como resultado del trabajo de la Agencia Central de Inteligencia (CIA). Los documentos divulgados por WikiLeaks daban a entender que la agencia de espionaje conocía docenas de *exploits* de día cero para dispositivos IoT, pero no reveló los errores porque esperaban usar las vulnerabilidades para grabar secretamente conversaciones que revelarían las actividades de los adversarios estadounidenses.

0.34 ***Spam.***

En enero de 2014, uno de los primeros ataques conocidos con dispositivos IoT utilizó más de 100.000 dispositivos de conexión a Internet, incluidos televisores, enrutadores y al menos un refrigerador inteligente para enviar 300,000 correos electrónicos no deseados por día. Los atacantes no enviaron más de 10 mensajes desde ningún dispositivo, por lo que es muy difícil bloquear o identificar el origen del ataque.

0.35 ***Ransomware.***

Ransomware se ha vuelto muy frecuente en las PC domésticas y las redes corporativas. Ahora los expertos dicen que es solo cuestión de tiempo antes de que

los atacantes de *Ransomware* comiencen a bloquear dispositivos inteligentes. Los investigadores de seguridad ya han demostrado la capacidad de instalar *Ransomware* en termostatos inteligentes. Estos ciberdelincuentes Podrían, por ejemplo, subir el calor a 95 grados y negarse a volver a la normalidad hasta que el propietario accediera a pagar un rescate en *Bitcoin*. También podrían lanzar ataques similares contra puertas de garaje, vehículos o incluso electrodomésticos conectados. ¿Cuánto pagarías para desbloquear tu cafetera inteligente a primera hora de la mañana? Lo que me pidan por tomarme un tinto a primera hora del día, les pagaría a los atacantes.

0.36 ***Robo de datos.***

La obtención de datos confidenciales, como nombres de clientes, números de tarjetas de crédito, números de seguridad social y otra información de identificación personal, sigue siendo uno de los principales objetivos de los ataques cibernéticos. Y según el Instituto *Ponemon*, la filtración de datos promedio les cuesta a las compañías $ 3.62 millones, o alrededor de $ 141 por registro robado. Los dispositivos IoT representan un nuevo vector de ataque para delincuentes que buscan formas de invadir redes corporativas o domésticas. Por ejemplo, si un dispositivo o un sensor de IoT con protección inadecuada está conectado a redes empresariales, generaría una puerta trasera facilitando el accionar de los atacantes una nueva forma de ingresar a la red y potencialmente encontrar los datos valiosos que están buscando.

0.37 ***Intrusiones en el hogar.***

A medida que las cerraduras inteligentes y los abridores inteligentes de puertas de garaje, se vuelven más comunes, también es más probable que los Ciberdelincuentes se conviertan en ladrones del mundo real. Los sistemas domésticos que no están debidamente protegidos podrían ser vulnerables a los delincuentes con herramientas y software sofisticados. Inquietantemente, los investigadores de seguridad han demostrado que es bastante fácil entrar en las cerraduras inteligentes de varios fabricantes diferentes, y las puertas de garaje inteligentes no parecen ser mucho más seguras.

0.38 ***Comunicarse con niños.***

Una de las historias más perturbadoras de la seguridad de la IoT fue el pirateo de un monitor para bebés. Una pareja descubrió que un extraño no solo había estado utilizando el monitor de su bebé para espiar a su hijo de tres años, sino que también había estado hablando con su hijo sobre el dispositivo. La madre oyó una voz desconocida que decía: "Despierta, hijito, papá te está buscando", y el niño dijo que tenía miedo porque alguien estaba hablando con él por el dispositivo por la noche.

A medida que más equipos y juguetes para niños se conectan a Internet, parece probable que estos escenarios atemorizantes se vuelvan más comunes.

0.39 ***Ataques personales.***

Algunas veces, el *IoT* abarca más que solo cosas: también puede incluir personas que tienen dispositivos médicos conectados implantados en sus cuerpos. Un episodio de la serie de televisión *Homeland* presentaba un intento de asesinato dirigido a un dispositivo médico implantado, y el Exvicepresidente Dick Cheney estaba tan preocupado por tal escenario que tenía desconectadas las capacidades inalámbricas de su desfibrilador implantado. Este tipo de ataque aún no ha sucedido en la vida real, pero sigue siendo una posibilidad ya que más dispositivos médicos se vuelven parte del IoT.[34]

0.40 ***Accesos para obtener datos de los pacientes.***

A medida que la informática avanza, con las bases de datos de los hospitales, información personal, (Nombre, cedulas números de contacto, fecha de nacimiento dirección, correo, la acumulación de datos de las citas médicas, diagnósticos de los pacientes) toda esta información confidencial no encriptada, está al alcance de los Ciberdelincuentes.

[34] CYNTHIA. Harvey. Top 10 IoT Security Threats – Datamation {En Línea}.2018 {11 de mayo de 2018}. Disponible en: https://www.datamation.com/security/.../top-10-iot-security-threat.

El principal vector de ataque es su infraestructura débil. Para obtener datos de los pacientes:
Los sistemas informáticos por medio de los Servidores, estaciones de trabajo, y todos los equipos médicos conectados a la red, son vulnerables de monitorio y robo de la información, otro ejemplo son las pulseras inteligentes, marcapasos, monitores de bomba de insulina, también dispositivos móviles con funciones de seguimiento de indicadores de salud (teléfonos móviles, relojes inteligentes, otros sistemas de información, accesibles) a través de una conexión inalámbrica (Wi-Fi, Bluetooth, RF): electroencefalogramas móviles, oxímetros, sensores de eventos para monitorear pacientes de alto riesgo.[35]

0.41 ***Ataques inodoro inteligente.***

"En agosto de 2013, se informó que el inodoro inteligente Satis fabricado por la compañía japonesa Lixi fue pirateado de forma inalámbrica. En este caso los hackers utilizaron una vulnerabilidad de puerta trasera. El inodoro inteligente es vulnerable a través de la comunicación Bluetooth, integrada en el dispositivo. Los piratas informáticos pudieron abrir o cerrar remotamente la tapa del inodoro, descargar el inodoro y también activar la función de bidé integrada en el dispositivo".[36]

0.42 ***La cafetera inteligente.***

La máquina de café, también este dispositivo de cocina pueda ser un excelente medio para espiarte, permitiéndote que se deslice la contraseña de tu casa.

Sorprendentemente, el problema resultó ser muy difícil de solucionar, por lo que el proveedor aún no ha logrado solucionar el error. Sin embargo, la situación no es tan grave: la ventana de oportunidad temporal para un hacker dura apenas unos minutos. Sin embargo, el problema persiste incluso si cambia la contraseña de Wi-Fi: la máquina de café le regalará la contraseña una y otra vez.

---

[35]MAKRUSHIN. Denis Los errores de la medicina "inteligente" - Securelist {En Línea}.2018 {08 Mayo de 2018}. Disponible en: https://securelist.lat/los-errores-de-la-medicina-inteligente/84832/
[36] ESCAMILLA-AMBROSIO, P. J., SALINAS-ROSALES, M., Acosta-Bermejo, R., & Rodríguez-Mota, A. Internet de las Cosas: 50 Mil Millones de Puntos Inseguros. {En Línea}. {11 de Mayo de 2018}. Disponible en: Internet de las Cosas: 50 Mil Millones de Puntos Inseguros

0.43 ***Técnicas de ataque IoT.***

- **Interrupción.** Servidor Web no disponible.

- **Interpretación.** Accede intercepta y copia información de la comunicación transmitida.

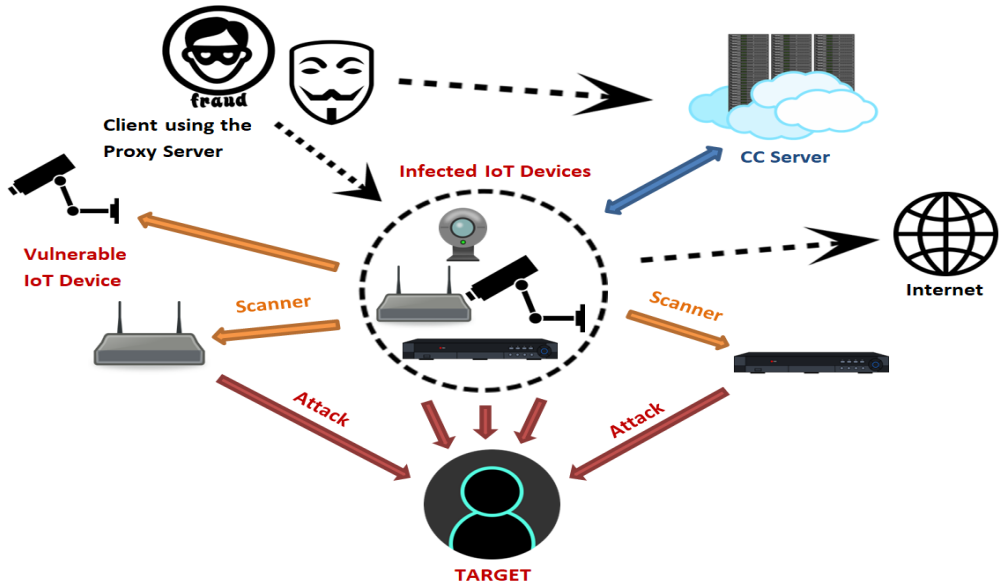
- **Modificación.** Accede y modifica o altera las cifras ejemplo una transacción bancaria.

- **Fabricación.**

El Ciberdelincuente se hace pasar por el destino de la transmisión para robar información.

En la ilustración 8 se muestra el diagrama de cómo se infectan los dispositivos y como pasan por medio de las arquitecturas servidores, e internet.

Ilustración 8 diagrama ataques e infección de dispositivos.



Fuente [En línea] Disponible en : https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers.html

0.44 ***Para conseguir su objetivo puede aplicar varias técnicas.***

3.6.1 Ingeniería social. La ingeniería social se puede lograr de muchas maneras, incluso a través de una computadora, usando una llamada telefónica, en persona o usando el correo postal tradicional. Hay tantas formas y variedades de ingeniería social que cualquier lista que pretenda catalogar todas las formas va a faltar a algunos de los métodos. Cuando la ingeniería social se origina en la computadora, generalmente se realiza mediante correo electrónico o en la web (aunque también se ha hecho mediante el uso de mensajería instantánea y casi cualquier otro tipo de programa informático). También usan ***Spoofing****, Sniffing, DoS (Denial of Service*, denegación de servicio). *DDoS (Distributed Denial of Service*, denegación de servicio distribuida.

0.45 ***Medidas de protección contra ataques de fuerza bruta.***

Adopte sistemas de defensa adecuados, como filtros de *spam, software antivirus* y *firewall*, y mantenga todos los sistemas actualizados, utilizar contraseñas no triviales, cambie las contraseñas con frecuencia, Bloquear o impedir ráfagas de intentos repetidos, establecer un máximo de fallos y después bloquear el acceso.

0.46 ***Tipos de atacantes:***

- **Hackers.** Los hackers están interesados en saber cómo funcionan las cosas. Les gusta explorar y descubrir los sistemas informáticos, la programación y las redes. Si bien algunos piratas informáticos solo pueden estar interesados en aprender las cosas que otros convierten su pasión en su profesión, lo que los convierte en hackers profesionales.

- **Cracker.** El propósito de un cracker es romper la seguridad de las computadoras y las redes. Es una actividad ilegal. Hacen uso de sus conocimientos para obtener ganancias personales y violar la seguridad en las redes. Adquieren un amplio conocimiento y aprendizaje sobre computadoras, su programación, software, códigos e idiomas y los utilizan para acceder a computadoras para obtener ganancias criminales.

- ***Script kiddie*.** Apenas se están iniciando, aprendices de hackers.

- **Programadores de *Malware***. Expertos una programación, buscan las debilidades del software y lo atacan.

- ***Sniffers*.** Se encargan de captura tráfico de red, y robar información interesante.

- **Ciberterrorista**. Crackers interesados en cuestiones políticas y económicas.[37]

0.47 ***Recogida de datos no autorizada:***

La recogida de datos no autorizada de sensores teléfonos, pulseras inteligentes, de las redes sociales, voz, texto, el principal objetivo de Big Data es aumentar la velocidad a la que los productos llegan al mercado, reducir la cantidad de tiempo y recursos necesarios para obtener la adopción del mercado, las audiencias objetivo y asegurar que los clientes permanezcan satisfechos.

- Incluso fuera de los negocios, los proyectos de *Big Data* ya están ayudando a cambiar nuestro mundo de varias maneras, tales como:

- Mejora de la atención médica: Esta recogida de datos es utilizada en la medicina para llevar estadísticas de las personas enfermas, sus comportamientos y por medio de análisis poder mejorar los medicamentos.

0.48 ***Debilidades Big Data.***

La integración del Big Data Trae muchos beneficios, pero como siempre pasa es utilizada con fines delincuenciales que puede traer consecuencias en las vidas de las personas, su seguridad la seguridad de los datos, todas las cosas que realizan

[37] ROA, B. J. F. (2013). Seguridad informática. España: McGraw-Hill España. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10692460&p00=firewall

en el día, sitios frecuentados, compras, la privacidad de las personas se está perdiendo, las aplicaciones piden autorización para la información pero las personas no leen , y dan acceso a todos sus datos valiosos, y los acumuladores de información las venden por cifras inmensas, para procesos de inteligencia artificial, para predecir nuestros comportamientos, con el propósito particular de las multinacionales, y gobiernos para ganar campañas políticas.[38]

0.49 ***Dispositivos inseguros.***

Muchos dispositivos IoT en sí mismos sufren de limitaciones de seguridad como resultado de sus capacidades informáticas mínimas. Por ejemplo, la mayoría no admite mecanismos suficientemente robustos para la autenticación, lo que deja a los administradores de red solo con alternativas débiles o, a veces, sin alternativas.

Antes de comprar un dispositivo inteligente IoT, Es recomendable investigar sus vulnerabilidades de seguridad, si el dispositivo usa una contraseña, asegúrese de que el dispositivo de IoT le permita cambiar su contraseña. (Algunos dispositivos vienen con contraseñas predeterminadas que no se pueden cambiar). Además, considere si es confiando en que el fabricante entregará actualizaciones de seguridad oportunas para combatir nuevos *malware* y amenazas de seguridad. Tener un dispositivo que está configurado para descargar fácilmente las actualizaciones de seguridad aumenta las posibilidades de que el dispositivo use las últimas protecciones.

0.50 ***El desafío de la seguridad IoT.***

En cuanto a la Domótica y las empresas deben consideran una estrategia de seguridad de IoT, que incluya administración y configuración de seguridad predeterminadas y la habilitación de la visibilidad adecuada de todos los dispositivos IoT. También contemplar la integridad, confidencialidad de la información,

[38] BERNARD. Marr, What is Big Data? A super simple explanation for everyone {En Línea}.2018 {11 de Marzo de 2018}. Disponible en: https://www.bernardmarr.com/default.asp?contentID=766

manteniendo la privacidad y la exclusividad de los datos, seguir trabajando en la infraestructura de IoT para que sean más agiles.[39]

0.51 ***El Código de prácticas exige que los fabricantes IoT:***

Garanticen el mínimo de ciberseguridad de los productos de tecnología que fabrican.

- Facilitar la instalación y el mantenimiento de dispositivos IoT.
- Garantizar la integridad del software y actualizaciones oportunas.
- Hacer que los servicios de IoT sean resistentes a las interrupciones.
- Tener una política de divulgación de vulnerabilidad y un punto de contacto (y responder a los informes de vulnerabilidad de manera oportuna)
- Asegúrese de que los datos personales estén protegidos de acuerdo con la ley de protección de datos y que los datos confidenciales estén encriptados.
- Facilitar a los consumidores la eliminación de datos personales en dispositivos y productos.
- Valide los datos de entrada y monitoree los datos de telemetría del sistema.
- Asegúrese de que las credenciales estén almacenadas de forma segura dentro de los servicios y en los dispositivos, y que las credenciales no estén codificadas.
- Asegúrese de que las contraseñas del dispositivo IoT sean únicas y no se puedan restablecer a ningún valor universal predeterminado de fábrica.
- Los fabricantes deben tener como prioridad la seguridad de los dispositivos IoT a medida que los desarrollan, y no recurran a la seguridad una vez que los dispositivos han sido fabricados, enviados y puestos en uso.

---

[39] CRICKET. Liu, Securing networks in the Internet of Things era - Help Net Security {En Línea}.2014 {04 MARZO de 2018}. Disponible en: https://www.helpnetsecurity.com/.../securing-networks-in-the-inte...

- Generando un esquema de etiquetado de productos para que los consumidores conozcan las características de seguridad de los productos en el punto de compra.

- Los dispositivos no fueron creados pensando en la seguridad. Envían y reciben información de diferentes partes sin una encriptación con la mínima seguridad.

- Falta de soporte para nuevos equipos que se descontinuaran dejando de sacar actualizaciones para parchear vulnerabilidades.

- **Autenticidad:**

Solo los usuarios legales deberían poder acceder al sistema o a información confidencial.

- **Autorización:**

Los privilegios de los componentes y aplicaciones del dispositivo deben ser limitados, ya que solo pueden acceder a los recursos que necesitan para realizar sus tareas.

- **Confidencialidad.**

La transmisión de información entre los nodos debe protegerse de los intrusos

- **Integridad:**

La información relacionada no debe ser alterada

- **Disponibilidad y continuidad:**

Con el fin de evitar posibles fallas e interrupciones operacionales, debe garantizarse la disponibilidad y la continuidad en la prestación de los servicios de seguridad.

- **Seguridad red,**

La seguridad de la capa de red se puede examinar en dos subcapas principales; inalámbricas y cableadas. Una de las acciones iniciales en la subcapa de seguridad

inalámbrica es el desarrollo de protocolos para la autenticación y la gestión de claves.[40]

0.52 ***Seguridad nube.***

LA seguridad en la nube para los dispositivos IoT serían los más débiles en este año 2018, y, efectivamente, así está siendo. El Internet de las Cosas es mucho más propenso a la contención de vulnerabilidades fáciles de explotar, lo que los convierte en objetivos cada vez más claros para los Ciberdelincuentes. Las soluciones de seguridad segmentadas, por ejemplo, la aplicación de firewalls en el perímetro de una red variable, no protegen los datos que ahora se encuentran en constante movimiento entre dispositivos, redes y nubes. Incluso entre los centros de datos,[41]

0.53 ***Riesgos y debilidades.***

Los Riesgos, debilidades y vulnerabilidades de seguridad de los dispositivos IOT, son una gran preocupación hoy en día, a la hora de querer implementarlas en las viviendas y edificios “Domótica” y organizaciones soluciones IoT; Sin embargo, la mayoría de las fabricantes no mitigan las amenazas a la seguridad existentes en estos dispositivos, los riesgos de seguridad de IoT podrían ser aún más significativos para el consumidor, por desconocimiento de las posibles amenazas y lo que deberían hacer para mitigarlas.

Con el flujo automático de información y la conexión entre dispositivos IoT, surge un nuevo conjunto de riesgos de seguridad cibernética. Si puede acceder a todos sus datos de forma remota, un ciberdelincuente también podría hacerlo, la naturaleza misma del IoT es la conectividad, pero con tantos dispositivos en una red, los hackers podrían tener múltiples puntos de acceso a su información, es por eso que la configuración de seguridad debe ser de vital importancia.

---

[40] JARA, A.J., LADID, L. and SKARMETA, A. (2013) The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4, 97-118.

[41] NETCLOUDENGINEERING. Seguridad en la nube para los dispositivos IoT | Ciberseguridad {En Línea}. {11 de mayo de 2018}. Disponible en: https://netcloudengineering.com/seguridad-dispositivos-iot/

La vulnerabilidad en los dispositivos IoT conectados se debe a que en muchos casos el ciclo de vida del *software* “el *firmware* “no es el adecuado, debido a que no hay actualizaciones o parches por parte de los fabricantes. En una mayoría, las contraseñas son asignadas por *defaul*t. A esto además se suma el poco conocimiento por parte del usuario.

Los atacantes encuentran diversas ventajas al atacar este tipo de dispositivos, pues tienen un bajo consumo de energía, son portables, son de bajo costo, están disponibles desde Internet y es posible configurarlos con herramientas *open source,* disponibles de manera gratuita.[42] La mayoría de *hackers* quiere lograr, el acceso a las viviendas y edificios tener acceso a los dispositivos IoT conectados para vigilar los movimientos, lugares y sitios que visiten, a qué hora entran salen, buscando robar la información, después cobren o simplemente que los llenen de virus, les roben las contraseñas con fines violación, a los sistemas biométricos, cámaras, sensores de movimientos, etc.

0.54 ***Riesgos y vulnerabilidades presentes en los dispositivos inteligentes IoT.***

Recursos limitados:

La mayoría de los dispositivos IoT, tienen capacidades limitadas en procesamiento, memoria y potencia, por lo que los controles de seguridad avanzados no pueden aplicarse eficazmente.

Debido a su bajo costo, fabricantes sin experiencia en el mercado, debido a esto los fabricantes descuidan la seguridad en el diseño de los dispositivos inteligentes IoT.[43]

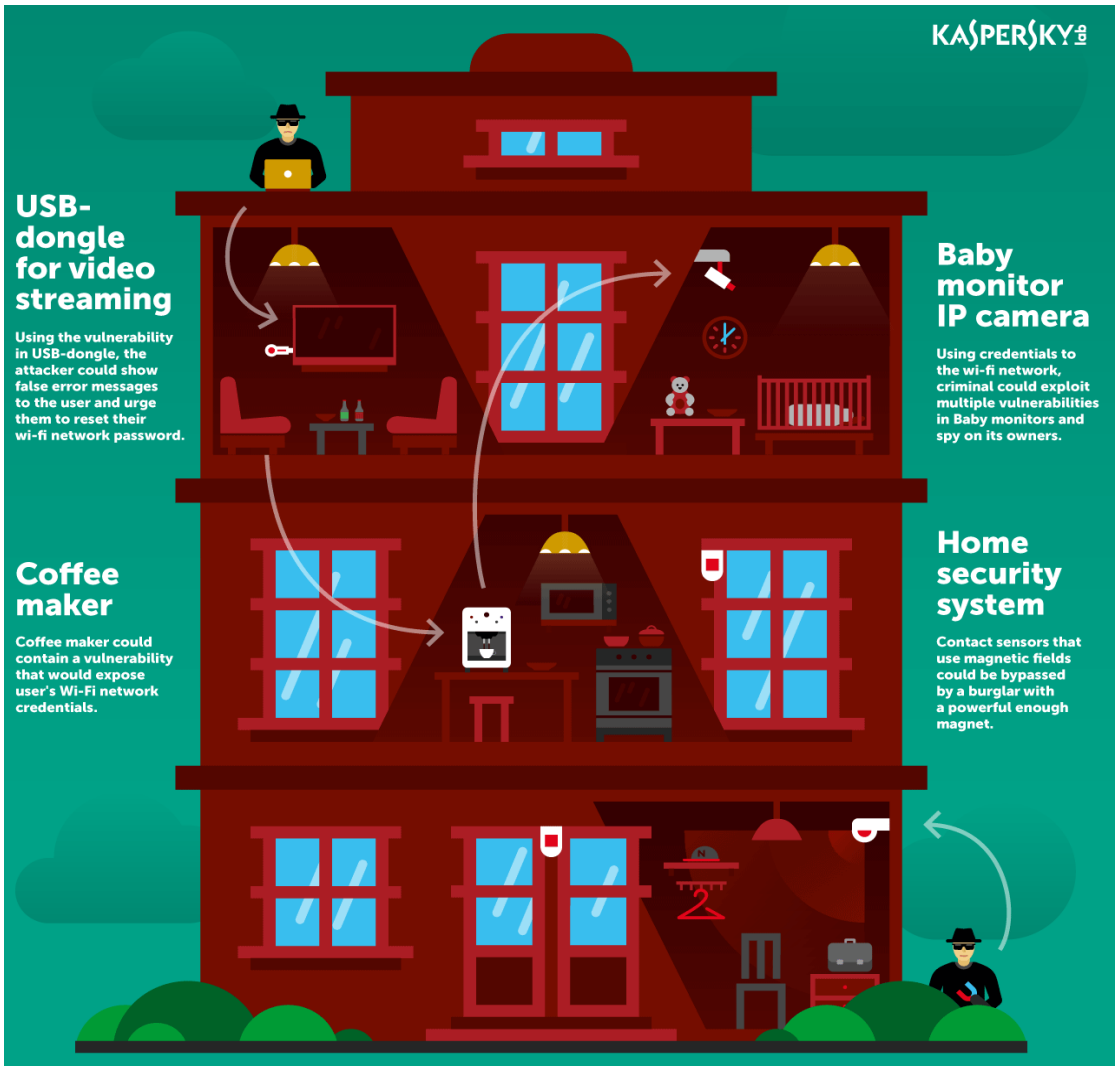
Seguridad débil en las plataformas, aplicaciones servidores, en la nube y en los sistemas de mensajería, dispuesto para el sistema de automatización Domótico.

[42] KASPERSKY LAB. detectó más 7,000 muestras de malware en dispositivos IoT a principios de año, {En Línea}.2017 {11 de mayo de 2018}. Disponible en: https://latam.kaspersky.com/.../kaspersky-lab-detecto...7000-muestras-de-malware-en...

[43] GARCÍA. Miriam, Puente, Riesgos y retos de ciberseguridad y privacidad en IoT | CERTSI {En Línea}.2017 {11 de Mayo de 2018}. Disponible en: https://www.certsi.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

Defectos de diseño en los dispositivos inteligentes IoT, con brechas de seguridad reales. En la ilustración 9 evidencia todos los dispositivos inteligentes pueden ser hackeables y podían ser fácilmente comprometidos y utilizados para hacer una oferta de un pirata informático.

Ilustración 9 diagrama donde se evidencia como atacan los delincuentes informáticos.



Fuente kaspersky 2015 [En línea] Disponible en: https://www.kaspersky.com/blog/surviving-iot/10480/

CONTROLES Y MEDIDAS PREVENTIVAS DISPOSITIVOS IoT.

Los mejores controles para los IoT, se basa en la prevención, conciencia acerca de la seguridad y las buenas prácticas en el uso y la codificación de la información evitando la vigilancia, modificación, alteración y manipulación de terceros. Para garantizar la confidencialidad, privacidad, integridad, confianza o no repudio de la información manejada por los dispositivos IoT, se requiere tener presente medidas preventivas, controles adecuados, y estar siempre actualizados de las últimas tendencias de ataques, para poder minimizarlos o evitarlos, en el mercado existen muchas solución por ejemplo, *Fireware, Ids, Ips, PKI*, métodos criptográfica de tipo firma Digital, para el cifrado tanto de archivos, como de las comunicaciones *(FTP, WEB, VPN*, CORREO).

0.55 ***Firewall de base de datos.***

Es una solución avanzada de seguridad basada en software con el objetivo de proteger de ataques o peticiones.

Esta solución la cual se compone de políticas o reglas de acceso, mejores prácticas, monitoreo, alertas entre otras se debe colocar o instalar en medio del servidor de aplicaciones o web o entre los usuarios y el servidor o gestor de Base de datos a proteger.

Dentro de las ventajas que tiene esta capa de seguridad esta no solo el bloqueo de las peticiones maliciosas sino la visibilidad especifica al lograr obtener una bitácora de las actividades que se llevan a cabo en las bases de datos, gracias a los sistemas de monitoreo o *logs* de auditorías con los que cuentan estos sistemas de seguridad. También algunos tienen la posibilidad de detectar las vulnerabilidades de las bases de datos, errores de configuración y las sugerencias para la corrección de estos, también podrían llegar a controlar ataques de *DoS*.

0.56 ***Por medio de Monitorización podemos controlar la red.***

La red constituye un entorno dinámico con cambios continuos en el que los usuarios están continuamente conectados a la red, enviando y transmitiendo información de todos sus dispositivos IoT conectados a los servidores, la nube donde se almacenan todos sus datos. Existen dos sistemas para enviar la copia del tráfico al analizador de redes:

- ***Port mirroring****.* Este sistema de monitorización se basa en configurar un dispositivo por el que pasa todo el tráfico de la red, como puede ser un *switch,* para que reenvíe una copia del tráfico que recibe a la herramienta de monitorización.

El puerto que conecta el analizador de la red con el *switch* recibe el nombre de *mirror* port o monitor port.

El funcionamiento de este sistema es simple: como todos los paquetes llegan al *switch,* se aprovecha esta circunstancia para reenviar una copia por el monitor port al equipo que analiza la red.

- -***Network tap.*** En esta forma de monitorización se utiliza un dispositivo hardware que permite acceder al tráfico de datos en un punto de la red donde no es posible usar *port mirroring*. El analizador de paquetes recibe todo el tráfico que le llega al dispositivo.[44]

0.57 ***Protección en redes inalámbricas.***

Las redes inalámbricas en la actualidad son muy utilizadas en las empresas y hogares. La seguridad de la red inalámbrica protege principalmente una red inalámbrica contra intentos de acceso no autorizados y maliciosos. Normalmente, la seguridad de la red inalámbrica se entrega a través de dispositivos inalámbricos (generalmente un enrutador/conmutador inalámbrico) que encripta y protege todas

[44] ESCRIVÁ, GASCÓ, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3217398.

las comunicaciones inalámbricas por defecto. Incluso si la seguridad de la red inalámbrica se ve comprometida, el hacker no puede ver el contenido del tráfico / paquete en tránsito.

Mecanismos de seguridad en una red inalámbrica solo deberían poder acceder a la red los equipos autorizados. Además, la información que circula por ella no debería ser comprensible para los equipos no legítimos. Por ello, las redes inalámbricas deben cifrar las comunicaciones y controlar la forma en que los equipos se autentican en la red. Estos son los principales mecanismos de seguridad utilizados en redes inalámbricas:

- ***WEP (Wired Equivalent Privacy).*** Es el mecanismo de seguridad utilizado por defecto por muchos puntos de acceso y *routers* inalámbricos en la actualidad. Presenta graves fallos de seguridad en el mecanismo de cifrado (RC4), con lo que un atacante podría obtener la contraseña muy rápidamente, por lo que se desaconseja su uso.

- ***WPA (Wireless Protected Access).*** Se le considera como un estadio intermedio en el camino desde el WEP hacia la implementación completa del estándar 802.11i.

- **(*WPA2).*** Ofrece una mayor protección que WEP, ya que proporciona una versión mejorada de RC4 e incorpora mecanismos de seguridad adicionales, como TKIP, pero se recomienda utilizar WPA2. WPA2. Se considera el mecanismo de seguridad más adecuado para redes inalámbricas y ofrece mecanismos de cifrado robustos (*AES, Advanced Encryption Standard*). Existen dos tipos de WPA2 (Personal y Enterprise) que se diferencian en los mecanismos de autenticación.

- ***WPA2 Personal o PSK.*** Su mecanismo de autenticación es PSK *(PreShared Key)*, en el que la contraseña se comparte entre el punto de acceso y los clientes de la red. Es la opción recomendada para redes domésticas.

- ***WPA2 Enterprise.*** Proporciona una mayor flexibilidad para gestionar los mecanismos de autenticación, pudiendo utilizarse un servidor de contraseñas aleatorias (servidor RADIUS) o diferentes tipos de protocolos EAP como usuario y contraseña, certificados digitales, tarjetas inteligentes (*smartcards*), etc. Es la opción recomendada para empresas. Existen otras

medidas que, en algunos casos, complican la gestión de la red o disminuyen el nivel de seguridad, por lo que pueden ser consideradas como falsas medidas de seguridad y se desaconseja su uso.

- **Filtrado de direcciones *MAC***. Esta medida crea una falsa sensación de seguridad, ya que puede ser fácilmente burlada mediante programas que cambien la dirección MAC del atacante.

- **Ocultación del *SSID*.** El problema de esta medida es que en este tipo de redes si los puntos de acceso no difunden el SSID, son las estaciones cliente quienes continuamente envían peticiones preguntando si esa red se encuentra dentro de su alcance. Un atacante podría aprovechar esta situación para suplantar la red y establecer conexiones. *Rogue ap,* en este tipo de ataque, un equipo se hace pasar por un falso punto de acceso al que se conecta el cliente, interceptando sus claves y toda la información que transmite por la red. Para evitarlo es importante mantener actualizados el sistema operativo, las aplicaciones que hacen uso de Internet y los *drivers* del dispositivo, no conectarse a redes inseguras y mantener la lista de redes preferidas actualizada, eliminando redes no utilizadas y redes que no difunden su *SSID* de esta lista.[45]

0.57.1 **Recomendaciones redes WIFI.**

Se recomienda el uso de protocolos WPA o WPA2 ya que son bastante fuertes, debemos tener en cuenta las mejores prácticas de seguridad, garantizando la seguridad de la información transmitida.

- Para algunos casos de usos de las redes *WiF*i, es recomendable cambiar la contraseña con frecuencia.

- No dejar la red inalámbrica abierta o sin condiciones de seguridad (Sin Contraseña)

[45] ESCRIVÁ, G. G., ROMERO, S. R. M., & RAMADA, D. J. (2013). Seguridad informática. España: Macmillan Iberia, S.A. {En Línea}. {11 de mayo de 2018}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820963&p00=seguridad+basica+en+redes+de+datos

- Cambiar la configuración por defecto del *router* (Direccionamiento y contraseñas de administración).

- De las opciones de Cifrado utilizar la más compleja de vulnerar en la actualidad es WPA2-PSK.

Otras Opciones de seguridad más avanzadas dispositivos IoT.

- Configurar que la consola de administración solo sea accedida mediante una conexión LAN o cable y prohibir que sea accedido por la red inalámbrica.

- Ocultar la red, haciendo que el SSID no se pueda ver a simple inspección de la red.

- Crear una lista de acceso por *MAC Address,* solo permitiendo los equipos conocidos.

- Estar monitoreando y comprobando los equipos conectados a la red.[46]

0.58 ***Los Sistemas de Detección de Intrusos (Intrusion Detection Systems , IDS).***

Son los sistemas encargados de detectar y reaccionar de forma automatizada ante los incidentes de seguridad que tienen lugar en las redes y equipos informáticos. La detección basada en la firma compara las firmas con los eventos observados para identificar posibles incidentes. Este es el método de detección más simple porque compara solo la unidad de actividad actual (como un paquete o una entrada de registro, a una lista de firmas) utilizando operaciones de comparación de cadenas.

[46] XATAKAHOME. Consejos de seguridad para redes WiFi, convierte tu red en una fortaleza inexpugnable, {En Línea}.2012 {20 Mayo de 2018}. Disponible en: https://www.xatakahome.com/la-red-local/consejos-de-seguridad-para-redes-wifi-convierte-tu-red-en-una-fortaleza-inexpugnable.

La detección basada en anomalías compara las definiciones de lo que se considera actividad normal con los eventos observados para identificar desviaciones significativas. Este método de detección puede ser muy eficaz para detectar amenazas desconocidas anteriormente.

0.59 ***Un sistema IPS (Intrusion Prevention System)***

Sistema de prevención de intrusos, controla el acceso a una red y previene ataques dando avisos al administrador y bloqueando el tráfico que pueda afectar el sistema de forma negativa.

- **Funcionamiento:**

Toman decisiones para controlar el acceso a los sistemas y a la red basándose en el tráfico de datos diferente a direcciones IP o los puertos.

Al igual que los IDS funcionan por módulos, pero la diferencia radica en que el IPS da una alerta al administrador ante un ataque. Comparando un IDS con un IPS se puede establecer que el IDS trabaja de forma reactiva mientras que un IPS de forma proactiva.

- **Características**:

IPS protege el sistema basándose en los registros, los cuales se evalúan gracias a la auditoría que realiza a las fuentes de datos, basados en la máquina o máquinas, en redes, en aplicaciones, en objetivos o híbridos que combinan las anteriores.

Los *honeypots y honeynets* proporcionan varios mecanismos para la monitorización, registro y control de las acciones de los intrusos. De este modo, permiten analizar cómo los intrusos emplean sus técnicas y herramientas para intentar entrar en un sistema o en una red informática (cómo consiguen analizar y explotar sus vulnerabilidades) y comprometer su seguridad (cómo pueden alterar o destruir los datos, instalar programas dañinos o controlar de forma remota los

equipos afectados). Además, estas actividades de monitorización y registro se realizan tratando de pasar de forma inadvertida para los intrusos.[47]

0.60 *Como combatir la amenaza de los virus y otros códigos dañinos.*

Recomendaciones para combatir de forma eficaz la amenaza de los virus y otros programas dañinos:

- ***Tests* de Penetración Internos** se llevan a cabo desde el interior de la red, mediante pruebas como el análisis de los protocolos utilizados y de los servicios ofrecidos; la autenticación de usuarios y la revisión de la política de contraseñas; la verificación de la seguridad lógica (permisos, acceso a recursos compartidos, restricciones en el uso de los servicios de red…); la explotación de agujeros de seguridad conocidos en los principales servicios y aplicaciones instalados, como los sistemas operativos, bases de datos o servidores de correo interno; el análisis de la seguridad en las estaciones de trabajo; la evaluación del comportamiento de los antivirus y otras herramientas de seguridad; el nivel de detección de la intrusión en los sistemas.

- ***Tests* de Penetración Externos** se realizan desde el exterior de la red de la organización, para tratar de forzar la entrada en algunos de sus servidores o comprometer su seguridad, mediante pruebas como el escaneo de puertos y la detección de los protocolos utilizados; el análisis del tráfico cursado, del rango de direcciones utilizado y de los servicios ofrecidos a través de la red; pruebas de usuarios y de la política de contraseñas; intentos de conexión vía Internet, líneas telefónicas, centrales telefónicas o redes inalámbricas; intentos de ataque de Denegación de Servicio (DoS); explotación de agujeros de seguridad conocidos.

- **Solución de seguridad integrada: *Symantec Gateway Security*.**

[47] GÓMEZ, VIEITES, Álvaro. Gestión de incidentes de seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3229340.

Estos dispositivos de seguridad integrados (“todo-en-uno”) incorporan, en sus últimas versiones, avanzados filtros de contenidos, protección contra programas espía (“*spyware* ”), filtros “*antispam* ”, protección contra intentos de estafas como el “ *phishing* ”, protección proactiva contra agujeros de seguridad detectados en navegadores y lectores de correo electrónico, etcétera.

Configuración de los cortafuegos para filtrar puertos que utilizan determinados troyanos y gusanos.

Configuración robusta de cada equipo informático: desactivación de innecesarios, cambios de contraseñas por defecto del fabricante.

Utilización de un Programa Antivirus permanente actualizado, que se encuentre siempre activo en el equipo informático. Para ello, conviene adquirir este producto a una empresa que ofrezca un buen soporte técnico a sus clientes, con servicios de alerta y una respuesta urgente ante nuevos virus.

Revisión de los registros de actividad (*“logs”*) de los servidores, cortafuegos y Sistemas de Detección de Intrusiones (IDS) para detectar qué equipos pueden estar realizando actividades sospechosas en la red. Escaneo de puertos para detectar posibles troyanos que se hayan podido instalar en equipos de la red.

0.61 ***Proteger las comunicaciones***

La protección de la comunicación requiere cifrado y autenticación para que los dispositivos puedan saber si puede confiar en un sistema remoto. Afortunadamente, las nuevas tecnologías como la criptografía de curva elíptica funcionan diez veces mejor que los predecesores en chips con recursos limitados, como chips de 8 bits y 8 MHz de IoT. Esto deja el núcleo desafío de administrar todas las "claves" para la autenticación. Como autoridad certificadora líder (CA), Symantec ya ha incorporado claves de "certificado de dispositivo" en más de mil millones de dispositivos IoT, ayudando mutuamente autenticar una amplia gama de dispositivos, incluidas estaciones base celulares, televisores y más.

0.62 ***Protección de dispositivos***

La protección de los dispositivos contra el ataque requiere la firma de código, para asegurarse de que todo el código esté autorizado para ejecutarse, y protección en tiempo de ejecución, para asegurarse de que los ataques maliciosos no sobrescriban el código una vez que se haya cargado. Firma de código criptográficamente asegura que el código no ha sido alterado después de ser "firmado" como seguro para el dispositivo, y puede hacerse en los niveles de "aplicación" y "firmware", incluso en dispositivos con solo una imagen monolítica de firmware. Todas

Los dispositivos críticos, ya sea un sensor, un concentrador o cualquier otra cosa, deben configurarse para que solo ejecuten código firmado y nunca ejecute el código sin firmar. Aun así, los dispositivos deben estar protegidos mucho después de que el código comience a ejecutarse. Las protecciones basadas en host ayudan aquí. Basado en host la protección proporciona el endurecimiento, el bloqueo, la inclusión de listas blancas, el espacio aislado, la prevención de intrusos frente a la red, seguridad basada en el comportamiento y la reputación, incluido el bloqueo, el registro y la alerta de una variedad de IoT sistemas operativos. Recientemente, algunas protecciones basadas en host se han adaptado para IoT, y ahora funcionan bien sin necesidad de acceder a la nube, y sin tensión excesiva en dispositivos limitados.

0.63 ***Entender su sistema.***

Por supuesto, no importa qué tan bien bloquee todo, y no importa qué tan bien maneje sus sistemas, algunas amenazas pueden derrotar todas esas contramedidas para establecer un punto de apoyo en sus sistemas. Por tales razones, es crucial tener una capacidad de IoT *Security Analytics* que lo ayude a comprender mejor su red al ayudarlo a detectar anomalías que pueden ser sospechosas o peligrosas, maliciosas o no.[48].

[48]SYMANTEC CORPORATION. Informe sobre las amenazas para la seguridad en Internet ... – Symantec {En Línea}. {11 de Marzo de 2018}. Disponible en: https://www.symantec.com/es/mx/security-center/threat-report

0.64 ***Firmas electrónicas es la criptografía.***

A nivel informático la criptografía está basada en logaritmos matemáticos permitiendo cifrar los datos y elementos como archivos, *software* y programas, donde se desea mantener la confidencialidad, integración y disponibilidad de la información, de esta forma la criptografía evita los accesos no autorizados, la interceptación de datos y también que no se pueda modificar y tampoco agregar datos sobre la información que únicamente compete entre quienes las transmiten y la reciben.

- **Cifrados de llave simétrica** llave equivalente tanto para el proceso de cifrado como para el proceso de descifrado de la información, tanto emisor como receptor conocen la clave.

- **Cifrado asimétrico** posee una mayor complejidad dos claves, la primera es pública y viaja con la información y la segunda es privada y solo la tiene el receptor. La combinación de las dos claves permite descifrar el mensaje.

- **Clave Publica** Se puede difundir sin ningún problema todas las personas que requieran enviar algo cifrado.

- **Clave Privada** Esta NO debe ser relevante nunca.

Permite cifrar los datos y elementos como archivos, *software* y programas, donde se desea mantener la confidencialidad, integración y disponibilidad de la información, de esta forma la criptografía evita los accesos no autorizados, la interceptación de datos y también que no se pueda modificar y tampoco agregar datos sobre la información que únicamente compete entre quienes las transmiten y la reciben.

Algunas medidas pueden ser:

- Fortalecer las credenciales de los usuarios e indicar que las contraseñas contengan seguridad aplicando combinaciones alfanuméricas y uso de mayúsculas.

- Aplicar las técnicas de criptografía necesaria para hacer difícil y accesible a los datos por parte de potenciales atacantes informáticos.

- Actuar y pensar como un atacante para identificar las vulnerabilidades que están expuestas para tomar los correctivos necesarios y si es el caso aislar temporalmente la red y que esta no pueda ser accedida por mecanismos, mientras se salvaguarda la infraestructura física y lógica como lo es la información.[49]

0.65 ***¿Herramientas PKI?***

Esta herramienta PKI, También las podemos utilizar para proteger ese intercambio de información; generados por los dispositivos IoT.

La infraestructura de clave pública en inglés (PKI) Comprende un conjunto de elementos de tecnología informática, con el fin de brindar seguridad en el intercambio y transacciones a nivel de datos, se ven involucrados; software, hardware y la criptografía. PKI contiene la infraestructura requerida para el manejo de claves y certificados, para lograr salvaguardar la autenticación, confidencialidad, integridad y no repudio en procesos cotidianos como son las transacciones comerciales, financieras que viajan por la red.[50]

0.66 ***VENTAJAS PKI.***

- PKI es una tecnología muy poderosa que puede ofrecer una variedad de servicios eficientes y confiables a través de Internet nos brinda confianza, privacidad y seguridad en cifrados.

- El cifrado puede proteger la información y la comunicación mitigando la pérdida de confidencialidad y accesos no autorizados a la información

---

[49] REYES, Krafft, Alfredo Alejandro. Las firmas electrónicas y las entidades de certificación, D - Universidad Panamericana, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3178023.

[50]LÓPEZ GARZÓN, Jose. Infraestructura de clave pública (PKI) para una pyme. Guayaquil, 2015. P 84, Magíster en Telecomunicaciones, Universidad Católica de Santiago de Guayaquil.

- Detección de cambios no autorizados en los datos transmitidos sobre las redes mitigando la pérdida de integridad

- Permite firmar los documentos digitalmente para garantizar la autenticidad del emisor garantizando el no repudio de los usuarios que originan los mensajes

- Crea, maneja, almacena, distribuye y revoca certificados digitales basados en criptografía asimétrica. Ahorro de recurso humano, tiempos, papelería, reducción de los robos electrónicos en las empresas gracias a esta herramienta PKI.

BUENAS PRÁCTICAS Y USO SEGURO IOT.

Como cualquier aspecto de la seguridad de la información, la seguridad de IoT no es absoluta y nunca se puede garantizar. Cada día se descubren nuevas vulnerabilidades y se debe mantener actualizados acerca de las amenazas, formas de ataque y los controles necesarios que se debe tomar en cuenta garantizado la seguridad.

En la actualidad los ataques de *Ramsomware*, es muy común, y en el último año generó bastante daño a nivel mundial, debemos generar conciencia y buenas prácticas para mitigar esta amenaza, buscando revisar los Riesgos, debilidades y vulnerabilidades de seguridad de los dispositivos con que contamos en las empresas y hogares, son una gran preocupación hoy en día, es necesarios implementar unas políticas de seguridad, que debe iniciar desde la capacitación y compromiso por parte de todo el personal que hace parte de las organizaciones, mediante el uso de políticas que minimicen los riesgos de sufrir un ataque informático, para ello es importante no compartir, ni descargar, ni abrir archivos de correos electrónicos dudosos, esto sería a nivel de usuario, pero deberá ir acompañado de fuertes acciones realizadas por parte del áreas de TI, en ello se deberán tener filtros de acceso de conexiones de red sospechosas, mantener las actualizaciones de seguridad sobre servidores y bases de datos, acompañados de copias diarias de los datos e información importante para las organizaciones, la Domótica, los gobiernos.

Medidas para reducir los riesgos a los cuales están expuestos los usuarios de los dispositivos inteligentes del internet de las cosas.

- Escanear monitorear, la red brindando privilegios a quien puede ver y modificar la información de los dispositivos inteligentes del internet de las cosas.

- Contemplar ataques reales y tener un plan de respuesta de incidentes, considerando los riesgos de seguridad de los dispositivos inteligentes del internet de las cosas.

- Actualizaciones de software, corta fuegos de los dispositivos inteligentes del internet de las cosas.

- Utilizar software legal, realizar Copias de seguridad periódicamente y guardarlas en sitios seguros usuarios IoT.

- Utilizar contraseñas fuertes en todos los dispositivos inteligentes IoT, en uso de credenciales para el ingreso de recursos informáticos.

- Restringir el acceso a datos y archivos importantes de los dispositivos inteligentes del internet de las cosas.

- Conciencia y sensibilización acerca de la seguridad de los dispositivos inteligentes del internet de las cosas.

0.67 ***Recomendaciones uso seguro de los dispositivos inteligentes del internet de las cosas.***

Al elegir un dispositivo que almacene información acerca de su vida personal y de las vidas de su familia, como un monitor para bebé, sería buena idea escoger el modelo RF más sencillo que exista en el mercado; el que sólo sea capaz de transmitir una señal de audio y que no se conecte a Internet.[51]

- Implemente *gateways* de seguridad: la capacidad de inspeccionar, auditar y controlar las comunicaciones dentro y fuera de su red es esencial a medida que aumenta el número, la variedad y la complejidad de los dispositivos conectados.

- Use una autenticación fuerte: muchos dispositivos de consumo aún se entregan con contraseñas predeterminadas débiles (admin / admin) que muchos usuarios no actualizan. Los fabricantes deben actualizar con contraseñas seguras antes de poder usar un dispositivo. En el mundo industrial donde los nombres de usuario y contraseñas no son factibles (o deseados) para cada dispositivo, se requiere un mecanismo alternativo para

[51] KASPERSKY LAB. Sobreviviendo en el mundo IoT: Expertos de Kaspersky Lab exponen... {En Línea}. 2018 {11 de Mayo de 2018}. Disponible en: https://latam.kaspersky.com/.../2015_sobreviviendo-en-el-mundo-iot-expertos-de-kas...

establecer identidad y confianza, como *blockchain*, especialmente cuando habilitamos más comunicación entre máquinas (M2M).

- Deshabilite los servicios no esenciales: muchos dispositivos se envían con telnet, FTP y otros servicios de alto riesgo expuestos a Internet.

- Utilice protocolos seguros: los protocolos como *HTTPS y SSH* están diseñados para admitir el cifrado y la autenticación sólida.

- Verifique la integridad de los datos: E l internet es un medio de comunicación no confiable y mientras protocolos como el TCP intentan introducir confiabilidad, las transferencias de datos pueden interrumpirse o corromperse, a pesar de los intentos maliciosos de secuestrar las comunicaciones. Para las comunicaciones críticas, además de la autenticación y el cifrado, recomendamos proporcionar una suma de comprobación o firma para permitir la verificación de la integridad de los datos.

- Planifique actualizaciones continuas: las vulnerabilidades críticas como *Shellshock y Heartbleed* siguen encontrándose en el corazón de los dispositivos conectados a Internet. Es esencial planear actualizaciones futuras para el software del dispositivo. Estas actualizaciones ocurrirán cada vez más en el aire y es posible que deban realizarse rápidamente dependiendo de la importancia de la actualización.

- Asegúrese de que los centros y servicios de gestión administrados por Internet y IoT sean seguros: si elige utilizar un concentrador o servicio que permita la administración de múltiples dispositivos IoT, tenga en cuenta que estos servicios pueden ser un punto de acceso central para comprometer todos sus dispositivos. Busque capacidades de seguridad robusta e integrada que se integrarán fácilmente en los sistemas existentes. Lo mismo ocurre con los dispositivos de IoT administrados por Internet; recuerde, el punto débil para estos dispositivos es cómo puede conectarse a ellos desde Internet.

- Varíe / cambie regularmente su contraseña: Esto parece algo dado estos días, pero vale la pena repetirlo. Asegúrese de no utilizar la misma contraseña para todos sus dispositivos IoT y trate de no utilizar su dirección

de correo electrónico "principal" como su nombre de usuario de IoT. Es una táctica común para los malos actores intentar *phishing* en su cuenta de correo electrónico para tratar de obtener su contraseña. Además, cambie regularmente su contraseña, cada 90 días como mínimo.[52]

- No dejar los dispositivos inteligentes IoT, con las contraseñas universales predeterminadas, y las credenciales o datos personales dentro del dispositivo deben almacenarse de forma segura, mientras que los dispositivos deben ser fáciles de configurar para los consumidores y eliminarlos nunca deben estar equipados con contraseñas universales predeterminadas.

0.68 ***POLÍTICA DE SEGURIDAD DISPOSITIVOS INTELIGENTES DEL INTERNET DE LAS COSAS.***

0.69 ***Políticas para obtener la seguridad de IoT correcta.***

El aspecto físico está relacionado con la seguridad física, control como de acceso físico a equipos, como en el de tener planes de contingencia y emergencia, así como de recuperación frente a desastres.

Para el caso de las viviendas y edificios “Domótica”, se debe definir las personas encargadas de realizar los mantenimientos correctivos, preventivos y el acceso a los mismos.

Como; Cámaras, dispositivos biométricos, sensores, encaminadores, especialmente los de perímetro de seguridad, Conmutadores y puntos de acceso inalámbrico, Servidores, especialmente aquellos que dispongan de la información más sensible del hogar.

Asimismo, la política de seguridad debe delimitar claramente la forma en la que se transporta información sensible en dispositivos físicos de procesado (portátiles, tabletas y teléfonos inteligentes) y de almacenamiento (discos sólidos, dispositivos

[52] CISCO IBSG, 8 Best Practices for Security Within the Internet of Things. {En Línea}.2011 {11 de Marzo de 2018}. Disponible en:https://www.netformation.com/.../8-best-practices-for-security-wit...

USB, etc.) móviles. Igualmente, debe haber unas normas claras sobre el control de acceso a los edificios donde estén situados los ordenadores y redes. [53]

Por otra parte, el papel importante que debe que debe realizar los gobiernos para generar estas políticas, puede involucrar a las partes interesadas a través de alianzas públicas privadas para promover el desarrollo, la seguridad y la privacidad de la IoT, y al mismo tiempo permitir la innovación tecnológica.

La flexibilidad normativa y reglamentaria será cada vez más importante en el desarrollo y la seguridad del IoT.[54]

[53] Procesos y herramientas para la seguridad de redes, UNED - Universidad Nacional de Educación a Distancia, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3220062.

[54] BROWN. Jamie, Three principles for getting IoT security policy right - Highlight ... {En Línea}. 2017{21 Mayo de 2018}. Disponible en:https://www.ca.com/...highlight/three-principles-for-getting-iot-se...

CONCLUSIONES.

A lo largo de este documento, se plasma los objetivos planteados, el propósito, acerca de la seguridad en el uso de los dispositivos inteligentes IoT, en la actualidad, la tecnología brinda miles de herramientas capaces de realizar muchas tares que se creía impensable, pero también va a causar miles de problemas relacionados, robo de información, monitoreo sin permisos accesos no deseados. Al mismo tiempo la gran cantidad de datos generados por emisores y receptores de los dispositivos inteligentes IoT, se necesitaran mecanismos de almacenamiento para procesar esta información ya que puede llegar a ser valiosa en algún momento, contemplando el aumento del tráfico de red los proveedores del servicio del internet deben analizar el aumento de su estructura, revisando el aspectos comercial y gubernamental mirando la posibilidad de la integración de distintas redes públicas y privadas que en algún momento se deben integrar para mejorar el funcionamiento de las tecnologías/arquitecturas y componentes IoT conectados, trabajando en conjunto fabricantes, consumidores y gobiernos para mejorar la conectividad, la estandarización de productos, y los protocolos.

Se encontraron y analizaron varias visiones y definiciones de Internet de las cosas. Es un poco complejo acertar con la definición exacta me quedo con dispositivos inteligentes IoT. Se pueden categorizar de diferentes maneras, dispositivos IoT, integra redes, servicios, comunicaciones, datos y cosas o dispositivos inteligentes IoT, esta integración de tecnologías permite brindar servicios basados en Internet y aplicaciones compatibles con dispositivos electrónicos conectados a elementos físicos para la adquisición de datos y procesos de control.

Los delitos informáticos están creciendo de forma desmesurada en cualquier lugar donde estemos conectados estamos expuestos a ser atacados por ciberdelincuentes, buscando un fin económico, por ambición de poder, odio, ocio o juego, venganzas laborales a nivel social, factores religiosos, ciberguerras.

Se debe tener aplicadas las mejores prácticas en seguridad informáticas, de acceso a muestras viviendas, para lograr una reducción del riesgo de materialización de ataques La importancia de la información debe empezar desde los mismos hogares, tomando conciencia sobre el manejo de la información de forma segura, de nada sirve que tengamos el mejor sistema de información actualizado y los mejores protocolos de seguridad, si los usuarios dejando la puerta abierta a los posibles ataques o filtraciones externas a la información crítica de la las viviendas y edificios inteligentes. “Domótica”.

Uno de sus temores o debilidades referente a los dispositivos inteligentes IoT, se centra en la gran cantidad de datos el Big data, recopilados por los sensores, y quien puede acceder a ellos y como se manejan.

El futuro los nuevos modelos de estudio del IoT, recientes están prestando más atención a las cosas o dispositivos inteligentes IoT, y lo que pueden hacer las cosas o dispositivos IoT, como parte de los nuevos servicios, aplicaciones y modelos comerciales inspirados en el IoT. Esta tecnología se encuentra en una etapa de maduración, evolución y su alcance comienza a ampliarse, descubrirse nuevos dispositivos IoT, mas usos, aplicaciones, más capacidades y posibilidades de mejorar la calidad de vida de los usuarios, en las viviendas, edificios, gobiernos, *smartcytis,* medicina, industria, agricultura, cuidado dl medio ambiente, etc.

BIBLIOGRAFIA.

AGGARWAL C.C., ASHISH N., Sheth A. The Internet of Things: A Survey from the Data-Centric Perspective. In: Aggarwal C.C., editor. Managing and Mining Sensor Data. Springer; Boston, MA, USA: 2013. pp. 383–428{En Línea}. {05 Marzo de 2018}. Disponible en: https://link.springer.com/chapter/10.1007%2F978-1-4614-6309-2_12. ALCARAZI, Marcelo. “Internet de las Cosas” {En Línea}. 2014. {112 Junio de 2017}. Disponible en:http://jeuazarru.com/wp-content/uploads/2014/10/Internet-of-Things.pdf.

Alvear-Puertas, V., Rosero-Montalvo, P., Peluffo-Ordóñez, D., & Pijal-Rojas, J. (2017). Internet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones: Revisión de Literatura. Enfoque UTE, 8(1), pp. 244 - 256. https://doi.org/https://doi.org/10.29019/enfoqueute.v8n1.121

ASHTON. Kevin .That 'Internet of Things' Thing - 2009-06-22 - Page 1 - RFID Journal {En Línea}. {11 deMarzo de 2018}. Disponible en: www.rfidjournal.com/articles/view?4986

BALLESTIN PEREZ, Alberto. Internet de las cosas, España. 2015, p5, Trabajo de investigación (Grado en Ingeniería Informática) Universidad Politécnica de Valencia, Facultad Ciencias e Ingeniería.

BARRIGA DOMINGEA. Ana. Nuevos retos para la protección de datos personales. En la Era del...Madrid (2004) P29.

BERNARD. Marr, What is Big Data? A super simple explanation for everyone {En Línea}.2018 {11 de Marzo de 2018}. Disponible en: https://www.bernardmarr.com/default.asp?contentID=766

BROCK. DL El Código Electrónico de Producto (EPC); Centro de autoidentificación, Libro Blanco MIT-AUTOID-WH-002, {En Línea}.2001 {08 de Marzo de 2018}. Disponible en: http://cocoa.ethz.ch/media/documents/2014/06/archive/MIT-AUTOID-WH 002.pdf

BROWN. Jamie, Three principles for getting IoT security policy right - Highlight ... {En Línea}. 2017{21 Mayo de 2018}. Disponible en:https://www.ca.com/...highlight/three-principles-for-getting-iot-se...

BUREAUCORP, Domótica. IoT.(Internet of Things , Internet de las cosas) - {En Línea}. {11 de Marzo de 2018}. Disponible en: www.bureaucorp.net/domotica-iot/

CISCO IBSG,8 Best Practices for Security Within the Internet of Things. {En Línea}.2011 {11 de Marzo de 2018}. Disponible en: https://www.netformation.com/.../8-best-practices-for-security-wit...

CISCO. Internet de las cosas (IoT) - {En Línea}. {11 de Agosto de 2017}. Disponible en: https://www.cisco.com/c/es_co/solutions/internet-of-things/overview.html

CISCO. The Vital Element of the Internet of Things {En Línea}. 2015. {11 de Marzo de 2018}. Disponible en: https://www.cisco.com/c/dam/en_us/.../iot/vital-element.pdf

COSTAS, SANTOS, Jesús. Seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, {En Línea}. {11 de Mayo de 2018}. Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3228430.

CRICKET. Liu, Securing networks in the Internet of Things era - Help Net Security {En Línea}.2014 {04 MARZO de 2018}. Disponible en: https://www.helpnetsecurity.com/.../securing-networks-in-the-inte...

CYNTHIA. Harvey. Top 10 IoT Security Threats – Datamation {En Línea}.2018 {11 de mayo de 2018}. Disponible en: https://www.datamation.com/security/.../top-10-iot-security-threat.

ELKHODR M., SHAHRESTANI S., CHEUNG H. The Internet of Things: Vision & Challenges; Proceedings of the IEEE 2013 Tencon Spring Conference; Sydney,

Australia. 17–19 April 2013; pp. 218–222. {En Línea}. {08 Marzo de 2018}. Disponible en: http://ieeexplore.ieee.org/document/6584443/.

ESCAMILLA-AMBROSIO, P. J., SALINAS-ROSALES, M., Acosta-Bermejo, R., & Rodríguez-Mota, A. Internet de las Cosas: 50 Mil Millones de Puntos Inseguros. {En Línea}. {11 de Mayo de 2018}. Disponible en: Internet de las Cosas: 50 Mil Millones de Puntos Inseguros

ESCRIVÁ, G. G., ROMERO, S. R. M., & RAMADA, D. J. (2013). Seguridad informática. España: Macmillan Iberia, S.A. {En Línea}. {11 de mayo de 2018}. Disponible en:http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820963&p00=seguridad+basica+en+redes+de+datos

ESCRIVÁ, GASCÓ, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. ProQuest Ebook Central.

GARCIA, Luis. Estudio del impacto técnico y económico de la transición de internet al internet de las cosas (IoT). Colombia, 2015, p18, Trabajo de investigación (Magister en Ingeniería de Telecomunicaciones) Universidad Nacional de Colombia, Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial.

GARCÍA. Miriam, Puente, Riesgos y retos de ciberseguridad y privacidad en IoT CERTSI {En Línea}.2017 {11 de Mayo de 2018}. Disponible en: https://www.certsi.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot.

GÓMEZ, VIEITES, Álvaro. Gestión de incidentes de seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3229340.

GOODIN. Dan, Rash of in-the-wild attacks permanently destroys … {En Línea}. {02 de mayo de 2018}. Disponible en: https://arstechnica.com/information-technology/2017/04/rash-of-in...

http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3217398.

JARA, A.J., LADID, L. and SKARMETA, A. (2013) The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4, 97-118.

JAZAYERI M., LIANG S., HUANG C.-Y. Implementation and Evaluation of Four Interoperable Open Standards for the Internet of Things. Sensors. {En Línea}.2015 {09 Marzo de 2018}. Disponible en: http://www.mdpi.com/1424-8220/15/9/24343

KASPERSKY LAB. detectó más 7,000 muestras de malware en dispositivos IoT a principios de año, {En Línea}.2017 {11 de mayo de 2018}. Disponible en: https://latam.kaspersky.com/.../kaspersky-lab-detecto...7000-muestras-de-malware-en....

KASPERSKY LAB. Sobreviviendo en el mundo IoT: Expertos de Kaspersky Lab exponen ...{En Línea}. 2018 {11 de Mayo de 2018}. Disponible en: https://latam.kaspersky.com/.../2015_sobreviviendo-en-el-mundo-iot-expertos-de-kas...

KOPETZ H. Real-Time Systems. Springer; Boston, MA, USA: 2011. Internet of Things; pp. 307–323.

LALIBERTE. Marc analista de amenazas de seguridad de la información en WatchGuard Technologies, helpnetsecurity {En Línea}. {11 de Febrero de 2018}. Disponible en: https://www.helpnetsecurity.com/.../11/iot-botnets-security-regulation

LIBELIUM. Top 50 Internet of Things Applications - Ranking | … {En Línea}. {11 de Marzo de 2018}. Disponible en: www.libelium.com/resources/top_50_iot_sensor_applications_ranking.

LONDOÑO ORTIZ, Roby Nelson. internet de las cosas. Manizales 2016, monografía presentada como requisito parcial para optar el título de tecnólogo en sistemas, universidad de Manizales.

LÓPEZ GARZÓN, Jose. Infraestructura de clave pública (PKI) para una pyme. Guayaquil, 2015. P 84, Magíster en Telecomunicaciones, Universidad Católica de Santiago de Guayaquil.

MAKRUSHIN. Denis Los errores de la medicina "inteligente" - Securelist {En Línea}.2018 {08 Mayo de 2018}. Disponible en: https://securelist.lat/los-errores-de-la-medicina-inteligente/84832/

MATTERN. Friedemann, FLOERKEMEIEr, Christian. “From the Internet of Computers to the Internet of Things”. Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich, Jul 2010.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y. COMUNICACIONES, Internet de las cosas -… {En Línea}. {11 de Octubre de 2017}. Disponible en: www.mintic.gov.co/portal/604

N. Gershenfeld, R. Krikorian, D. Cohen, “The internet of things”, Scientific American, vol. 291, no. 4, pp. 76-81, 2004. {En Línea}.2016. {3 de Marzo de 2018}. Disponible en: www.sciepub.com/reference/146435.

NETCLOUDENGINEERING. Seguridad en la nube para los dispositivos IoT | Ciberseguridad {En Línea}. {11 de mayo de 2018}. Disponible en: https://netcloudengineering.com/seguridad-dispositivos-iot/.

OCDE. sobre la economía digital. Microsoft, México. 2015 - Página 69

OPENMIND .El Internet de Todo - BBVA {En Línea}. 2016. {11 de Marzode 2018}. Disponible en: https://www.bbvaopenmind.com/el-internet-de-todo/

Pinto, A. C., De la Hoz Franco, E., & Pinto, D. C. (2012). Las redes de sensores inalámbricos y el internet de las cosas. Inge Cuc, 8(1), 163-172.

Procesos y herramientas para la seguridad de redes, UNED - Universidad Nacional de Educación a Distancia, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3220062.

REDACCIÓN GESTIÓN. El impacto de Internet de las cosas en la vida cotidiana | Tecnología... {En Línea}. 2014. {11 de Febrero de 2018}. Disponible en: https://gestion.pe/tecnologia/impacto-internet-cosas-vida-cotidiana-58481

REYES, Krafft, Alfredo Alejandro. Las firmas electrónicas y las entidades de certificación, D - Universidad Panamericana, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3178023.

ROA, B. J. F. (2013). Seguridad informática. España: McGraw-Hill España. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10692460&p00=firewall

SARMA S., BROCK DL, ASHTON K. The Networked Physical World; Centro de autoidentificación, Libro Blanco MIT-AUTOID-WH-001, {En Línea}.2001. {1 de Marzo de 2018}. Disponible en: http://cocoa.ethz.ch/downloads/2014/06/None_MIT-AUTOID-WH-001.pdf.

SYMANTEC CORPORATION. Informe sobre las amenazas para la seguridad en Internet ... – Symantec {En Línea}. {11 de Marzo de 2018}. Disponible en: https://www.symantec.com/es/mx/security-center/threat-report

TELEFÓNICA, F. Smart Cities: un primer paso hacia la Internet de las Cosas. Fundación Telefónica. {En Línea}. 2011. {11 de Octubre de 2017}. Disponible en:https://www.socinfo.es/.../1404smartcities6/01-TelefonicaSMART_CITIES-2011.pdf

TIKI-TOKI. Internet of Things Timeline,{En Línea}. {10 Octubre de 2017}. Disponible en: www.tiki-toki.com/timeline/entry/.../Internet-of-Things-Timeline.

TYAGI, S., DARWISH, A. y KHAN, MY (2014), Gestión de la infraestructura informática para datos de IoT. Avances en Internet of Things, 4, 29-35. {En Línea}. {03 Marzo de 2018}. Disponible en: https://doi.org/10.4236/ait.2014.43005.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT) Internet of Things - ITU Internet Reports. ITU;Ginebra, Suiza: 2005. {En Línea}. {11 de Marzo de 2018}. Disponible en: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf.

WAUGH, Rob. Seguridad en Internet de las Cosas: cómo proteger... – WeLiveSecurit. {En Línea}. 2014. {11 de mayo de 2018}. Disponible en: https://www.welivesecurity.com/la-es/2014/11/25/seguridad-internet-de-las-cosas

WEISER M. The Computer for the 21st Century. Sci. A.m. 1991; 265: 94-104. doi: 10.1038 / scientificamerican0991-94.

XATAKAHOME. Consejos de seguridad para redes WiFi, convierte tu red en una fortaleza inexpugnable, {En Línea}.2012 {20 Mayo de 2018}. Disponible en: https://www.xatakahome.com/la-red-local/consejos-de-seguridad-para-redes-wifi-conv...