CONSTRUCCIÓN DE PROCEDIMIENTOS PARA MINIMIZAR LAS VULNERABILIDADES A LAS QUE SE VEN EXPUESTAS LAS ORGANIZACIONES (FRENTE AL IOT.)

DIDIER AHIMELEC CASTRO CASTRO
JORGE ANDRÉS GONZÁLEZ CARMONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

CONSTRUCCIÓN DE PROCEDIMIENTOS PARA MINIMIZAR LAS VULNERABILIDADES A LAS QUE SE VEN EXPUESTAS LAS ORGANIZACIONES (FRENTE AL IOT.)

DIDIER AHIMELEC CASTRO CASTRO
JORGE ANDRÉS GONZÁLEZ CARMONA

Monografía de grado para optar al título de
Especialista en Seguridad Informática

Director del Curso
Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, D.C. 18 de mayo de 2018

Dedico este trabajo a Dios, por permitirme seguir fortaleciendo mis habilidades cognoscitivas, por siempre guiarme y bendecir cada pasó que doy en el trasegar de la vida y permitirme siempre cumplir mis propósitos.

A mi amada esposa Johana Niño Gaitán, por su amor, motivación y apoyo incondicional, en cada una de las metas propuestas.

A mis padres, que con su formación y enseñanzas, inculcaron valores solidos que me permiten ser un hombre de bien para la sociedad, fundamentado en principios y valores.

Didier Ahimelec Castro Castro.

Primeramente, agradezco a Dios por darme la fortaleza y las habilidades necesarias, en todos los momentos difíciles por los que se debe pasar, en el difícil proceso del aprendizaje a distancia, ayudándome a enfrentar los retos que me propongo y lograr las metas trazadas.

Agradezco a mi Esposa Stefania Viteri Salas por sus palabras de aliento, por su gran apoyo y motivación para la culminación de este logro

Le agradezco al Ingeniero Didier Ahimelec Castro Castro, compañero de Posgrado y proyecto, quien acepto junto conmigo el reto de hacer esta monografía

Jorge Andrés González Carmona

AGRADECIMIENTOS

Didier Ahimelec y Jorge Andrés expresan sus agradecimientos a:

Esp. Ing. Freddy Enrique Acosta por su orientación y compartir sus conocimientos en pro de elevar las capacidades y aptitudes para el ejercicio de la profesión, así mismo por el acompañamiento realizado el cual permitió la culminación del proyecto.

A docentes involucrados en el proceso de enseñanza en la Especialización en Seguridad Informática impartida por la Universidad Nacional Abierta y a Distancia UNAD, ya que sin ellos no habría sido posible alcanzar esta meta.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ILUSTRACIONES

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ARDUINO[1]: entorno que proporciona prototipos electrónicos bajo ambiente de software libre (open-source), dispone de recursos basados en hardware y software con características de flexibilidad y de fácil utilización. Su estructura permite que sea utilizada por artistas, diseñadores, ser tomada como un medio de hobby por quienes estén motivados a crear objetos o entornos interactivos.

Esta solución tiene la capacidad de percibir el entorno, a través de la recepción de entradas desde una variedad de sensores y puede generar la afectación del mismo, en aspectos como el de controlar luces, motores y diversos artefactos. La placa cuenta con un microcontrolador el cual se programa mediante el software *Arduino Programming Language* (basado en Wiring) y el *Arduino Development Environment* (basado en Processing). Las soluciones de Arduino pueden tomar condiciones autónomas o llevar a cabo comunicaciones con software en ejecución en un ordenador (por ejemplo, con *Flash, Processing, MaxMSP*, etc.).

Estos elementos pueden ser ensamblados a mano o requeridos preensamblados, así mismo el software requerido puede ser descargado de forma gratuita. Por otra parte, en cuanto a los diseños de cada referencia de hardware estarán disponibles bajo los parámetros de la licencia open-source, permitiendo la autonomía de ajustarlo a las necesidades.

BIG DATA[2]: este concepto encierra aspectos relacionados con grandes cantidades de volúmenes de datos, que exceden la capacidad de las herramientas de software convencional para su procesamiento, captura y administración en tiempo razonable.

El crecimiento de los datos se presenta de forma acelerada, por lo cual se está pasando de hablar de petabytes y zettabytes a incorporar el concepto de yottabyte que es el nivel más grande de data que un sistema informático puede tener.

Esta nueva era donde los datos serán el factor predominante para los distintos entornos empresariales y productivos, pero también tendrán una connotación frente a su confidencialidad y tratamiento.

CIBERDELINCUENTE[3]**:** se refiere a todas las actividades cometidas mediante la utilización de un sistema informático a través del cual se busca realizar una actividad ilícita que afecta tanto a infraestructura tecnológica, informática y de información.

[1] MCI electronics. ¿qué es arduino?. [En línea]. [Consultado 17 de octubre de 2017]. Disponible en internet: http://arduino.cl/que-es-arduino/
[2] Fundación Wikimedia, Inc. Big Data. [En línea]. 2017 [Consultado 22 de noviembre de 2017]. Disponible en internet:https://es.wikipedia.org/wiki/Big_data#Definici.C3.B3n
[3] INTERPOL. Delincuencia informática. [En linea]. [Consultado el 17 de Octubre de 2017]. Disponible en internet: https://www.interpol.int/es/Crime-areas/Cybercrime/Cybercrime

COSA[4]**:** en cuanto a la Internet de las Cosas, este es un objeto del mundo físico (cosas físicas) o el mundo de la información (cosas virtuales), que es capaz de ser identificado e integrado al interior de las redes de comunicaciones, enmarcar todos los elementos utilizados de forma cotidiana, pero que ahora mediante la utilización de herramientas de software y hardware, pasan a la galería de los Smart Things, su función principal facilitar al usuario la vida, y permitir un control del ambiente donde desarrolla.

DISPOSITIVO[5]: Con respecto a la Internet de las cosas, este es una parte de los equipos con las capacidades obligatorias de comunicación y las capacidades opcionales de detección, actuación, captura de datos, almacenamiento y procesamiento de datos, la mayoría de la literatura considera que la IOT implica la intercomunicación entre una base virtual y un objeto físico con estas características o también llamada cosa.

DOMÓTICA[6]: hace referencia al conjunto de herramientas tecnológicas que ejercen, control, dominio y supervisión de los elementos que se integran a una edificación compuesta por oficinas o sencillamente una vivienda. La estructura de esta tecnología cuenta con una adaptación para proveer un uso eficiente de la energía, así como aportar seguridad y comodidad. Ello permite una comunicación de doble vía ente el beneficiario y el sistema.

INTERNET DE LAS COSAS (IOT)[7]: Tiene una infraestructura global para la información en unos servicios avanzados que mediante la interconexión entre (servicios físicos y virtuales) basadas en la interoperabilidad existente y en evolución entre las tecnologías de la información y la comunicación.

M2M[8]: Este mecanismo de comunicación permite entablar conexión entre dos dispositivos de forma remota y poder intercambiar información llevando a cabo procesos de verificación, control e inspección de los procesos que realizan estos elementos.

NFC[9]: Este tipo de tecnología inalámbrica incorporada en dispositivos móviles tiene su fundamento en permitir una comunicación instantánea entre estos elementos de una forma rápida y de doble vía.

---

[4] TechTarget. Internet de las cosas (IoT). [En línea]. 2017. [Consultado el 17 de octubre de 2017]. Disponible en internet: http://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT

[5] DEL VALLE HERNÁNDEZ, Luis. Arduino y los dispositivos del IoT. [En línea]. [Consultado el 02 de noviembre de 2017]. Disponible en internet: https://programarfacil.com/podcast/61-arduino-y-los-dispositivos-del-iot/

[6] Venemedia. ¿Qué es domótica?. [En línea]. [Consultado el 18 de Octubre de 2017]. Disponible en internet: http://conceptodefinicion.de/domotica/

[7] Fundación Wikimedia, Inc. Internet de las cosas. [En línea]. [Consultado el 02 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/Internet_de_las_cosas

[8] Fundación Wikimedia, Inc. M2M. [En línea]. [Consultado el 03 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/M2M

[9] Fundación Wikimedia, Inc. Near field communication. [En línea]. [Consultado el 03 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/Near_field_communication

OBJETOS INTELIGENTES[10]: En este tipo incluimos objetos virtuales, un tema que se verifica como cualquier cosa que se pueda comunicar dentro del ámbito de la información y el uso de tecnologías de comunicación que se puedan proporcionar en cualquier momento y lugar.

PROTOCOLO IPV6[11]: Dado el incremento de los dispositivos que se conectan a internet, surge IPV6 como una solución a la limitante de direccionamiento IP la cual limitaría el acceso a la red mundial, de igual forma permitirá transmitir grandes volúmenes de datos.

RASPBERRY PI[12]: placa base conformada por un chip Broadcom BCM2835 con procesador ARM hasta a 1 GHz de velocidad, GPU Video Core IV y hasta 512 Mbytes de memoria RAM, las características varean según el modelo, pero básicamente se trata de un minicomputador del tamaño de una caja de cigarrillos, su costo es muy bajo oscilando entre los 30 – 60 dólares.

RFID[13]: Este tipo de tecnología permite establecer comunicación entre un dispositivo por conexión remota mediante la utilización de ondas de radio y así transmitir la identificación de un elemento.

SEGURIDAD DE LA INFORMACIÓN[14]: Hace mención a todos aquellos mecanismos, protocolos, procedimientos y normas adoptadas, con el fin de garantizar que el recurso más valioso que es la información, no sea expuesto a vulneraciones y afecten el normal desarrollo de los procesos

SENSOR[15]**:** para este ámbito, son los elementos que llevan a cabo las tareas críticas dentro de los procesos de captura de datos, monitoreo y medición, tienen la facultad de detectar y responder a señales eléctricas u ópticas. Este tipo de mediciones se basarán en factores como temperatura, humedad, presión, intensidad lumínica, distancia etc.

---

[10] TENENGA. Ciudad inteligente y objeto inteligente: ¿qué es el IoT y cuál es su importancia para los negocios?. [En línea]. [Consultado el 02 de noviembre de2017]. Disponible en internet: http://www.tenenga.it/es/ciudad-inteligente-y-objeto-inteligente-que-es-el-iot-y-cual-es-importancia-para-los-negocios/

[11] Fundación Wikimedia, Inc. IPv6. [En línea]. [Consultado el 03 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/IPv6

[12] CASTRO, Alberto. ¿Qué es Raspberry Pi, dónde comprarla y cómo usarla?. [En línea]. 2014. [Consultado el 18 de octubre de 2017]. Disponible en internet: http://computerhoy.com/noticias/hardware/que-es-raspberry-pi-donde-comprarla-como-usarla-8614

[13] Fundación Wikimedia, Inc. RFDI. [En línea]. [Consultado el 03 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/RFID

[14] Fundación Wikimedia, Inc. Seguridad de la información. [En línea]. [Consultado el 19 de octubre de 2017]. Disponible en internet. https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

[15] Fundación Wikimedia, Inc Sensor. [En línea]. 2017. [Consultado el 28 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/Sensor

SERVIDOR[16]: mediante este hardware se centralizan los procesos que realizan los dispositivos y se encarga de recibir y enviar la información que estos capturan, así mismo permite llevar a cabo la gestión y administración de una forma eficiente de cada elemento.

[16] Domodesk. A fondo: ¿qué es iot (el internet de las cosas)?.[En línea]. [Consultado el 18 de octubre de 2017]. Disponible en internet: http://www.domodesk.com/221-a-fondo-que-es-iot-el-internet-de-las-cosas.html

RESUMEN

La necesidad de controlar los dispositivos "cosas" que hacen parte de nuestro día a día, ha generado una gran interconexión de aparatos tecnológicos, todo esto generando una transformación en el desarrollo de actividades y la forma en que se prestan los servicios, cambiando considerablemente la manera de ver las "cosas", pasando de ser simples objetos que se utilizan para prestar un servicio independiente, a ser aparatos que hacen parte de un conglomerado logístico que nos brinda soluciones prontas y valederas, este factor donde las “cosas” están vinculadas a la red mundial, abrió la puerta a lo que hoy se define como el Internet de las Cosas “IoT” un entorno donde las cosas se conectan e interactúan entre sí para desarrollar alguna actividad o función.

Esta transformación tecnológica involucra diversas esferas industriales, impulsado por la adaptación masiva de cosas de uso cotidiano generando herramientas que agilizan diversos procesos, esta transformación de interconexión tecnológica ha llevado a un uso indiscriminado de aparatos sin prestar mayor importancia a la seguridad informática, poniendo en riesgo a los usuarios y sus datos.

Dando respuesta a la gran problemática antes expuesta, se presenta a lo largo de esta Monografía en forma amplia y concreta que es IoT, sus vulnerabilidades y la forma de dar solución a las mismas, con esto dando a conocer los riesgos a que se exponen los usuarios y se plantean mecanismos para preservar la integridad, confidencialidad y disponibilidad de todos los recursos tecnológicos, informáticos y de información.

Palabras claves: Accesibilidad, IoT, procesos industriales, riesgo Informático, transformación, usuario, vulnerabilidades

ABSTRACT

The need to control the devices "things" that are part of our day to day, has generated a great interconnection of technological devices, all this generates a transformation in the development of activities and the way in which services are provided, changing the way of seeing "things", going through simple objects that are used to provide an independent service, devices that are part of a logistics conglomerate that provides us with prompt and valid solutions, this factor where "things" are linked to the global network , opened the door to what today is defined as the Internet of Things "IoT", an environment where things are connected and interact with each other to achieve their activity or function.

This technological transformation involves various industrial spheres, driven by the massive adaptation of everyday things that generates tools that streamline various processes, this transformation of technological interconnection has led to an indiscriminate use of devices without paying attention to the importance of information technology, putting at risk to users and their data.

In response to the aforementioned big problem, this monograph is presented in a broad and concrete way that is IoT, its vulnerabilities and the way to solve them, with this, giving information about the risks to which they are exposed. users and mechanisms are proposed to preserve the integrity, confidentiality and availability of all technological, information and information resources.

Keywords: Accessibility, IoT, industrial processes, computer risk, transformation, user, vulnerabilities

INTRODUCCIÓN

El auge de la tecnología, entendiendo ella como las herramientas que hacen más fácil el desarrollo de las actividades cotidianas, viene siendo revolucionada por un nuevo concepto de Internet donde este no solo permite su interacción con personas, sino que trascendió a aplicarse sobre objetos, es ahí donde figura el concepto de la Internet de las cosas. Este nuevo patrón tecnológico, permite que los dispositivos que se encuentran en el entorno cercano se interconecten a la red, sirviendo como medio para ampliar y mejorar la interconexión global, es decir, que aquellos elementos que tenían un comportamiento automático previamente programada pasen a ser medios inteligentes, que transmitan y reciban información a través de internet basado en el actuar de las personas[17].

Este actuar de las personas está basado en espacios tan sencillos como hacer las compras semanales por internet, esto podría cambiar con una nevera inteligente, con acceso a internet, que tuviese como misión a través de sensores identificar las fechas de vencimiento de los productos, o cuáles serían los elementos de acceso más común para llegar hasta armar un presupuesto familiar que lleve a interactuar con una de las grandes superficies para hacer pedidos en línea y hacerlo llegara hasta la puerta de la casa[18].

Este sencillo ejemplo muestra como la internet de las cosas puede abarcar desde cuestiones sencillas hasta complejas como el monitoreo de la casa, encender luces, controlar accesos y salidas de la casa, entre otros, así mismo al interior de las organizaciones lograr un uso adecuado de las tecnologías. Tal vez uno de los aspectos más preocupantes para aquellos sujetos que utilizan este tipo de tecnologías tiene que ver con el tema de la privacidad y la seguridad que puedan llegar a proveer los artefactos que se encuentran conectados a la red de internet y que interactúan tanto con un ser humano como entre ellos[19].

La búsqueda del desarrollo de las IoT se ha hecho por medio de aplicaciones que son utilizadas socialmente para ser desarrolladas de una manera sencilla, que sean de fácil acceso, económicas y que con ellas se puedan hacer múltiples tareas en un mínimo de tiempo y de fácil acceso.[20]

---

[17] DOMODESK. A fondo: ¿qué es iot (el internet de las cosas)?.[En línea]. [Consultado el 05 de noviembre de 2017]. Disponible en internet: http://www.domodesk.com/221-a-fondo-que-es-iot-el-internet-de-las-cosas.html

[18] HIDALGO MARTÍN, Elena. The Internet Of Things. [En línea]. 2016. [Consultado el 05 de noviembre]. Disponible en internet: https://himarele.wordpress.com/2016/09/14/the-internet-of-things/

[19] LOVELOCK, Julián. hacia un internet de las cosas confiable (IOT). [En línea]. [Consultado el 05 de noviembre de 2017]. Disponible en internet: http://www.seguridadenamerica.com.mx/noticias/de-consulta/articulos-destacados-de-seguridad/27704-hacia-un-internet-de-las-cosas-confiable-iot

[20] MARTÍNEZ, Isaura. Internet de las Cosas (IoT): Ventajas para las empresas. [En línea]. 2017. [Consultado el 07 de noviembre de 2017]. Disponible en internet: https://www.commercient.com/internet-de-las-cosas-iot-ventajas-para-las-empresas/

Toda esta perspectiva y evolución tecnológica, apuntara a construir ciudades inteligentes en un futuro, allí convergerán factores como el transporte, la energía y las tecnologías de información y las comunicaciones, que serán el vehículo transformador para lograr un crecimiento competitivo y sostenible, que se reflejara en la calidad de vida de la ciudadanía y en los estamentos gubernamentales que promoverán la participación ciudadana al optimizar sus servicios.

Con gran jubilo se puede decir que IoT ya es una realidad, el internet de las cosas es parte de la vida cotidiana de las personas y de las organizaciones, su aplicabilidad en diversos entornos de la sociedad, ha beneficiado a gran parte de la población disponiendo de recursos más eficientes y accesibles, que se reflejan en la reducción de costos y aumento de productividad.

Pero lamentablemente todo no es alegría, puesto que hay una gran preocupación por parte de toda la comunidad tecnológica, frente a las problemáticas de seguridad que presenta esta tecnología. Son precisamente todas esas cuestiones las que serán abordadas a lo largo del documento, con el fin de lograr reflexiones y contextos de aporte a la seguridad informática, la arquitectura de software, la utilización por parte del usuario final, los códigos y la privacidad de los individuos en un ambiente controlado.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

En 1968 durante la conferencia de la OTAN (Mcllroy, 1968) introdujo por primera vez el concepto de componente de software. Este paradigma de programación promueve la reutilización de componentes y de software fabricado mediante el ensamblaje de componentes tecnológicos de diversa índole.[21]

Pero hoy en día, el campo de los componentes de software no va a cumplir sus promesas en cuanto a la reutilización y portabilidad de los componentes. De hecho, a menudo es necesario para crear un código de programación, para permitir el montaje de componentes existentes, crear nuevos elementos de trabajo por medio de la arquitectura de software. Por lo tanto, a menudo es más barato trasladar un componente en lugar de desarrollar la reutilización de los componentes existentes. Eso sin revisar que además de que la construcción de los componentes por parte de otras máquinas inteligentes a veces falla en cuanto a la estandarización, ya que no todos los modelos de este tipo están en esa misma medida.

Con el aumento progresivo de la cantidad de artefactos presentes en las realidades cotidianas de los individuos, se hace posible un concepto de democratización de la tecnología en el hogar; llamada también domótica[22], esto crea nuevas necesidades en términos de ingeniería de software estando presentes lo virtual y lo físico, para hacer frente a la heterogeneidad que se da en cuestiones de la utilización de la tecnología, la jerarquización del software, su adaptación al entorno durante su ejecución, y muchos otros momentos a tener en cuenta en la configuración de la presente monografía.

> Desde ahí se puede decir qué:
>
> Estos elementos disponen de ciertas características que los enmarca dentro de tres criterios fundamentales, el primero ser compactos y portables, un ejemplo claro los dispositivos de telefonía móvil los cuales pueden operar como cámara fotográfica, reproductor de música, editor de texto entre otras, una segunda característica es la relacionada con su movilidad, es decir puede ser ubicados de acuerdo a su funcionalidad y así mismo poder ejercer control sobre el mismo, y la tercera característica su complejidad, esto dado por las condiciones y características que deben estar inmersas dentro de los dispositivos para su interactuar con recursos a nivel de hardware y software.

[21] RANDELL, Brian. Conferencia de Ingeniería de Software de la OTAN. [En línea]. 1996. [Consultado el 07 de noviembre de 2017]. Disponible en internet: http://homepages.cs.ncl.ac.uk/brian.randell/NATO/NATOReports/
[22] CEDOM. Qué es Domótica. [En línea]. [Consultado el 08 de noviembre de 2017]. Disponible en internet: http://www.cedom.es/sobre-domotica/que-es-domotica

Para cumplir con las expectativas que ha planteado el uso de software en las diferentes aplicaciones móviles, la cotidianidad en los hogares y las empresas ha llevado a buscar características específicas de cada instalación para hacer frente a cuestiones que van desde la incapacidad para el ahorro de energía, así como sistemas de software para la gestión y control de las instalaciones haciéndolo de forma rápida y confiable siendo fácil buscar la personalización por parte del usuario.

La tesis central de este trabajo toma la apuesta por la utilización conjunta de un componente de software de modelo restringido, inspirado por la electrónica, y un entorno de ejecución libre y sin restricciones un open source que permita abordar las cuestiones de interoperabilidad, escalabilidad, adaptabilidad y fiabilidad, abriendo el campo de posibilidades en el área de hábitat de la tecnología y el uso de estos para la ayuda en los domicilios a personas dependientes de estos artefactos.

La construcción y configuración de software se basa en paradigmas de programación orientada a servicios y, enriquecido por una aproximación a la utilización de un modelo que cumpla con los tiempos de ejecución, desarrollo de un modelo de software. Basándose en gran medida en la electrónica, reutilizando y proporcionando una fácil integración de productos y servicios de automatización del hogar disponibles a través de Internet.[23]

La Internet de las cosas se refiere a un enfoque en el que los objetos cotidianos alcanzan un grado de construcción de software para que puedan interactuar entre sí y hacer que los servicios que prestan tengan unos valores añadidos como los que se han trabajado anteriormente así como a lo largo del texto. Aunque todavía con muchos principios por desarrollar, este enfoque sigue buscando herramientas de desarrollo de software para describir las interacciones y los servicios prestados por medio de los componentes y la arquitectura del software.[24]

Dentro del proceso que da cuenta para el cliente final hay una preocupación constante por la forma de protección y seguridad para los artefactos y la información y funcionalidad que hay en ellos. Los sistemas de automatización del hogar desplegados asegurarán niveles de fiabilidad, disponibilidad, seguridad (seguridad de bienes y personas) y la seguridad (servicios de control de acceso en función del tipo de tecnología) de altura. En particular, un equipo debe funcionar con un nivel

[23] Justindeveloper. Desarrollo de Aplicaciones Móviles, Servicios Web, Arquitectura SOA. [En línea]. 2008. [Consultado el 10 de noviembre de 2017]. Disponible en internet: https://justindeveloper.wordpress.com/2008/12/15/arquitectura-de-software-%E2%80%93-overview/

[24] ÉCIJA, Álvaro. una aproximación a algunos elementos de internet de las cosas. [En línea]. 2015. [Consultado el 12 de noviembre de 2017]. Disponible en internet: https://www.ecixgroup.com/una-aproximacion-algunos-elementos-de-internet-de-las-cosas/

adecuado de servicio, a pesar de la presencia de fallos de dispositivos de hardware, o la pérdida de una conexión de red.[25]

1.2 FORMULACIÓN DEL PROBLEMA

El avance tecnológico a lo largo del tiempo, ha repercutido considerablemente dentro de la sociedad, estas herramientas se convirtieron en parte esencial para el desarrollo de procesos productivos, siendo adoptadas e implementadas dentro de las organizaciones y consumidas por los usuarios. Estos procesos llevados a cabo al interior de las organizaciones mediante el uso de herramientas y/o dispositivos en su gran mayoría utilizan una conexión a la internet, es en este apartado donde estos elementos pueden ser catalogados de acuerdo a sus funciones. Se puede establecer la organización de estos elementos basados en la captura de información del entorno en el cual se encuentran y que los transmiten de forma constante por medio de los protocolos de transmisión de datos en aquellas funciones en las cuales se realizan funciones a partir de instrucciones recibidas por vía internet.

Se puede encontrar dentro de las estadísticas globales que las conexiones a la red de internet va en aumento y apunta a que para el año 2020 haya alrededor de 24 mil millones de dispositivos en línea, esta cantidad de artefactos plantean una serie de retos y desafíos con respecto a la seguridad informática. Este crecimiento tiene varios beneficios, ya que cambiará la forma en que la gente realiza las tareas cotidianas y potencialmente transforma el mundo, ya que los nuevos desarrollos permitirían por ejemplo a los automóviles conectarse con la infraestructura inteligente de la ciudad para crear un ecosistema completamente diferente para el conductor, que simplemente está acostumbrado a la forma tradicional de llegar del punto A al punto B, tener dispositivos de asistencia sanitaria conectados dan a la gente una mirada más profunda y completa de su propia salud, o la falta de ella, pero esa entramada de relaciones cibernéticas tiene su riego[26].

Con todos estos beneficios viene el riesgo, este riesgo se mide distintas maneras, por ejemplo el aumento en los dispositivos conectados da a los piratas informáticos y los criminales cibernéticos más puntos de entrada a la red, especialmente en las redes domésticas que son las más vulnerables.

La gran problemática, surge cuando el mundo se conecta, y con él todas las cosas de cotidiano que lo rodean, sin más hoy día podemos ver la gran industria china produciendo por millares productos que comparten la misma llave de entrada, por así decirlo las cosas que nos rodean cada día son más inteligentes, pero nuestra

[25] SORIA PASTOR, Javier. Seguridad en Internet de las Cosas. [En línea]. 2016. [Consultado el 13 de noviembre de 2017]. Disponible en internet: https://aunclicdelastic.blogthinkbig.com/la-seguridad-como-preocupacion-universal/

[26] GARRIDO, Felipe. El 2020 habrá 4 mil millones de conexiones a internet. [En línea]. 2016. [Consultado el 18 de noviembre de 2017] Disponible en internet: https://www.fayerwayer.com/2016/06/el-2020-habra-4-mil-millones-de-conexiones-a-internet/

inteligencia no ha podido comprender el problema que suscita, el hecho de que todos nuestros datos estén en constante movimiento, analizados y disponibles para alguien con conocimientos mínimos los pueda obtener.[27]

A partir de ello, es evidente la preocupación frente a la privacidad y seguridad de los datos que viajan mediante la red, y sobre lo que se generan interrogantes como:

¿Que se pude mejorar de la seguridad de la información en las nuevas tecnologías de internet de las cosas?.

¿Cuál es el nivel de exposición a nivel de riesgos de seguridad a la cual están expuestos los usuarios en la internet de las cosas?.

1.3 JUSTIFICACIÓN

La internet de las cosas es una creación relativamente nueva para una sociedad de consumo basada en la interacción de objetos por dinero, pero esta relación se posiciona más allá en las IoT, en una sociedad donde la interacción entre cosas y personas va más allá de la información para pasar a ser parte de los modelos de confiabilidad social.[28]

Ante esta situación se debe comprender que las IoT se desarrollan en el contexto de un mundo globalizado que interactúa constantemente, en donde los sistemas de información y los objetos por medio de los cuales esto se hace posible llevan a acortar tiempos, distancias, recorridos, pero esta cuestión entraña un problema mayor, la confianza que se pueda generar, la seguridad que se debe tener al procesar datos, acumular contenidos.[29]

Pero no es solamente desde ahí que se justifica un estudio de estos, sino también desde la perspectiva de los dispositivos que se encuentran en los hogares, en las empresas y grandes organizaciones que permitan pasar de un mundo virtual en el cual las interfaces son parte cotidiana, pero que se debe buscar hacerlas amigables para los usuarios, capaces de lograr que la seguridad, la confianza y la verdad de

[27] LÓPEZ TAZÓN, Javier. El lado oscuro del Internet de las Cosas. [En línea]. 2016. [Consultado el 13 de noviembre de 2017]. Disponible en internet: http://www.elmundo.es/tecnologia/2016/01/28/56aa295922601d3d548b4653.html

[28] GÓMEZ ABAJO, Carlos. La Internet de las Cosas es una oportunidad asequible para el desarrollo. [En línea]. 2016. [Consultado el 12 de noviembre de 2017]. Disponible en internet: https://www.tendencias21.net/La-Internet-de-las-Cosas-es-una-oportunidad-asequible-para-el-desarrollo_a41840.html

[29] RODRÍGUEZ, Karina. Usuarios aún no tienen confianza en la seguridad de los dispositivos IoT. [En línea]. 2017. [Consultado el 14 de noviembre de 2017]. Disponible en internet: http://computerworldmexico.com.mx/usuarios-aun-confianza-en-la-seguridad-los-dispositivos-iot/

las actividades que se desarrollan por medio de ellos sea capaz de lograr una interacción constante en condiciones de fácticas y realizables.[30]

La necesidad de dar a conocer con claridad, que está pasando con nuestro entorno tecnológico, y las problemáticas de seguridad que se suscitan en este, llevan a la construcción de un documento contenedor, que pueda explicar con claridad que es IoT, cuáles son sus vulnerabilidades y dar una guía que ayude a prevenir y orientar

Es raíz de ello, que cobra relevancia esta monografía, la cual en la medida que permita comprender aspectos que van desde la cotidianidad de los individuos hasta las empresas que hacen uso de la tecnología con la confianza que se deposita sobre los sistemas tecnológicos, se podrán determinar los problemas y situaciones ya trabajados anteriormente y que están por desarrollar, estableciendo un método para prevenir los riesgos que trae un sistema tan complejo pero que debe tener ciertos niveles de control y procesamiento de los datos.

1.4 OBJETIVOS

1.4.1 Objetivo General.

- Identificar los elementos que componen la seguridad informática en las IoT, teniendo en cuenta lograr soluciones prácticas de trabajo frente a las vulnerabilidades a las cuales se ven expuestos los usuarios de los servicios en la internet y los artefactos que sirven como herramientas de manifestación.

1.4.2 Objetivos Específicos

- Identificar los elementos que componen el internet de las cosas y establecer las vulnerabilidades que se presentan en los recursos tecnológicos relacionados.

- Determinar cuáles son los riesgos a los cuales están expuestas las organizaciones frente al auge del internet de las cosas (IOT) y los mecanismos que pueden ser adoptados para minimizar las vulnerabilidades.

- Establecer controles para el buen uso de las herramientas que están dentro del IOT.

- Crear un manual de procedimientos para la utilización en forma más segura de IOT las cosas de Internet, que les permita a los usuarios interactuar con estas tecnologías reduciendo sustancialmente los problemas de vulnerabilidad.

[30] RIVERA, Nicolás. Qué es el Internet of Things y cómo cambiará nuestra vida en el futuro. [En línea]. 2015. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://hipertextual.com/2015/06/internet-of-things.

1.5 ALCANCE Y DELIMITACIONES

1.5.1 Alcance

La presente monografía, tiene un alcance descriptivo para el lector, ya que mediante el texto se permite identificar las afectaciones de seguridad, vulnerabilidades y riesgos, a que se exponen los dispositivos enmarcados dentro del IoT, y un alcance explicativo que llevara a la prevención, ya que cumple con establecer controles que permitan minimizar las acciones delictivas, mediante la adopción de mecanismos y buenas prácticas de uso.

El lector final entenderá cuales son los componentes Hardware y Software de IoT, ayudando a esclarecer la problemática que presenta la tecnología y sus vulnerabilidades, permitiendo con esto analizar los problemas correlacionales entre usuario y tecnología

Por tanto, este proyecto será una carta de navegación descriptiva, la cual contendrá los mecanismos y procedimientos de seguridad que deben tener en cuenta los encargados de los departamentos del área de tecnología, con el fin de minimizar la vulnerabilidad de la información contenida y manejada por estos dispositivos.

1.5.2 Limitaciones

El constante crecimiento de la industria productora de componentes, lleva a una limitación práctica frente a la adopción de soluciones viables frente a los ataques realizados a dispositivos instalados sin tomar medidas de seguridad pertinentes.

- No hace parte del desarrollo de la monografía, procesos paso a paso, sobre la ejecución de herramientas de seguridad informática convirtiéndose en una limitación práctica, como tampoco la adopción de los procedimientos propuestos, dado que es responsabilidad del profesional encargado de la seguridad informática de la organización, tener el conocimiento para ejecutarlos.

- Tampoco hace parte del proyecto la creación de dispositivos, ni entornos de pruebas para determinar las deficiencias de seguridad del IoT.

- Por consiguiente, el desarrollo del presente proyecto es de tipo documental y define únicamente los elementos teóricos acerca de la seguridad que se debe impartir sobre los dispositivos IoT aplicados a nivel organizacional.

2. MARCO REFERENCIAL

2.1 MARCO TEÓRICO

2.1.1 ¿Qué es el internet de las cosas y cuando nace?

Antes de abarcar con la historia del internet de las cosas, es necesario hacer mención del inicio del internet, puesto que es la razón principal que permite que en la actualidad se disponga de conectividad y acceso para diversos dispositivos de uso cotidiano.

Determinar un punto exacto dentro de la historia en el cual se indique cuando fue creado Internet se puede tornar algo complejo, ya que este fue el resultado de diversas investigaciones llevadas a cabo en diferentes sitios abarcando temas diferentes. Las actividades principales para desarrollar esta tecnología en primera medida tiene relación con la conmutación de paquetes, ante ello se genera las teorías de redes de datos, la arquitectura y su implementación, un segunda etapa se da con la creación de ARPA, entidad quien lleva a cabo el financiamiento e implementación de esta tecnología, bajo este proyecto se centralizan los objetivos con la finalidad de crear comunicaciones directas entre ordenadores para poder comunicar las diferentes bases de investigación.

Consecutivamente y llevando a cabo la integración de estos dos recursos, se da el desarrollo de ARPANET, una conexión interna entre computadores para compartir información y evitar la pérdida de comunicación en caso de cualquier daño. Allí se demuestra que este nuevo sistema de comunicación es operativo logrando establecer una conexión de 40 puntos ubicados en diferentes localizaciones, todo ello permitió que se promulgara y profundizara sobre este campo dando creación a nuevas redes. Este nuevo entorno de conectividad fue un poco caótico a pesar de que ARPANET marcaba los lineamientos para la comunicación y solo fue hasta los años 80 cuando se adopta el protocolo TCP/IP que se da paso a la creación de internet “International Net).

Bajo estas premisas la evolución del internet de pueden catalogar bajo 4 fases:

- Fase 1: Abarca el inicio de las telecomunicaciones, comprendido desde su uso como una red informática militar, dentro de esta fase su aplicabilidad era bastante limitada así como su usabilidad donde era dominada por profesionales de la ingeniería y desarrolladores y sobre la cual se llevaban a cabo actividades de exploración y experimentación.

- Fase 2: Aquí el acceso a la red pasa a ser público, particulares pueden acceder a los servicios de internet a costos elevados y bajo ciertos parámetros de

complejidad. Aun así la mayor parte de interacción era acogida por las empresas que disponían de áreas o departamentos de sistemas, a través de ello estas entidades pasaban a desarrollar operaciones dentro de la red.

- Fase 3: Se pasa a acortar la brecha digital, la accesibilidad se ve aumentada dado la reducción de costes y la simplificación tecnológica, en este punto no solo las empresas tienen la exclusividad de desarrollar actividades sobre la red, si no que los usuarios también tienen los espacios y oportunidades para incursionar en la red. Todo ello da pie para que emergiera la internet social o Web 2.0. Dentro de este entorno notoriamente se evidencio una comunicación más abierta, empleando canales como redes sociales, blogs, etc. en las cuales se realizaban publicaciones y se mantenía una interacción más personal.

  El aumento considerado de usuarios conectados y la aplicabilidad que se le da a la red, permite transformar la mayor parte de procesos incluso la forma tradicional de hacer negocios, la información y el conocimiento trascienden y se incrementan de forma acelerada modificando los mercados.

- Fase 4: El crecimiento acelerado, la simplificación y bajo coste para acceder a los recursos tecnológicos abren un amplio campo de acción, ahora no solo las organizaciones y las personas pueden interactuar con la red para ofrecer servicios, emergen los sistemas inteligentes donde se involucran elementos para recolectar datos, entornos virtuales para almacenarlos y aplicaciones para darles tratamiento convirtiéndolos en información útil para la sociedad. Ante ello se profundiza en lo que se denomina la internet de las cosas (IoT)

El avance tecnológico ha sido un factor trascendental para el desarrollo de múltiples actividades en los entornos de la sociedad, convirtiéndose en un proceso imparable, allí las acciones de innovación que se dan a diario y de forma secuencial hacen que sus reacciones se multipliquen de forma acelerada. Dentro de este entorno se encuentran las Tecnologías de información donde se pueden resaltar diversos momentos, la transmisión de datos, la digitalización de las señales, la telefonía móvil, vías de comunicación como fibra óptica o banda ancha tanto fija como móvil, todo ello ha permitido la transformación del mundo de las comunicaciones.

Todo este accionar tecnológico que se ha dado a través del tiempo, dio cavidad a disponer de una conexión universal como lo es la Internet, la cual no ha sido ajena a la transformación pasando del campo de internet de las personas al de internet de las cosas (IoT).

¿Qué es el Internet de las Cosas?, es la transformación de un primer internet más focalizado en las personas donde su cualidad se fundamenta en la capacidad de armonizar datos con personas, procesos y objetos. Mediante el uso de sensores, redes avanzadas de comunicación y métodos de análisis basados en Big Data dan

permiten la puesta en operación de entornos de aplicaciones que repercutirán en la mejora de la calidad de vida de las personas, serán herramientas que incidirán en optimizar los procesos educativos y de sanidad, potenciaran a las ciudades, se tendrán edificios y redes de electricidad inteligentes y mejorara la eficiencia de las organizaciones a todos los niveles de la sociedad.

Enmarca todo aquello que hace referencia a la interconexión por medios digitales de objetos cotidianos con la red mundial, por consiguiente, tienen las virtudes de proporcionar una amplia oportunidad para las empresas y consumidores abordando diversas áreas de la economía.

Este tema puede considerarse una definición ambiciosa con repercusiones tecnológicas y sociales. Desde la perspectiva de la normalización técnica, IoT puede comprenderse como una infraestructura global de la sociedad de la información, que permite ofrecer servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la Inter operatividad de tecnologías de la información y la comunicación presentes y futuras. Aprovechando las capacidades de identificación, adquisición de datos, procesamiento y comunicación, IoT utiliza plenamente las "objetos" para ofrecer servicios a todos los tipos de aplicaciones, garantizando a su vez el cumplimiento de los requisitos de seguridad y privacidad[31].

Es así que el internet de las cosas se fundamenta en el uso de sensores, redes de comunicación, dispositivos y entornos inteligentes que manejan todo el proceso y el recurso de información que se genera a través de ellos. Allí los sensores juegan un papel fundamental considerándose como los sentidos del sistema, los cuales deben tener características de bajo consumo y de coste para que puedan ser accesible y empleados de forma masiva, por otro lado su tamaño y flexibilidad serán de gran aporte para diversos entornos o requerimientos.

La transformación de la Internet proporciona entornos precisos y potentes mediante sus redes de comunicación inalámbrica M2M, las cuales posibilitan la integración de los objetos a las redes y sistemas externos, por último la incorporación de entornos inteligentes para aprovechar los datos recolectados por los sensores y hacerle los procesos y analítica necesaria para convertirlos en información útil. Ante ello y de acuerdo al volumen de datos recolectados requerirá del uso de técnicas relacionadas con el Big Data vitales para el cumplimiento de los procesos, así mismo en ocasiones será indispensable la inclusión de potentes sistemas de información y de software avanzado para el tratamiento de grandes volúmenes de datos con connotaciones variables y de gran velocidad.

[31] Unión Internacional De Telecomunicaciones. Y.2060 : Visión general de la Internet de las cosas. [En línea]. 2012. [Consultada 18 de noviembre de 2017]. Disponible en internet: https://www.itu.int/rec/T-REC-Y.2060-201206-I/es

El impacto y de lo que es capaz de generar el IoT se puede ver reflejado en las llamadas ciudades inteligentes, dentro de ellas y aplicando los elementos que integran esta revolución tecnológica, posibilitan a las ciudades que proporcionan servicios que estos sean entregados de forma más eficiente y sostenible, viéndose reflejado en una mejor calidad de vida, abriendo nuevas posibilidades de negocios, promulgar el turismo e inversión entre otras.

Allí se abarca diversos entornos sobre los cuales se tiene una afectación de optimización, entre estos se encuentran lo relacionado con el suministro y consumo de agua potable y energía, transporte y movilidad, seguridad, ambientes propicios para los negocios, trasparencia y gobierno, participación ciudadana, turismo, manejo de residuos, energías eficientes para edificación y aparcamientos.

Otros puntos de aplicación del IoT abarca los sectores de la sanidad, en donde se realiza monitorización de pacientes haciendo enlaces con profesionales del área, otro campo es el sector de energía y transporte, allí busca establecer conexión entre clientes y proveedores, en el área de ventas, con el fin de predecir cuándo llevaran a cabo los proceso de compra los consumidores, en las comunicaciones y servicios de información, en el área financiera o fabricas inteligentes. En realidad los campos de acción de esta tecnología tienen gran injerencia sobre aspectos cotidianos, es muy común encontrar su aplicación en procesos de marketing, educación, en los vehículos, juegos, medios de entretenimiento, redes inteligentes en donde se alcanza un máximo de rendimiento y posibilidades. Es así que el IoT emanara un alto nivel de habilidades y conocimientos específicos interrelacionados con áreas como la tecnología, matemáticas y fundamentos organizacionales, ante ello se abrirán nuevos campos de oportunidades laborales dadas las connotaciones que estas requieren para su optima operatividad.

Pero ¿Cuándo nace IoT?, esta nueva revolución tecnológica, fue insinuada por primera vez por el Británico Kevin Ashton en una conferencia en la compañía Procter & Gamble en 1998: “Adicionando identificación por radio frecuencia y otros sensores a objetos cotidianos, crearemos un Internet de las Cosas y se sentaran las bases de una nueva era de percepción de la máquina[32], es decir permitir que las cosas se comuniquen para mejorar la calidad de vida.

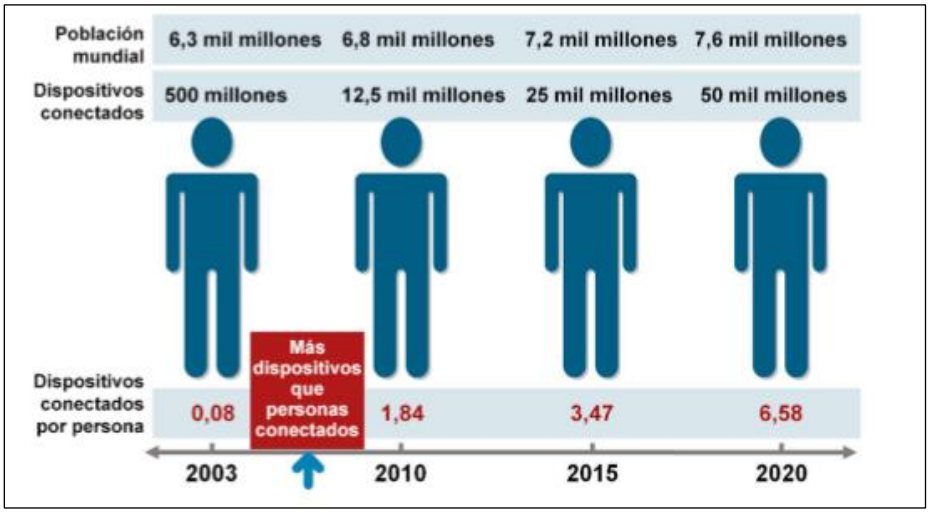
Según Forrester Research de la Oficina de Censos de EE.UU, en el año 2003, había aproximadamente 6,3 mil millones de personas en el planeta, y había 500 millones de dispositivos conectados a Internet[33]. Si dividimos la cantidad de dispositivos conectados por la población mundial, el resultado indica que había menos de un

[32] SANTUCCI, Gérald. Official opening of the conference – Plenary sesión. [En línea]. 2009. [Consultado el 14 de noviembre de 2017]. Disponible en internet:http://cordis.europa.eu/pub/fp7/ict/docs/enet/20090128-speech-iot-conference-lux_en.pdf

[33] EVERS, Joris. Forrester CEO: Web services next IT storm. [En linea]. 2003. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.infoworld.com/article/2681101/operating-systems/forrester-ceo--web-services-next-it-storm.html

dispositivo (0,08) por persona. De acuerdo con la definición de Cisco IBSG, IdC "nació" en algún punto entre 2008 y 2009[34], tal y como se observa en la ilustración 1.

Ilustración 1. Crecimiento y proyección de IoT



Fuente: EVANS, Dave. Internet de las cosas - Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Business Solutions Group (IBSG). [En línea]. 2011. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf. 3 p.

Las oportunidades y desafíos que emergerán frente a estas tecnologías tendrán repercusión en diversos sectores, las actividades humanas afrontaran cambios comportamentales dado el gran número de objetos que estarán interconectados viéndose reflejado en impactos económicos y sociales, así mismo estarán las preocupaciones frente a velar por la seguridad de la privacidad un gran cuello de botella de Iot.

2.1.2 Pilares de IoT

Este concepto de IoT presenta una interrelación inteligente entre datos, cosas, procesos y personas, que unidas soportan el ecosistema sobre el cual se desenvuelve esta tecnología, con lo cual se permite una transformación de los entornos de desarrollo, mejorando y optimizando procesos en función de mejorar y hacer más fácil las actividades cotidianas.

[34] EVANS, Dave. CISCO Internet Bussiness Solutions Group – IBSG. Internet de las Cosas: Como la próxima evolución de Internet lo cambia todo [en línea]. 2011. [Consultado el 14 de noviembre de 2017]. Disponible en internet: http://www.cisco.com/web/LA/soluciones/executive/assets/pdf/internet-of-things-iot-ibsg.pdfdf

- Datos: Hace referencia al resultado obtenido mediante la interconectorización de elementos inteligentes los cuales serán susceptibles a ser analizados y darles un tratamiento de acuerdo a la finalidad establecida. Aquí los datos seguirán siendo la razón y núcleo de todos los procesos que encierran IoT y a medida de que estos evolucionen tomaran mayor importancia dado su utilidad para diversas aplicaciones dentro de la sociedad.

- Cosas: Abarcan los objetos físicos a través de los cuales se realizan los procesos de recolección de datos, estos elementos se integran a través de mecanismos de comunicación y placas ejecutando acciones, cumpliendo funciones según su programación.

- Procesos: Comprende la integración y consolidación de elementos e información, allí se conforma el ecosistema de IoT, su armonización es fundamental para lograr transformar los datos en algo más provechoso y beneficioso a través de los cuales se pueda aportar a la solución o mejora de problemáticas.

- Personas: Se pueden considerar como el punto final de la cadena y sobre quien está la administración de este entorno tecnológico, adicional tienen la función de darle las connotaciones e interpretaciones a los resultados obtenidos y sin su participación lo anterior no tendría sentido.

2.1.3 Tipos de Conexiones dentro de IoT

Desde la perspectiva de la operatividad de los elementos que hacen parte del IoT, es pertinente indicar como llevan a cabo las conexiones para intercambiar, transmitir o procesar datos.

- Conexión máquina a máquina (M2M): A través de esta conexión se permite la comunicación de un equipo con otro a través de un entorno inalámbrico, lo cual facilita el desarrollo de las actividades dentro de las organizaciones en diversos sectores. Las bondades que proporcionan este tipo de conexiones, garantizan que diversos dispositivos puedan estar conectados de forma remota mediante alguna aplicación, intercambiando información o entablando alguna comunicación de doble vía sin requerir intervención manual.

- Conexión maquina a persona (M2P): Este tipo de conexión permite a las personas enviar información hacia los sistemas y así mismo recibir información, con ello se puede establecer que este intercambio es de tipo transaccional, ya que el flujo de datos se transmite en ambas direcciones, permitiendo así el movimiento y administración de los datos en función de que las personas puedan tomar decisiones fundamentadas.

- Conexiones persona a persona (P2P): Se fundamenta en la intervención de personas con la finalidad de contribuir al entorno de desarrollo, allí la información se transfiere de persona a persona empleando los recursos del ecosistema de la solución IoT, por consiguiente se torna como la arquitectura que genera una conexión bidireccional de datos y comandos en relación con el dispositivo.

2.1.4 Modelos de comunicación de IoT

De acuerdo a lo expuesto por el Comité de Arquitectura de Internet (IAB)[35] se da a conocer cuatro modelos de comunicación que se utilizan para los dispositivos enmarcados dentro de IoT.

- Comunicaciones dispositivo a dispositivo: Dentro de este modelo se abarca la comunicación entre dos o más dispositivos conectados entre sí, sin disponer de servidores de aplicación o intermediaros para llevar a cabo sus operaciones mediante el uso de redes IP o de internet. Para lograr una conexión directa se emplean protocolos como Bluetooth, Z-Wave o ZigBee.

- Comunicaciones dispositivo a la nube: A través de este modelo, el dispositivo IoT se conecta de forma directa al entorno virtual con la finalidad de intercambiar datos y controlar el tráfico de mensajes. Aquí se aprovecha los entornos de comunicación existentes como el Wifi o medios cableados, para entablar una conexión entre el dispositivo y la red IP que posteriormente se enlace con la nube. Con este tipo de comunicación, el usuario podrá acceder al recurso de forma remota empleando algún recurso tecnológico.

- Modelo dispositivo a puerta de enlace: Frente a la forma en que se establece comunicación dentro de este modelo, el dispositivo IoT lleva a cabo su conexión mediante la utilización de un servicio ALG para lograr interactuar con el entorno virtual, es decir el dispositivo dispone de un software de aplicación, el cual actúa como puerta de enlace local que actúa como intermediario entre el dispositivo y la nube, adicional a ello proporciona herramientas de seguridad y transcripción de protocolos o datos.

- Modelo de intercambio de datos a través del back-end: Se constituye como la arquitectura de comunicación la cual permite a los usuarios la administración sobre los insumos recolectados a través de los objetos inteligentes, llevando a cabo procesos tanto con los datos que reposa en el entorno virtual como a través de fuentes externas.

[35] TSCHOFENIG, Hannes; ARKKO, Jari; THALER, Dave y MCPHERSON, Danny. Internet Architecture Board (IAB). [En linea]. 2015. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://tools.ietf.org/html/rfc7452

2.1.5 Evolución de las redes para IoT

Las redes de comunicación han venido evolucionando a lo largo del tiempo, proporcionando nuevas alternativas y beneficios para los diversos sectores de la sociedad, esto ha conllevado a que se optimicen los entornos productivos, abriendo nuevas formas de interacción no solo con personas si no pasando a un ámbito de transmisión con sistemas inteligentes. Partiendo de ello, es necesario repasar un poco la historia y analizar las características que estas poseían.

- La Red 1G: Esta red de connotaciones analógicas emergió sobre los años setenta y tenía funciones exclusivas que solo permitían el tráfico de voz, su limitada cobertura la hacía intermitente presentando una baja calidad de sonido, así mismo incorporaba la utilización de múltiples celdas para transferir las llamadas a usuarios que estaban en movimiento.

- Red 2G: Emerge con procesos digitales, se incorporan mecanismos que permiten la transmisión de voz y datos, con ello se proporcionaron mecanismos más eficientes al usuario incorporando la mensajería de texto.

- Red 3G: Se integra un factor muy importante, la velocidad de transmisión, adicional a ello incorpora mecanismos de seguridad a través de la autenticación sobre la red. Tenía como objetivo facilitar la transferencia de archivos multimedia, la conectividad permanente inalámbrica a estándares altos de velocidad.

- Red 4G: Su característica primordial frente a sus predecesoras, es la rapidez para acceder a internet, se basa prácticamente en el uso del protocolo IP, por tanto es una solución integral dada su adaptación entre las redes cableadas e inalámbricas que permiten incrementar considerablemente la transferencia de información sobre un mismo canal.

- Red 5G: Su incorporación dará pie a que emerja el ecosistema IoT, bajo su entorno permitirá la conexión de miles de millones de dispositivos inteligentes bajo un esquema de velocidad, latencia y costo, adaptándose a cualquier entorno y a las necesidades específicas de los usuarios.

2.1.6 Seguridad de los dispositivos IoT

De acuerdo a expuesto por la empresa Symantec, la mayoría de los dispositivos IoT están "cerrados". Los clientes no pueden incorporar software de seguridad una vez que los dispositivos se envían desde la fábrica. A menudo, dicha manipulación anula la garantía. Por consiguiente, la seguridad estará integrada en los dispositivos IoT a partir de su "diseño". En otras palabras, para IoT, la seguridad debe evolucionar desde la seguridad simplemente "atornillada" sistemas existentes como servidores

y computadoras personales (PC) portátiles y de escritorio, a estar "incorporada" al sistema antes de que este salga de la fábrica. Para la mayoría de la industria, la seguridad "intrínseca", incorporada en la fábrica, es una nueva forma de ofrecer seguridad, incluida la clásica tecnologías de seguridad como cifrado, autenticación, verificación de integridad, prevención de intrusiones y seguridad capacidades de actualización.

Dado el estrecho acoplamiento de hardware y software en el modelo IoT, a veces más fácil para el software de seguridad IoT para aprovechar las características avanzadas de hardware de seguridad a menudo pasado por alto por vendedores de seguridad tradicionales que simplemente deben construir capas de seguridad "extrínsecas" para ejecutar en "menos común denominador "hardware".

Afortunadamente, muchos fabricantes de chips ya crean características de seguridad en el hardware. Desafortunadamente, la capa de hardware es solo la primera capa requerida en seguridad integral, requerida para seguridad respaldada por hardware para proteger las comunicaciones y proteger el dispositivo. Exhaustivo la seguridad requiere una integración limpia de la gestión de claves, seguridad basada en host, infraestructura OTA y análisis de seguridad mencionados anteriormente. No abordar ninguno de los pilares de la seguridad deja su destino a los caprichos de los agresores.[36]

Por otra parte, el CSIRT-CV expone que al materializarse las amenazas a las que están expuestos los dispositivos del IoT, puede afectar a la accesibilidad sobre el recurso, la integridad de la información que contiene y la identidad del usuario que la posee, ya que puede provocar una suplantación de identidad. Así mismo, la disponibilidad quizá sea uno de los aspectos que más problemas puede generar, principalmente si hablamos por ejemplo de entornos industriales, donde una interrupción del servicio debido a un ataque de denegación de servicio (DoS) entre otros, puede provocar grandes pérdidas. Otro factor a tener en cuenta está relacionado directamente con la información y es la confidencialidad de los datos, que se debe garantizar tanto a los datos almacenados en el dispositivo, como a la transmitida en las comunicaciones que éste realice, más si tiene relación directa con el Internet. Todos estos factores son considerados riesgos asociados a IoT[37].

Kris Flautner, director general de IoT en la empresa de seguridad ARM, expone que en teoría, los dispositivos IoT son muy susceptibles a ataques, ya que a menudo su seguridad no es muy buena, por tanto hay que saber sobre estos dispositivos y

[36] Symantec. iot-security-reference-architecture. [En línea]. 2016. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

[37] CSIRT-CV. Informe-Internet_de_las_Cosas. [En línea]. [Consultado el 14 de noviembre de 2017]. Disponible en internet: http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

cómo están configurados, Rob Ragan socio de seguridad sénior de Bishop Fox indica que la piratería informática está aumentando[38].

Internet de las cosas (IoT) plantea desafíos únicos para la seguridad, la privacidad y el cumplimiento a empresas de todo el mundo. A diferencia de la tecnología cibernética tradicional donde estos problemas giran en torno al software y cómo se implementa, a IoT le preocupa lo que sucede cuando los mundos cibernético y físico convergen. Proteger las soluciones IoT requiere garantizar el aprovisionamiento seguro de los dispositivos, proteger la conectividad entre estos dispositivos y la nube y garantizar la protección de los datos en la nube durante su procesamiento y almacenamiento. Sin embargo, trabajar con esta funcionalidad tiene sus inconvenientes: la limitación de recursos de los dispositivos, la distribución geográfica de las implementaciones y la existencia de un gran número de dispositivos dentro de una solución.[39]

De acuerdo a los pronósticos expuestos por la empresa Garner, para el año 2020 en el mercado la cantidad de dispositivos que se enmarcan dentro de este concepto de IoT, oscilaran entre unos 26 millones de objetos incorporados en todos los niveles de la sociedad. Por otra parte, Abi Research indica que el número de dispositivos inalámbricos que estarán conectados a internet ascenderán a 30 millones. Cada uno de estos elementos generara gran cantidad de datos, recursos que podrán ser utilizados para la toma de decisiones[40].

De acuerdo a estudios realizados sobre la materia, se expone uno de los factores de mayor preocupación que tiene el crecimiento e introducción acelerada de los dispositivos IoT, la agudización de los problemas de seguridad y de privacidad.

Esta situación representa nuevos retos desde varios campos de la seguridad, así como para el entorno académico y de investigación dado el alto impacto que puede generar la materialización de las amenazas que presentan los objetos del IoT, teniendo en cuenta que no solo se afectara la accesibilidad del mismo, si no que trasciende a afectar la integridad de la información personal que este recolecta.

2.2 MARCO CONTEXTUAL

La internet de las cosas “IoT” se puede definir como la interconexión digital de elementos de uso cotidiano con la red de internet, logrando que se genere un

[38] Dassault Systèmes. El internet de las cosas. [En línea]. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.3ds.com/es/historias/como-influye-la-tecnologia-en-el-futuro/el-internet-de-las-cosas/

[39] Microsoft. Seguridad de Internet de las cosas desde el principio. [En línea]. 2017. [Consultado el 15 de noviembre de 2017]. Disponible en internet: https://docs.microsoft.com/es-es/azure/iot-suite/securing-iot-ground-up

[40] Allied Business Intelligence, Inc. ABIresearch. [En linea]. [Consultado el 15 de noviembre de 2017]. Disponible en internet: https://www.abiresearch.com/

intercambio de información con otros dispositivos o núcleos de control con la particularidad que no se requiere intervención humana. Mediante la utilización de estos mecanismos se logra capturar gran cantidad de información clave para determinar condiciones comportamentales, usos y rendimiento, facilitando el monitoreo y operación de los mismos, así mismo generan nuevos campos de desarrollo y oportunidades inéditas para personas, empresas y ciudades.

Así mismo, la operatividad de estos dispositivos proporcionan entornos de eficiencia a partir de la obtención de información en tiempo real, que permiten conocer el estado de productos o servicios, con lo cual se pueden optimizar los procesos y dar un crecimiento sobre la productividad, generando así un mayor grado de ventaja y competitividad en el mercado ya que se pueden incorporar nuevas funcionalidades como valor agregado que repercutiría frente a otras ofertas.

Es tan amplio el mercado y el crecimiento de Internet of Things (IoT) que en cifras de dispositivos conectados, se estima alrededor de unos cinco mil millones de dispositivos intercambiando información, teniendo una expectativa de crecimiento de conexiones para el año 2020 de más de veinticinco mil millones, que tendrá un impacto considerado en las actividades que normalmente se desarrollan en el diario vivir, así mismo serán parte de un mercado influyente para la generación de recursos económicos.

De acuerdo a ello, se verá una gran transformación digital en la cual el IoT apalancará e integrara las tecnologías operaciones con las tecnologías informáticas, siendo adoptadas e impulsadas como una fuerza de trabajo digitalizado y móvil. Allí jugara un papel fundamental la incorporación que tengan estas herramientas en el ámbito empresarial quienes serán realmente las que den el valor protagónico y promuevan su expansión. Allí se abrirán nuevos mercados basados en la utilización de sensores más asequibles, medios de transmisión más eficientes y expandidos, medios de cloud computing e intervención de procesos analíticos avanzados.

También se encontrara bajo el marco del IoT, el aprovechamiento que tendrán los datos obtenidos mediante el flujo de procesos e interacción entre dispositivos, tomando así un valor muy importante para el crecimiento empresarial y buscar generar en el usuario nuevas experiencias de satisfacción mediante la transformación de la prestación de servicios. Además de ello, se pretenderá formar industrias eficientes donde la reducción de costos será uno de los mayores beneficios y puntos clave que impartirá el IoT. Así mismo, el IoT estará muy ligado a entornos de procesamiento en la nube, en los cuales dictara y promoverá una nueva forma de interacción expandida, disponiendo de recursos mediante la interoperalidad entre diversos sectores donde se buscara abarcar temas cruciales que están ligados a estas tecnologías como lo es la ciberseguridad. Estos ambientes de nube pública o privada involucrando las IoT, apalancaran nuevas soluciones para los usuarios finales que les dará la posibilidad de suplir las

deficiencias y necesidades de seguridad de igual forma con las industrias que aún no trascienden a estos nuevos retos tecnológicos.

2.3 MARCO CONCEPTUAL

El Internet de las Cosas e Industria 4.0 tuvo su origen en Alemania pero los conceptos están en armonía con las iniciativas mundiales, incluidas las fábricas inteligentes, “IoT industrial, la fabricación inteligente y avanzada.

Se catalogó como la cuarta revolución industrial, antecedida por tres revoluciones las cuales presentaron connotaciones como la mecanización de la producción mediante el uso de agua y vapor como medio de producción de energía, otra connotación la producción en masa donde se le atribuye a Henry Ford como su inventor y la era de la incursión digital.[41]

Pero el término “Internet of Things” fue propuesto por Kevin Ashon en 1999. El concepto se popularizó en el Auto-ID Center del MIT (Instituto de Tecnología de Massachusetts) y publicaciones relacionadas, para posteriormente ser utilizado alrededor del mundo para hablar de la interconectividad entre dispositivos que se ha dado de manera acelerada en los últimos decenios.

Pero solo fue hasta el año 2009 cuando Ashton manifiesta que, si bien fue probablemente la primera persona en decir “Internet de las cosas”, como un término para atraer la atención de los ejecutivos de la compañía P&G, hoy su importancia creció al punto de decirse que tiene el poder de cambiar al mundo. Su intención original con este nombre era la de referirse a la necesidad de obtener información del entorno, de los objetos, es decir de “las cosas”, sin depender de un humano quien es limitado en tiempo, atención y precisión; en otras palabras “no muy bueno” al capturar información.

Las capturas de datos bajo la idea de Ashton, se llevó a cabo inicialmente mediante la tecnología RFID “identificación de radio frecuencia”, pero esta trascendió a cualquier dispositivo capaz de conectarse a internet.

El haber sido expuesto este nuevo modelo revolución tecnológica, en un entorno empresarial buscando la automatización de procesos, se profundizo más adelante por Parthasarthy & Sethi en el año 1992, el análisis sobre el impacto de la automatización flexible determinado que las estrategias y la tecnología son reciprocas. Dentro del marco de trabajo propuesto, se obtienen resultados que permiten generar un mayor desempeño cuando la estrategia y la estructura están alineadas con el proceso de selección tecnológica.

[41] LYDON, Bill. Industria 4.0: producción inteligente y flexible. [En línea]. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.isa.org/intech/20160601/

Por tanto esta nueva tecnología impacta e involucra diversos entornos, la forma en que se comunican los seres humanos, ambientes de trabajo, procesos educativos, habita etc, con ello también se integran a nivel organización trascendiendo a la automatización de procesos y mejorar los sistemas existentes. El mundo tal cual como se conoce hoy en día, tendrá una transformación tecnológica, habrá muchos más dispositivos, vehículos, equipos y otros elementos de la vida diaria, con la posibilidad de interpretar los datos de su entorno, procesarlos o no y transmitirlos a otros sistemas, podemos aceptar que alguno de ellos tendrán funciones que les permiten ser autónomos, teniendo la potestad de tomar decisiones por si solos sin la intervención de los humanos.

No se debe ser ajeno a lo que representara el IoT, la evolución de Internet dará un enorme salto en su capacidad para reunir, analizar y distribuir datos que se transforman en información, conocimiento y en última instancia, sabiduría.

2.3.1 Desafíos que enmarcan al IoT

Esta nueva revolución tecnológica plantea grandes desafíos en virtud de los atributos que contendrán los dispositivos, se afrontaran consideraciones de seguridad con características nuevas y únicas, por tanto los esfuerzos por minimizar las afectaciones sobre los elementos deberán ser una prioridad fundamental. Ante ello, los distintos sectores que tendrán relación con esta tecnología, deben poder confiar en que al incorporar estas soluciones dentro de sus entornos productivos, dispondrán de ambientes seguros y libres de vulnerabilidades en la medida que estas sea más difundidas y se integren con el diario vivir.

Aquellos dispositivos y servicios enmarcados dentro de IoT y que presenten características de poco seguras o que sus políticas de protección sean inadecuadas, serán puntos débiles y riesgosos que podrán ser sujetos de ataques cibernéticos, dejando a merced de terceros la información que estos manejan la cual tendrá una connotación de confidencial.

Este ciclo de interconexión de dispositivos sin las medidas de seguridad adecuadas tendrá una repercusión mucho mayor cuando estos se encuentren enlazados con la red de internet pudiendo generar una afectación a escalas más allá del entorno en que llevan a cabo sus operaciones. Así mismo, los desafíos por garantizar la seguridad ira en ascenso, partiendo de que existirán factores como la gran cantidad de elementos inteligentes con características de homogeneidad, dispositivos que poseerán la capacidad de conectarse de forma automática a los ecosistemas y aquellos que se adecuen en entornos poco seguros.

En este orden de ideas, deberá existir una corresponsabilidad tanto en las áreas de desarrollo como en los mismos usuarios que harán uso de estos dispositivos, con el fin de asegurar la no exposición de sus clientes y de la misma internet a

situaciones de afectación, por tanto deberá dársele un enfoque colaborativo para desarrollar soluciones eficientes, adaptables y acordes a los desafíos de seguridad que emana IoT.

Otro punto neurálgico dentro de la adopción de IoT, es lo relacionado con la privacidad, existirán interrogantes frente a los lineamientos que se establecerán para respetar la reserva de la información y que se convertirán en factor primordial para que se dé una adopción plena del IoT, de igual forma esto fortalecerá la confianza de los usuarios frente al internet, los dispositivos y los servicios asociados.

Este contexto está planteando un rediseño sobre el IoT, conllevando a que posiblemente se den cambios transcendentales en la forma en que se recolectan, analizan, se aplican y utiliza los datos personales, adoptando las acciones necesarias que respeten las políticas de privacidad individuales, sin que estas tampoco interfieran con los avances e innovación en nuevas tecnologías y servicios.

Existe también, una situación que puede llegar a inhibir tanto a los usuarios como a las organizaciones, a que tengan un acercamiento a ciertas implementaciones o soluciones de IoT, la razón de ello radica en la ausencia de mecanismos de interoperabilidad, esta falta de flexibilidad y adaptación para integrarse a entornos, dispositivos, servicios, proveedores y nuevas tecnologías, generan escepticismo al momento de incorporar estas herramientas en los entornos productivos. Adicional a ello, también estarán presentes las falencias de diseño y malas configuraciones de los dispositivos, esto generara un ambiente negativo dentro de los entornos donde sean implementados. Aquí jugara un papel fundamental, la disponibilidad de estándares apropiados y precisos para contrarrestar la propagación de dispositivos defectuosos, permitiendo un mayor aprovechamiento de las ventajas que estas tecnologías proporcionan, ampliar el campo de innovación lo cual se reflejara en mejores oportunidades económicas.

De igual forma, otro de los desafíos a que se ve expuesto el IoT, tiene que ver con los lineamientos legales y reglamentarios, aquí se tendrá un acrecentamiento de los vacíos que se presentan en torno al internet, ello no es un caso alejado, el rápido avance tecnológico supera la capacidad de adopción de lineamientos, políticas o normas, dejando sin fundamentos y sin un soporte que garanticen la protección de los flujos de datos desde los diferentes puntos que se encierran bajo los dispositivos de IoT.

Finalmente el gran impacto y los entornos que involucran al IoT, obligaran a que estas tecnologías sean accesibles no solo a los países industrializados si no que deberán estar al alcance de todas las regiones, involucrando recursos de expansión tecnológica que garanticen la accesibilidad y nuevas oportunidades de negocios.

2.3.2 Seguridad de la información dentro de IoT

No es un secreto que en los últimos años, las tecnologías de la información (TI) han revolucionado el mundo en todos sus aspectos, desde las actividades más comunes de nuestra vida diaria, hasta las más complejas, a tal punto que ahorran tiempo, espacio y acortan distancias. Pero sin duda, así como proporcionan grandes beneficios, se debe tener mucho cuidado y tomar las medidas de prevención con el fin de defender uno de los recursos (datos - información) más valiosos dentro de los distintos entornos de la sociedad y dentro del ámbito productivo.

Este tipo de tecnología no es ajena a ser tratadas dentro del marco de la seguridad de la información dado el contexto y entorno sobre el cual opera, es allí que mediante esta premisa, se puede considerar a la seguridad de la información, como todos aquellos mecanismos, protocolos, procedimientos y normas adoptadas, que buscan garantizar que el recurso más valioso que es la información, no sea expuesto a vulneraciones y afectaciones de terceros, así mismo velar por la seguridad de los elementos que hacen parte del mundo IoT.

La seguridad de la información, es uno de los contextos que cada vez toma mayor importancia dentro del auge y puesta en marcha de IoT, sobre estos elementos recaerá la responsabilidad de la operatividad y manejo de operaciones trascendentales en todos los entornos de la sociedad los cuales operaran con insumos valiosos como los datos.

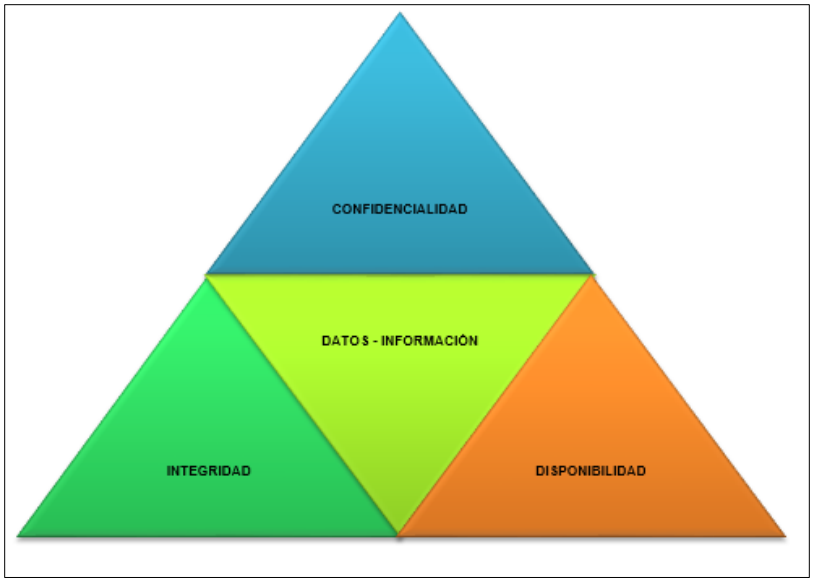
Por tanto, la seguridad de la información no se deberá considerar como una simple instrucción o ejercicio de cumplimiento, se deberá pasar del modelo pasivo a darle un nuevo enfoque integrado y predictivo que abarque todos los puntos involucrados dentro del proceso, es decir desde el momento de la creación de un elemento inteligente, hasta la última fase que involucre el ecosistema IoT. Por consiguiente, dentro de esta nueva esfera tecnológica también deberán garantizarse los pilares esenciales que fundamentan la seguridad de la información, la confidencialidad, integridad y disponibilidad, tomando como referencia las directrices expuestas mediante la norma ISO/IEC 27001:2013, la cual expone los procedimientos, políticas y protocolos que se deben tener en cuenta para garantizar estos tres pilares de la seguridad. (Ver ilustración 2)

- Confidencialidad, pretende garantizar que la información, almacenada y que fluye a través del recurso tecnológico o que se transmite por la red, solamente va a ser accesible por personal autorizado.

- Integridad, busca que los recursos de información que fluyen o se almacenan dentro del recurso tecnológico conserve su estado de originalidad y que no sufra alteraciones sin la debida autorización.

- Disponibilidad, la accesibilidad tanto al recurso tecnológico como de información debe estar garantizada para ser usada sin ninguna interrupción.

Ilustración 2. Pilares seguridad de la información



Fuente: Los autores

Los recursos tecnológicos que se enmarcan dentro del IoT, estarán sujetos a sufrir afectaciones por sus estructuras haciéndolos vulnerables a riesgos y amenazas. A partir de ello, será muy importante que estos elementos tengan una clasificación en pro de asegurar que la información cuente con los niveles de protección adecuados y sus tratamientos según su valoración. En este orden de ideas, los elementos de IoT deberán estar clasificados de acuerdo a los lineamientos que se describen en la tabla 1.

Tabla 1. Clasificación según su confidencialidad, integridad y disponibilidad

Confidencialidad Hace mención a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados	
Información pública reservada	Información disponible sólo para un escenario, dado el caso que esta pueda ser accedida o conocida por terceros sin previa autorización, podrá generar consecuencias negativas bajo criterios de legalidad, operatividad, credibilidad y factores económicos.
Información pública clasificada	Información disponible para todos los procesos dentro del escenario y dado el caso que esta pueda ser accedida o conocida por terceros sin previa autorización, podrá generar consecuencias negativas dentro del mismo desarrollo. Esta información es propia del entorno o de terceros con la autorización respectiva y puede ser utilizada por todos los involucrados dentro del proceso para realizar labores propias.

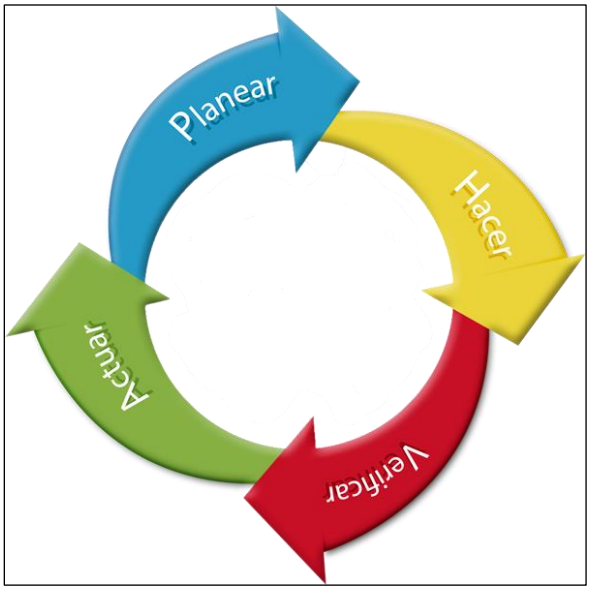
Tabla 1. (Continuación)

Confidencialidad Hace mención a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados	
No clasificada	Recursos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como recursos de INFORMACIÓN PUBLICA RESERVADA.
Información pública	Información que puede ser trasmitida o divulgada sin restricciones a cualquier persona dentro y fuera del entorno, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
Integridad Hace mención a la exactitud y completitud de la información, esta característica es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción	
A (ALTA)	Recursos de Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar los procesos o generar una pérdida de credibilidad severa sobre las soluciones o productos creados y de la organización.
M (MEDIA)	Recursos de Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar los procesos o generar una pérdida de credibilidad moderada sobre las soluciones o productos creados y de la organización.
B (BAJA)	Recursos de Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo de las soluciones o productos creados o agentes externos.
NO CLASIFICADA	Recursos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como recursos de información de integridad ALTA.
Disponibilidad Hace mención a que la accesibilidad y usabilidad debe estar siempre dispuesta para el entorno requerido y en la forma que se solicite dentro de los parámetros autorizados.	
A (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar los procesos, o generar pérdidas de credibilidad severas a entes externos.
M (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar los procesos, o generar pérdidas de credibilidad severas a la organización.
B (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la organización o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de credibilidad.
NO CLASIFICADA	Recursos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como recurso de información de disponibilidad ALTA.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. Guía para la Gestión y Clasificación de Activos de Información. [En línea]. 2016. [Consultado el 14 de noviembre de 2017]. Disponible en internet: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html. 16 p.

Mediante la norma citada y en conjunto con el ciclo PHVA, se realizan los análisis de los procesos para la gestión de la seguridad tomando como una constante la mejora continua a través de las cuatro fases “Planificar, Hacer, Verificar y Actuar” tal y como se observa en la ilustración 3.

Ilustración 3. Ciclo PHVA



Fuente: Auditoría y control interno. Ciclo PHVA. [En línea]. 2015. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://audycontrolintunivers2015.blogspot.com.co/2015/04/ciclo-phva.html

- Planificar, dentro de esta fase se lleva a cabo de definición de los objetivos y el medio que permitirá su cumplimiento.

- Hacer, comprende las actividades o acciones planeadas para el complimiento de los objetivos.

- Verificar, a través de esta fase se adelantan las acciones de seguimiento frente al cumplimiento de los objetivo determinando el grado de avance.

- Actuar, de acuerdo al análisis aplicado en la verificación se determinan y adelantan las acciones correctivas requeridas en pro del cumplimiento de los objetivos.

El amplio mercado que generara la incorporación de un gran número de dispositivos inteligentes y que constituirán el ecosistema de IoT, traerá consigo una extensa puerta a las amenazas, vulnerabilidades y riesgos que serán el mayor desafío a que se enfrentaran tanto fabricantes y consumidores. Cabe traer a colación estos factores que enmarcaran la puesta en operatividad de esta nueva revolución tecnológica.

- Amenazas del IoT: Comprende todo aquello que puede generar afectación a la seguridad de los recursos tecnológicos y/o de información. Frente a esta situación, las amenazas a que se encuentran expuestos los dispositivos de IoT no difieren frente a las de los otros recursos que hacen uso de la conexión a la

red, su principal diferencia se centra en el volumen excesivo de dispositivos conectados, su permanente conexión, ausencia de seguridad que se fundamenta por el diseño y bajo costo. Partiendo de ello, las amenazas del IoT pueden ser englobadas bajo criterios de privacidad, protección y seguridad.

Existen diversas afirmaciones donde dejan ver la preocupación en relación con el efecto devastador que pueden generar las amenazas de seguridad para todo el ecosistema que conforma IoT, su estructuración será un blanco fijo para llevar a cabo acciones como el espionaje a todos los niveles, denegación de servicios entre otros ataques. Todo ello, enlazado con la intranquilidad frente a la protección del flujo de datos que se moverán a través de la red y que pueden estar al alcance de los delincuentes informáticos.

Allí se deberá tener presente que esta tecnología está en un proceso de inserción dentro de los entornos de la sociedad, para lo cual, la evaluación de las necesidades de protección, deberán estar abiertas al avance e innovación y cubrir los sectores de inmersión de estas soluciones. Así mismo, se debe tener presente que al ser parte esencial de la operatividad de estos dispositivos su interconexión, ocasiona una pérdida de la protección dentro del ámbito físico, esto debido a las condiciones de ubicación lo cual profundizara su exposición a ser sujeto de afectación.

Ay que dejar claro que las amenazas siempre existirán y más aun con esta nueva incursión tecnológica, ante ello se deberán optar por incorporar acciones para minimizar en gran parte todo este escenario, como por ejemplo optimizar los mecanismos de cifrado de datos, reforzar la autenticación, estructurar una codificación resistente y estandarizar las interfaces de aplicación para que estas actúen de forma predecible, así mismo existirán factores propios de los dispositivos que requerirán una dependencia sobre otros elementos para contrarrestar acciones amenazantes.

- Vulnerabilidad de IoT: Abarca todas aquellas debilidades que posean los recursos, entornos y ecosistemas que comprometen la seguridad de los mismos, por tanto se debe tener conciencia de que si no adoptan las medidas suficientes existirá una gran afectación negativa con desenlaces devastadores.

Partiendo de ello se describe lo expuesto por la OWASP[42], organismo que plantea algunos lineamientos a tener en cuenta tanto parar fabricantes, desarrolladores y consumidores frente a los inconvenientes de seguridad que se relacionan con los ecosistemas de IoT. (Ver tabla 2).

[42] OWASP. OWASP Internet of Things Project. [En linea]. 2018. [Consultado el 28 de marzo de 2018]. Disponible en internet:https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities

Tabla 2. Lineamientos expuestos por OWASP vulnerabilidades IoT

Vulnerabilidad	Superficie de ataque	Resumen
Cuentas de acceso	Interfaz administrativa	Posibilidad de recopilar un conjunto de nombres de usuario válidos mediante la interacción con el mecanismo de autenticación.
	Interfaz web del dispositivo	
	Interfaz de la nube	
	Aplicación móvil	
Contraseñas débiles	Interfaz administrativa	Estructuras deficientes que permiten programar contraseñas débiles. Uso de contraseñas predeterminadas pre programadas.
	Interfaz web del dispositivo	
	Interfaz de la nube	
	Aplicación móvil	
Bloqueo de cuenta	Interfaz administrativa	Procedimientos recurrentes que permiten un número indefinido de intentos para acceder al recurso.
	Interfaz web del dispositivo	
	Interfaz de la nube	
	Aplicación móvil	
Servicios sin cifrado	Servicios de red de dispositivo	Los servicios de red no están encriptados correctamente para evitar el espionaje o la manipulación por parte de los atacantes
Autenticación de doble factor	Interfaz administrativa	La falta de mecanismos de autenticación de doble factor amplían los entornos de vulneración, la incorporación de herramientas como el token de seguridad o un escáner de huellas dactilares serán de gran beneficio.
	Interfaz web de la nube	
	Aplicación móvil	
Cifrado mal implementado	Servicios de red de dispositivo	Se incorporan acciones de cifrado pero este no se aplica de forma correcta
Actualización enviada sin encriptación	Mecanismo de actualización	Las actualizaciones se transmiten a través de la red sin usar TLS o encriptando el archivo de actualización
Actualizar ubicación escritura	Mecanismo de actualización	La ubicación de almacenamiento para los archivos de actualización es mundialmente modificable, lo que permite modificar y distribuir el firmware entre todos los usuarios
Negación de servicio	Servicios de red de dispositivo	El servicio puede ser atacado de manera que niega el servicio a ese servicio o a todo el dispositivo
Eliminación de medios de almacenamiento	Interfaces físicas del dispositivo	Posibilidad de eliminar físicamente los medios de almacenamiento del dispositivo
Sin mecanismo de actualización manual	Mecanismo de actualización	Sin posibilidad de forzar manualmente una verificación de actualización para el dispositivo
Mecanismo de actualización faltante	Mecanismo de actualización	Los dispositivos no cuentan con mecanismos para su actualización
Visualización de la versión del firmware y / o la última fecha de actualización	Firmware del dispositivo	No se evidencia la versión del firmware que utiliza el dispositivo ni la fecha de su última actualización
Extracción de firmware y almacenamiento	Interfaz JTAG / SWD	El firmware contiene mucha información útil, como código fuente y binarios de servicios en ejecución, contraseñas preestablecidas, claves ssh, etc.
	Dumping in situ	
	Interceptar una actualización de OTA	

Tabla 2. (Continuación)

Vulnerabilidad	Superficie de ataque	Resumen
	Descarga desde la página web del fabricante	
	tapping eMMC	
	Desoldar el chip SPI Flash / eMMC y leerlo en un adaptador	
Manipular el flujo de ejecución de código del dispositivo	Interfaz JTAG / SWD	Con la ayuda de un adaptador JTAG y gdb podemos modificar la ejecución del firmware en el dispositivo y eludir casi todos los controles de seguridad basados en software.
	Ataques de canal lateral como glitching	Los ataques de canal lateral también pueden modificar el flujo de ejecución o se pueden usar para filtrar información interesante del dispositivo
Obteniendo acceso a la consola	Interfaces en serie (SPI / UART)	Al conectarnos a una interfaz en serie, obtendremos acceso total a la consola de un dispositivo
		Por lo general, las medidas de seguridad incluyen cargadores de arranque personalizados que evitan que el atacante ingrese al modo de usuario único, pero también se pueden omitir.
Componentes inseguros de terceros	Software	Versiones desactualizadas de busybox, openssl, ssh, servidores web, etc.

Fuente: OWASP. OWASP Internet of Things Project. [En línea]. 2018. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities

- Riesgos de IoT: Se relaciona a aquellas situaciones que impiden u obstaculizan la operatividad de los recursos imposibilitando el desarrollo de las funciones respectivas. Es así, que al proliferase esta nueva revolución tecnológica lo hará de la mano de una serie de deficiencias de seguridad que afectaran la privacidad de información confidencial.

Ante ello, las tecnologías de Iot se enfrentan a una serie de riesgos tales como:

Limitación del recurso: La gran mayoría de los dispositivos IoT presentan un limitante de capacidades de procesamiento, memoria y potencia, por lo cual es improbable que se le puedan aplicar los controles de seguridad avanzados de forma eficaz.

Ecosistemas complejos: Existe una mayor preocupación frente a los entornos de seguridad dado que las soluciones IoT deben verse como un ecosistema, lo cual implica que se incorporen otros elementos de comunicación, interfaz y personas.

Bajo costo: Existirán limitantes frente a la incorporación de mecanismos de seguridad en los dispositivos por parte de los fabricantes buscando disminuir los

costos, ante ello será muy factible que el mismo dispositivo sea incapaz de contener los ataques.

Falta de experiencia: Al ser una tecnología emergente, se expondrá a la falta de recurso humano idóneo para el manejo de la seguridad que permitan una reacción inmediata ante alguna situación indeseable.

Diseños de dispositivos inseguros: El afán por producir y comercializar los dispositivos harán que los factores de seguridad pasen a no ocupar en factor clave dentro de los objetivos de los fabricantes.

Ausencia de controles: Aquí se involucra el tratamiento que se le dan a los datos recolectados a través de los dispositivos inteligentes, es muy común que los usuarios no visualicen la importancia que tiene el tratamiento de la información, esto es aprovechado por estos entornos exponiendo la información a terceros sin que el propietario tenga el debido conocimiento.

Entornos privados: La incorporación de esta nueva tecnología hará que todo sea visible, por tanto se deberán optar por la aplicación de mecanismos eficientes que permitan la privacidad en todos los entornos de quien hace uso de los dispositivos.

Mayor eficiencia: Entran en juego dos factores, la seguridad frente a la eficiencia, ello pondrá a prueba a quienes fabrican los dispositivos, encontrándose bajo las directrices de dar cumplimiento a la comercialización acelerada de esta tecnología limitando el desarrollo de entornos seguros para ella. Adicional a ello, se encontraran con presupuestos débiles ante lo cual primara la funcionalidad y usabilidad que la seguridad.

Clarificación de las responsabilidades: Este entorno es de gran importancia, dado que da el alcance y límites de responsabilidad ante alguna situación que ponga en riesgo la seguridad del entorno IoT, allí se involucran tanto a fabricantes, prestadores de servicios y usuarios, por consiguiente una mala estipulación de ellos será contraproducente paras las partes.

2.3.3 Criterios de valoración

De acuerdo a la evaluación que se realiza a los elementos que conforman el Internet de las Cosas (IoT), es necesario estipular las convenciones que se aplican dentro del proceso de valoración de riesgos y vulnerabilidades.

En la tabla 3, se muestran los criterios para la asignación de las dimensiones de seguridad.

Tabla 3. Criterios para las dimensiones

DIMENSIONES	
Nomenclatura	**Categoría**
B	Bajo
M	Medio
A	Alto
MA	Muy Alto
MB	Muy Bajo

Fuente: Los autores

En la tabla 4, se muestran los criterios de valoración para la probabilidad del riesgo.

Tabla 4. Criterios para probabilidad del riesgo

PROBABILIDAD DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Probabilidad	MA	**Prácticamente seguro**	5
	A	**Probable**	4
	M	**Posible**	3
	B	**Poco probable**	2
	MB	**muy raro**	1

Fuente: Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas. [En línea]. 2012. [Consultado el 28 de marzo de 2018]. Disponible en línea: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WtO5SZq23IU. 7 p.

En la tabla 5, se muestran los criterios de valoración para el impacto del riesgo.

Tabla 5. Criterios para impacto del riesgo

IMPACTO DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Impacto	MA	**Muy Alto**	5
	A	**Alto**	4
	M	**Medio**	3
	B	**Bajo**	2
	MB	**Muy Bajo**	1

Fuente: Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas. [En línea]. 2012. [Consultado el 28 de marzo de 2018]. Disponible en línea: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WtO5SZq23IU. 6 p.

En la tabla 6, se muestran los criterios de valoración del riesgo.

Tabla 6. Criterios para valoración del riesgo

VALORACIÓN DEL RIESGO						
IMPACTO	MA	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5
RIESGO		MB	B	M	A	MA
		PROBABILIDAD				

Fuente: Los autores

En la tabla 7, se muestran las convenciones para la valoración del riesgo.

Tabla 7. Convención para la valoración del riesgo

CATEGORÍA DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoración del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente: Los autores

En la tabla 8, se muestran las convenciones para la criticidad neta.

Tabla 8. Convención para la criticidad neta

CRITICIDAD NETA		
Nomenclatura	Categoría	Valoración
C	**Critico**	21 a 25
I	**Importante**	16 a 20
A	**Apreciable**	10 a 15
B	**Bajo**	5 a 9
D	**Despreciable**	1 a 4

Fuente: Los autores

En la tabla 9, se muestran las convenciones para la criticidad residual.

Tabla 9. Convención para la criticidad residual

CRITICIDAD RESIDUAL		
Nomenclatura	**Categoría**	**Valoración**
C	**Critico**	21 a 25
I	**Importante**	16 a 20
A	**Apreciable**	10 a 15
B	**Bajo**	5 a 9
D	**Despreciable**	1 a 4

Fuente: Los autores

En la tabla 10, se muestran las convenciones para el nivel de aceptación del riesgo.

Tabla 10. Convención para la aceptación del riesgo

NIVEL DE ACEPTACIÓN DEL RIESGO		
Nomenclatura	**Categoría**	**Valoración**
I	**Inaceptable**	16 a 26
M	**Moderado**	6 a 15
A	**Aceptable**	1 a 5

Fuente: Los autores

En la tabla 11, se muestran las convenciones para la calificación de gestión.

Tabla 11. Convención para la aceptación del riesgo

ACEPTACIÓN DEL RIESGO	
Categoría	**Valoración**
Control no existe	1
Existe pero no efectivo	2
Efectivo pero no documentado	3
Efectivo y documentado	4

Fuente: Los autores

2.4 ANTECEDENTES

Con el fin de aproximar esta investigación frente al tema de la seguridad de los dispositivos que se enmarcan dentro del IoT y que tienen injerencia sobre los procesos organizacionales, se describen algunos antecedentes que servirán de herramienta de apoyo para comprender la importancia de la temática abordada.

Entre estos se pueden mencionar:

Proyecto "**Seguridad en internet de las cosas**"[43], presentado por Daniel Felipe Tarquino Murgueito y Edwin Sebastián García García. El propósito principal llevado a cabo, fue la investigación y revisión de escenarios en los cuales se están implementando el internet de las cosas, describiendo las amenazas y sus posibles soluciones.

Proyecto "**Arquitectura de seguridad ligera para el internet de las cosas basada en HIMNO**"[44], presentado por José Luis Torre Arce. A través de este documento se plantea una nueva arquitectura de seguridad para el Internet de las Cosas basados en HIMMO para hacer frente a esa problemática. Para ello, se analiza el escenario del Internet de las cosas y se presenta una lista de requerimientos que una arquitectura de seguridad del Internet de las cosas debería cumplir, teniendo en cuenta todo el ciclo de vida de un dispositivo desde el momento en que es fabricado. Con base en este análisis, diseñamos una arquitectura de seguridad para el Internet de las cosas y su implementación de software. Creamos una aplicación de software para las criptografías primitivas utilizadas en nuestra arquitectura de manera que puedan ser utilizadas en el futuro para probar su desempeño en diferentes escenarios. Por último, se presentan los resultados de rendimiento que apoyan nuestra afirmación de que nuestra solución es factible bajo las limitaciones de los dispositivos del Internet de las cosas"

Proyecto "**Internet de las cosas privacidad y seguridad**"[45], presentado por Miguel Castro Sola. El proyecto plantea el estudio sobre las cuestiones de privacidad y seguridad de los datos en el paradigma de internet de las cosas. Allí se buscan analizar en profundidad todos los cambios que va a suponer la implantación de esta nueva forma de entender la tecnología en general, y con ella la sociedad y la manera de hacer las cosas tanto cotidianas como laborales.

Una vez hecho esto, se analizan y evalúan los riesgos que conlleva vivir inmersos en esta tecnología, donde toda la información estará al alcance de "todo y todos" y finalmente se exploran y se proponen diferentes soluciones para estos problemas.

Proyecto "**La protección de datos ante el Internet de las Cosas**"[46], presentado por María Teresa Romero García. El proyecto hace una incursión frente al internet de las cosas, pasado, presente y futuro, sus características y entornos de

[43] TARQUINO MURGUEITO, Daniel Felipe y GARCÍA GARCÍA, Edwin Sebastián. Escuela Colombiana de Ingeniería Julio Garavito. Trabajo fin de grado: Seguridad en Internet de las cosas. [En línea]. 2017. [Consultado 27 de marzo de 2018]. Disponible en internet: https://repositorio.escuelaing.edu.co/handle/001/605

[44] TORRE ARCE, José Luis. Universidad de Cantabria. Trabajo fin de grado: Arquitectura de seguridad ligera para el Internet de las Cosas basada en HIMMO. [En línea]. 2015. [Consultado el 18 de noviembre de 2017]. Disponible en internet: https://repositorio.unican.es/xmlui/handle/10902/7228

[45] CASTRO SOLA, Miguel. Universidad de Jaén. Trabajo fin de grado: Internet de las cosas. Privacidad y Seguridad. [En línea]. 2016. [Consultado el 18 de noviembre de 2017]. Disponible en internet: http://sinbad2.ujaen.es/sites/default/files/publications/Memoria_0.pdf

[46] ROMERO GARCÍA, María Teresa. La protección de datos ante el Internet de las cosas. [En línea]. 2017. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://oa.upm.es/47426/

aplicabilidad, así mismo lleva a cabo un análisis frente a las amenazas y riesgos a que se enfrenta la sociedad al introducirse dentro del mundo de IoT.

Proyecto "**Panorama de aplicación de internet de las cosas (IoT)**"[47], presentado por David Leonardo Pinzón Niño. El documento encierra la temática relacionada con el internet de las cosas y los campos de acción dentro de la sociedad, mediante ello se pretenden abrir nuevos panoramas de IoT que permitan expandir los campos de investigación de la Universidad.

Libro blanco de ciberseguridad IoT de Huawei "**Creación de un mundo IoT fiable y gestionado**"[48], redactado por INCIBE, Red.es, Huawei. Este documento busca la unificación de los gobiernos, organizaciones internacionales y sectores verticales para conseguir que el ecosistema del Internet de las Cosas sea más seguro, así como para desarrollar políticas orientativas, promulgar leyes y reglamentos, establecer normas, implantar nuevas tecnologías y desarrollar ecosistemas de IoT fiables, gestionados y compartidos que beneficien a todos los interesados.

Documento "**Futuro inteligente**"[49] redactado por Leandro Zanony. El documento da una explicación de cómo el hombre cada vez es más consumista, y los errores que se están cometiendo frente a no mediar la seguridad, frente a los dispositivos conectados, todo con el afán de estar en el círculo de la moda.

2.5 MARCO LEGAL

En materia legal frente a la temática del IOT no es muy amplia y específicamente para Colombia es casi nula, por tanto las normativas que aborden estos mecanismos de interacción entre dispositivos y sobre los cuales se intercambia información se encuentra en una fase de observación basada en los comportamientos que se lleven a cabo mediante dichos dispositivos. Sin embargo a lo largo del tiempo se han venido abordando temáticas sobre la protección de información realizada mediante el uso de elementos tecnológicos, así mismo garantizar la confidencialidad e integridad de datos personales y procesos transaccionales.

[47]PINZÓN NIÑO, David Leonardo. Panorama de aplicación de internet de las cosas (IoT). [En línea]. 2015. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://repository.usta.edu.co/handle/11634/201/browse?type=author&value=Pinz%C3%B3n+Ni%C3%B1o%2C+David+Leonardo

[48] INCIBE, Red.es, Huawei. Creación de un mundo IoT fiable y gestionado. [En línea]. 2017. [Consulado el 19 de noviembre de 2017]. Disponible en internet: https://underc0de.org/foro/almacen-de-manuales/(pdf)-libro-blanco-de-ciberseguridad-iot-de-huawei/

[49] ZANONY, Leandro. Futuro inteligente. [En línea]. 2014. [Consultado el 19 de noviembre de 2017]. Disponible en internet: http://appstercerclick.com/futurointeligente/FuturoInteligente.pdf

2.5.1 Nacionales

2.5.1.1 Ley 527 de 1999[50]

“Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

2.5.1.2 Ley 1266 de 2008[51]

“Contempla las disposiciones generales en relación al Derecho de Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

2.5.1.3 Ley 1273 de 2009[52]

“Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

2.5.1.4 CONPES 3701[53]

“Lineamientos de política para ciberseguridad y ciberdefensa”.

2.5.1.5 Ley 1480 de 2011[54]

A través de la cual se establecen los mecanismos de protección al consumidor por medios electrónicos, seguridad en transacciones electrónicas.

---

[50] COLOMBIA CONGRESO DE LA REPUBLICA. Ley 527. Bogotá. (Agosto 18 de 1999). Diario Oficial 43.673 de agosto 21 de 1999. p. 19.
[51] COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (diciembre 31 de 2008). Diario Oficial 47219 de diciembre 31 de 2008. p. 17.
[52] COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (enero 5 de 2009). Diario Oficial 47223 de enero 5 de 2009. p. 5.
[53] DEPARTAMENTO NACIONAL DE PLANEACIÓN. CONPES 3701. Bogotá. (julio 14 de 2011). p. 43
[54] COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1480. Bogotá. (octubre 12 de 2011). Diario Oficial 48220 de octubre 12 de 2011. p. 33.

2.5.1.6 Ley 1581 de 2012[55]

A través de esta normativa se reglamenta el régimen general de la protección de datos personales en Colombia.

2.5.1.7 Decreto 2758 de 2012[56]

"Se reestructura la organización del Ministerio de Defensa, en el sentido de asignar al despacho del Viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.

2.5.1.8 Resolución SIC No. 76434[57]

"Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países".

2.5.1.9 Resolución 3933 de 2013[58]

"Creó el Grupo ColCERT y asignó funciones a la dependencia de la Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional, respecto a promover el desarrollo de capacidades locales/sectoriales para la gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil".

2.5.1.10 Decreto 1377 de 2013[59]

Mediante la cual se reglamenta parcialmente la ley 1581 de 2012 y se establecen nuevas medidas para la protección de datos personales.

---

[55] COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1581. Bogotá. (octubre 18 de 2012). Diario Oficial 48587 de octubre 18 de 2012. p. 15.
[56] COLOMBIA CONGRESO DE LA REPUBLICA. Decreto 2758. Bogotá. (diciembre 28 de 2012). Diario Oficial 48658 de diciembre 29 de 2012. p. 2.
[57] COLOMBIA MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Resolución 76434. Bogotá. (diciembre 4 de 2012). p. 13
[58] MINISTERIO DE DEFENSA NACIONAL. Resolución 3933. Bogotá. (junio 4 de 2013). Diario Oficial 48813 de junio 7 de 2013. p. 3.
[59] COLOMBIA CONGRESO DE LA REPUBLICA. Decreto 1377. Bogotá. (junio 27 de 2013). Diario Oficial 48834 de junio 27 de 2013. p. 11.

2.5.1.11 Ley 1712 de 2014[60]

Por la cual se regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y excepciones a la publicidad de la información.

2.5.1.12 Decreto 857 de 2014[61]

“Por medio del cual se reglamenta la Ley estatutaria 1621 de 2013, que establece el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, para cumplir con su misión constitucional y legal. Adicionalmente, establece la reserva legal, los niveles de clasificación y el sistema para la designación de los niveles de acceso a la información y clasificación de documentos”.

2.5.1.13 CONPES 3854[62]

“Política nacional de seguridad digital”.

2.5.1.14 Resolución 2710 de 2017[63]

“por la cual se establecen lineamientos para la adopción del protocolo IPv6”

2.5.2 Internacionales

2.5.2.1 ETS No.185 Convenio sobre ciberdelincuencia[64]

“La Convención es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. También contiene una serie de poderes y procedimientos tales como la búsqueda de redes de computadoras y la interceptación.

Su principal objetivo, establecido en el preámbulo, es perseguir una política criminal común dirigida a la protección de la sociedad contra el delito cibernético,

[60] COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1712. Bogotá. (marzo 4 de 2014). Diario Oficial 49084 de marzo 4 de 2014. p. 14.
[61] COLOMBIA CONGRESO DE LA REPUBLICA. Decreto 857. Bogotá. (mayo 2 de 2014). Diario Oficial 49143 de mayo 6 de 2014. p. 8.
[62] DEPARTAMENTO NACIONAL DE PLANEACIÓN. CONPES 3854. Bogotá. (abril 11 de 2016). p. 91
[63] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Resolución 2710. Bogotá. (octubre 3 de 2017). Diario Oficial 50376 de octubre 4 de 2017. p. 4
[64] CONCEJO DE EUROPA. Tratado 185. Budapest. (noviembre 23 de 2001). p. 26.

especialmente mediante la adopción de legislación apropiada y el fomento de la cooperación internacional."

2.5.2.2 Resolución AG /RES 2004[65]

"Mediante la cual se establece una estrategia integral para combatir las amenazas a la seguridad cibernética con un enfoque multidimensional y multidisciplinario, para la creación de una cultura de la seguridad cibernética".

[65] ASAMBLEA GENERAL DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Resolución AG /RES 2004. EEUU. (junio 8 de 2004). p. 46

2.6 DISEÑO METODOLÓGICO

2.6.1 Unidad de análisis

La presente investigación está constituida por la determinación e identificación de los factores a que se exponen los dispositivos del IoT, que operan dentro de los ambientes empresariales.

2.6.2 Población y Muestra

2.6.2.1 Población

El desarrollo del proyecto está dirigido a las áreas de tecnología de las organizaciones, que incorporen para el desarrollo de sus actividades misionales dispositivos que se enmarcan dentro del grupo de IoT.

2.6.2.2 Muestra

Para determinar los criterios y deficiencias de seguridad, se tomaran muestras basadas en pruebas de pentest, sobre algunos dispositivos IoT y que son utilizados por las organizaciones para el desarrollo de sus actividades misionales.

2.6.3 Estudio metodológico

Esta monografía se orienta desde un enfoque cualitativo, que permite reflexionar sobre la incidencia de la arquitectura de software en la vida cotidiana de los individuos y la internet de las cosas “Se enfoca a comprender y profundizar los fenómenos, explorándolos desde la perspectiva de los participantes en un ambiente natural y en relación con el contexto”, Sampieri. (1998). Tiene como finalidad la construcción de procedimientos para minimizar los riesgos del IoT dentro de las organizaciones, la metodología propuesta es de tipo descriptivo dado que esta busca determinar las condiciones, características, comportamientos mediante la descripción exacta de las acciones, elementos, métodos e individuos.

Métodos cualitativos, son las maneras en las cuales se va a recolectar la información y generar los instrumentos e insumos académicos para sacar adelante la información de trabajo y constituir un cuerpo elaborado que genere nuevas formas de conocimiento, por ello a continuación se enuncian los principales elementos que se utilizaran dentro de la investigación.

Hay una gran variedad de métodos que son comunes en la medición cualitativa. De hecho, los métodos están en gran medida limitados por la imaginación del investigador.

2.6.3.1 Observación del participante

En esta se hace necesario tener una participación directa por parte del investigador, buscando generar estrategias de análisis capaces de dar cuenta de los elementos a investigar, por ejemplo durante los 5 años que ha funcionado el proyecto, donde se da la inmersión de los actores por medio de experiencias significativas capaces de alcanzar descripciones asertivas de los lugares visitados.

2.6.3.2 Observación directa

Se basa en las observaciones directas sobre el tema propuesto haciendo coincidir las materias que se han presentado y los elementos propios de la investigación, por medio de las descripciones definidas que dan las características de las actividades a desarrollar dentro del conjunto investigativo, dentro de esta participación metodológica se hace necesario hablar de cómo lograr una consulta de temas sin llegar a intervenir en ellos, haciéndola de tipo objetivo.

2.6.3.3 Estudios de caso

Un estudio de caso es un estudio intensivo de un individuo específico o contexto específico. Por ejemplo, Freud desarrolló estudios de casos de varios individuos como base para la teoría del psicoanálisis y Piaget hizo estudios de casos de niños para estudiar las fases de desarrollo. No hay una sola manera de llevar a cabo un estudio de caso, y una combinación de métodos (por ejemplo, entrevistas no estructuradas, observación directa) pueden ser utilizadas.

Si bien es cierto no hay una sola manera de sistematizar y ahí está la riqueza de esta estrategia de adquisición del conocimiento se tomara finalmente en cuenta la Sistematización de los 5 tiempos de Jara (1994), los cuales son:

2.6.3.4 Punto de partida

Se inicia con los actores primarios en la búsqueda de su papel investigativo dentro de la sistematización con quienes se buscan los registros escritos, visuales y audiovisuales que den cuenta de los momentos de la sistematización

2.6.3.5 Preguntas iniciales

es la manera de entender como iniciar el proyecto investigativo y la sistematización de la experiencia, ¿De qué manera la sistematización de una experiencia en el campo de la pedagogía crítica y alternativa contribuye a la cualificación de las prácticas de enseñanza en espacios de la localidad de Bosa para estudiantes, padres de familia y docente del grado tercero de la IED Pablo de Tarso?, así como

complemento de las sub preguntas de apoyo metodológico ¿Por qué y para qué sistematizar una experiencia en el campo de las pedagogías críticas y alternativas?, ¿Cuáles son las opciones didácticas qué se hacen visibles a través de la sistematización de una experiencia pedagógica en el campo de la educación alternativa?, ¿De qué modo la intención por sistematizar una experiencia contribuye a la reflexión y transformación de la propia práctica?

2.6.3.6 Recuperación del proceso vivido

Para este punto se tienen en cuenta teniendo en cuenta dos momentos: por un lado acudir a la reconstrucción desde lo histórico, teniendo en cuenta las situaciones, acontecimientos que se ordenan de manera cronológica, por el otro lado en un segundo momento se ordena y se hace la clasificación de la información para generar un fichero de la experiencia, desde ahí se hace el procesos descriptivo basado en primera instancia en la observación.

2.6.3.7 Reflexión de fondo o ¿Por qué paso lo que paso?.

En este momento de la metodología se interpreta críticamente los aspectos relevantes de la sistematización, pasando a la conceptual, desde ahí se hace necesario desarrollar un ejercicio analítico serio de manera dialéctica puedan evidenciar como se dio la sistematización para retomar aspectos centrales del proceso de manera sintética desde el interior de la situación realizando una síntesis del mismo, para poder llegar a hacer una conceptualización del mismo a partir de las categorías emergentes del mismo, que son aquellos enunciados con los que se busca explicar el proceso, las dinámicas y las actividades presentes en el desarrollo del trabajo, "(…) decir esos enunciados con los cuales nombra, es un ejercicio desde el cual se visibiliza la cualidad que ha tenido su práctica y la vivencia profunda en su subjetividad. En el nombrar se da el reconocimiento y se hacen visibles los nuevos aprendizajes logrados por los diferentes actores participantes de la experiencia" (Mejía, 2008, p.94)

Las categorías de análisis se toman desde una perspectiva inductiva en la cual el tratamiento de datos sea manejada a partir de lo cualitativo "(…) no tiene como fin reflejar la teoría sino el marco de referencia cultural del grupo estudiado…" (Bonilla & Rodríguez, 2005, p. 254). Los momentos de desarrollo categorial se describen como ordenamiento, clasificación de material que abundan a lo largo de las sesiones de trabajo, pero que transforman datos en unidades relacionales, de tipo comparativo, y añadidas a categorías más amplias del análisis semiótico "Este método propone un procedimiento de trabajo para el análisis de textos y de representaciones pero, al mismo tiempo, construye un objeto y que da cuenta de la estructura que organiza los sentidos del texto" (Martinic, 2006, pp.301).

2.6.3.8 Puntos de llegada

Este último tiempo es importante para mostrar las conclusiones en el terreno —teórico y práctico— a este punto se llega por medio de la reflexión que debe caracterizar la formulación de conclusiones y dar cuenta de los aprendizajes adquiridos, por ello comunicarlos se convierte en una máxima de vital importancia, porque ello permitirá determinar los alcances y propuestas que se han podido cumplir "(…) las conclusiones teóricas podrían ser formulaciones conceptuales surgidas directamente de lo reflexionado a partir de la experiencia, que deberían relacionarse con las formulaciones teóricas acuñadas por el saber constituido estableciendo un dialogo de mutuo enriquecimiento. También permitirán formular hipótesis que apunten, desde la experiencia, a una posible generalización de mayores alcances teóricos" (Jara, 1994, p. 91). En un segundo momento se buscara lograr material visual y audiovisual capaz de servir de evidencia y muestra para el proyecto, capaz de dar cuenta de las actividades desarrolladas y como muestra de trabajo a mostrar a las instituciones.

Es así que los cinco pasos propuestos, serán la guía para obtener y gestionar las fuentes e implementar instrumentos de trabajo investigativo para la sistematización de la investigación.

- Las Fuentes

La sistematización de la experiencia inicia con los actores primarios, sus testimonios, quienes de forma vivida pueden dar cuenta del proceso desarrollado: el docente que ha orientado el proceso de formación, los estudiantes que han hecho parte activa de la experiencia. Por otro lado en la construcción de documentos con los actores primarios, queda un archivo voluminoso que hace parte de; actas de reuniones, resúmenes, grabaciones magnéticas, videos, entre otras que hayan sido relevantes para el proceso.

- Instrumentos

    a. Archivo –recolección y análisis

"El archivo va a ser uno de los principales dispositivos de la Sistematización, no porque es simplemente un lugar para guardar documentos, sino un sitio donde se construye la secuencia del proceso y queda registrada la forma viva, bajo la cual el proyecto tomo forma en los grupos humanos que lo construyen" (Mejía, 2008, p.44). Es importante generar un archivo que dé cuenta de las experiencias adquiridas, las experiencias compartidas y los momentos de transito que ocurrieron durante la experiencia con el fin de lograr caracteres propios del proceso formativo ciudadano propuesto.

b. Entrevistas no estructuradas

La entrevista no estructurada implica la interacción directa entre el investigador y un encuestado o grupo. Difiere de las entrevistas estructuradas tradicionales en varias formas importantes. En primer lugar, aunque el investigador puede tener algunas preguntas de orientación inicial o conceptos básicos para preguntar, no hay ningún instrumento formal estructurado o protocolo. En segundo lugar, el entrevistador es libre de mover la conversación en cualquier dirección de interés que pueda surgir. En consecuencia, las entrevistas no estructuradas son particularmente útiles para explorar un tema en general. Sin embargo, hay un precio por esta falta de estructura. Debido a que cada entrevista tiende a ser única sin un conjunto predeterminado de preguntas hechas a todos los encuestados, generalmente es más difícil analizar datos de entrevista no estructurados, especialmente cuando se sintetiza entre los encuestados.

c. Grupo Focal

Los datos se recogen a través de un proceso semi-estructurado de entrevista en grupo. Los grupos focales son liderados por un líder del grupo. Los grupos focales se utilizan generalmente para recopilar datos sobre un tema específico. Los métodos de los grupos focales surgieron en los años cuarenta con el trabajo de Merton y Fiske que utilizaron grupos focales para realizar estudios de audiencia., “se trata de ver lo que dicen los sujetos en una situación y grupo particular, lo que alguien dice, la manera en que lo dice” (Mejía, 2008, p.61). Desde ahí la tarea que desarrollaran los grupos focales será el de tener actividades concretas de sistematización dentro de unos comités específicos que se encargan de manejar la memoria que se quiere dejar de las actividades propuestas.

Como producto de trabajo focal se hará una guía de trabajo que permitirá lograr resultados demostrativos de la experiencia y sus especificidades.

d. Diario de Campo

Esta herramienta se da como parte de la experiencia de parte de los actores primarios quienes han hecho resúmenes, fichas, encuestas y memorias de las visitas a los lugares visitados, es por ello que “Este diario va a ser el instrumento fundamental en el cual cada participante del equipo de sistematización va a ir acumulando la reflexión, que le va a permitir leer la unidad del proceso” (Mejía, 2008, p. 16)

A partir de ello, se establecen las fases para adelantar el desarrollo de la problemática planteada.

- Fase de identificación

Se adelantará la identificación de los dispositivos que se encuentran inmersos en el IOT y los cuales son utilizados por las organizaciones para el desarrollo de sus procesos misionales. Estos dispositivos que al estar conectados a la red de internet tiene un alto grado de vulnerabilidad deben de contar con mecanismos de protección que garanticen su disponibilidad y no alterar las actividades y/o servicios dentro de la organización.

- Fase de recopilación

Se hará una caracterización de las vulnerabilidades de los dispositivos que son utilizados por las organizaciones, adelantando una revisión de los requerimientos de seguridad y sus mecanismos de protección existentes.

- Fase de análisis

Se realizará la interpretación de las situaciones a las que se exponen los dispositivos que están enmarcados dentro del IOT, sus deficiencias, limitaciones, y demás aspectos que alteren y pongan en riesgo la información y continuidad del negocio.

- Fase de resultados

Dado que la mayor parte de las amenazas y riesgos a que se exponen los dispositivos del IoT provienen del Internet, deben contener un mínimo de seguridad antes de ser conectados e integrados a los procesos organizacionales, por consiguiente se establecerán las acciones o políticas a tener en cuenta cuando se hace uso de estas herramientas tecnológicas dentro de una organización.

Ahora bien cabe resaltar que los momentos investigativos deben tener una secuencia de acción que permita entender de manera analítica los propósitos y desarrollo de la cuestión investigativa, es por ello que se debe tener en cuenta como sistematizar la información recolectada de manera sintética, para ello se plantearán una serie de preguntas que ayuden a perfilarlas.

Por ello se presentan a consideración una serie de preguntas que permitan perfilar los estudios con el fin de lograr una estructura acorde a las necesidades dentro de las organizaciones y las personas, ¿cuáles son las condiciones en las cuáles se desarrollan las Iot?, ¿cuáles son las condiciones de aplicación para la arquitectura informática en un mundo globalizado?, ¿cómo se logra tener unas condiciones mínimas de se desarrollan los objetos móviles en condiciones de seguridad para la cadena?, ¿por qué adquiere importancia el tema de la internet de las cosas en medio de las condiciones de seguridad, confiabilidad y seguridad qué buscan los

usuarios?, estas preguntas son las orientadoras de la formulación del trabajo de seguridad en la internet de las cosas con el fin de lograr el éxito de los indicadores propuestos en los objetivos formulados.

3. IDENTIFICACIÓN DE LOS ELEMENTOS QUE COMPONE INTERNET DE LAS COSAS (IoT) Y LAS VULNERABILIDADES QUE PRESENTAN LOS RECURSOS TECNOLÓGICOS

3.1 INTRODUCCIÓN

La internet de las cosas plantea los elementos que deben hacer parte de una arquitectura de software acorde a la seguridad informática y a las aplicaciones móviles desde una perspectiva del entorno en el cual las amenazas de seguridad se vean disminuidas o anuladas con el propósito de mejorar la confiabilidad de los artefactos creados con el fin de mejorar actividades desarrolladas por los seres humanos en doble vía con máquinas inteligentes.

Desde esa primera perspectiva esta monografía busca establecer parámetros de acción que tengan relación con las IoT capaces de ser fiables, confiables y capaces de soportar embates de amenazas de seguridad en condiciones de equilibrio y tranquilidad para los usuarios.

Por otro lado se busca dentro del manual de procedimientos lograr una manera de llegar a las IoT y que sean de crecimiento progresivo en un país como Colombia donde se evidencia su aplicabilidad y que busca posicionarse como parte de la cotidianidad de los sujetos, unos sujetos que requieren alfabetizarse en términos de seguridad informática, que quieren tener confiabilidad y desde ahí asegurar que su privacidad no se verá amenazada por personas o virus maliciosos que buscan información de manera ilegal.

Por último y no menos importante dentro de los contextos que se quieren analizar es de resaltar el manejo que se le está dando al tema a nivel global, donde cada día adquiere una mayor relevancia, y en el caso colombiano como lograr que la presencia de IoT crezca en proporción a la demanda cautiva, es por ello que dentro de la manual de procedimientos que se quiere lograr habrá un capítulo especial para la implementación en organizaciones colombianas y sus logros en la materia.

Internet de las cosas, para muchas personas este concepto puede resultar un poco extraño incluso no tener sentido, mientras que para otros es un término que utiliza a diario, pero en realidad ¿qué es el internet de las cosas y que elementos lo componen? para explicar este concepto lo dividiremos en dos partes, el internet y las cosas. Según la Ilustración 4 se enmarca el concepto del IoT.

Ilustración 4. Conectividad en el mundo IoT

Fuente: 6 tipos de sensores para aplicación en la internet de las cosas. [En línea]. 2017. [Consultado el 31 de octubre de 2017]. Disponible en internet: http://blogmexico.comstor.com/6-tipos-de-sensores-para-aplicacion-en-la-internet-de-las-cosas

3.2 EL INTERNET

La definición de Internet[66] se estructura de las palabras en inglés Interconnected Networks, que indica “redes interconectadas”, es decir, que se entrelazan todas las redes y sistemas informáticos que están distribuidos por todo el mundo, haciendo uso de protocolos compatibles entre sí. La red de redes como es conocida, integra diversos tipos de recursos tecnológicos independiente de sus connotaciones físicas, integrados en todos los entornos de la sociedad, mediante ellas se deja a disposición de millones de usuarios recursos valiosos como lo es la información.

Este medio de comunicación surge como resultado de un experimento que llevo a cabo el Departamento de Defensa de Estados Unidos en el año 1969, que dio como resultado la construcción de la red ARPAnet, que permitía enlazar instituciones universitarias y centro de tecnología para transmitir datos científicos y militares, posteriormente se adhieren nodos de varias partes del mundo formando la Word Wide Web.

[66] Venemedia. ¿Qué es internet?. [En línea]. 2014. [Consultado 19 de octubre de 2017]. Disponible en internet: http://conceptodefinicion.de/internet/.

Internet, nuestra ya conocida red de redes, la cual nos permite estar interconectados por medio de nuestros equipos de cómputo, permitiéndonos acceder a recursos, servicios y páginas web, desde nuestro hogar o en cualquier parte del mundo.

3.3 LAS COSAS

Hace referencia a todos los objetos físicos que se encuentran en nuestra vida diaria, por ejemplo el televisor, un automóvil, el reloj, nuestra cobija, un cepillo de dientes, la lavadora, en fin cualquier cosa, solo que estos objetos tienen algo que los diferencia de los demás, la gran peculiaridad es que tienen Sensores, Circuitos integrados, Conectividad que les permite recolectar y compartir datos ya sea entre ellos o a raves de internet, a estos objetos los conocemos como nodos IoT o dispositivos inteligentes, es de suma importancia entender que son inteligentes no por su conexión a internet, sino porque son capases de cumplir una o múltiples funciones estas se pueden enumerar de la siguiente manera:

3.3.1 Monitoreo

Se podría decir que esta es la más importante de todas, debido que a partir de la integración de diversos sensores, podrá reconocer todo lo que ocurre alrededor del dispositivo inteligente, como ejemplo pueden medir la velocidad, temperatura, luminosidad, altitud, movimiento entre muchos de los elementos que puedan ocurrir a su alrededor.

3.3.2 Control

Con base a los datos recogidos con el monitoreo estas tomaran una acción, la cual será capaz de decidir si deben abrir o cerrar otro objeto, encender o apagar algún dispositivo, emitir una alarma todo esto preestablecido para una finalidad.

3.3.3 Optimización

Con el análisis de la información recolectada, será capaz de utilizar los recursos estrictamente cuando sea necesario y requerido

3.3.4 Automatización

Se trata de facilitar y poder programar cualquier tipo de actividad, considerada como rutinaria

De todo lo anterior. Podemos analizar que el internet de las cosas, son los objetos que nos rodean día a día, que mediante circuitos integrados y censores, podrán recolectar información, la cual podrá ser intercambiada entre los propios dispositivos

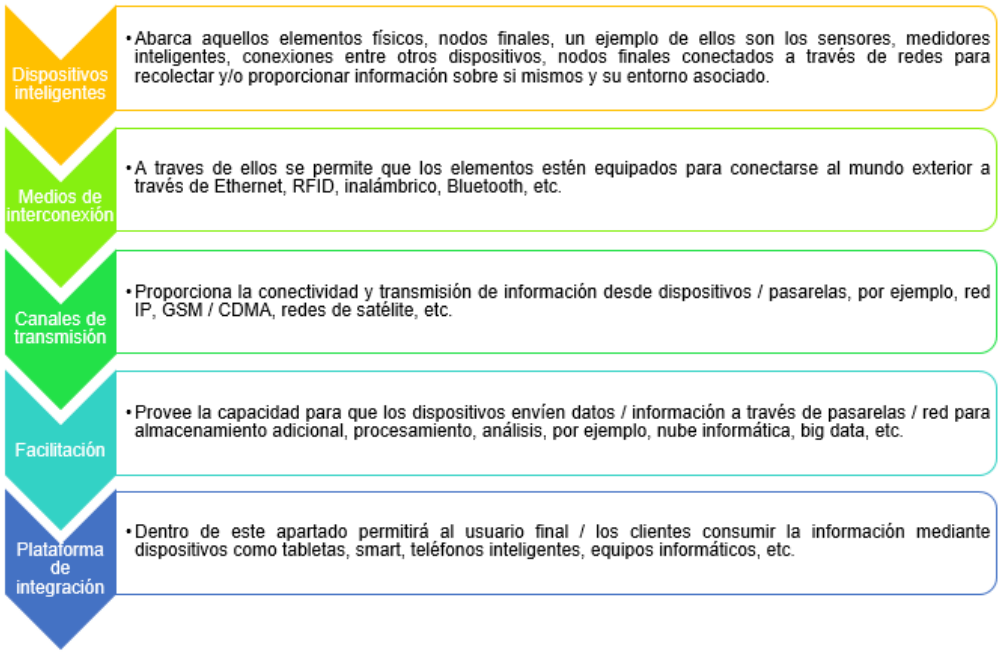
inteligente o con algún servidor en internet, en el cual se analizaran los datos para posteriormente optimizar los recursos como ejemplo veremos varias cosas que pasaron del común a engrosar el mundo del internet de las cosas

3.4 ELEMENTOS QUE INTEGRAN IOT

Existe diversidad de conceptos relacionados con IoT lo cual hace que su interpretación sea algo compleja y dispendiosa, ante ello se pretende dar claridad frente a lo que realmente hace parte de esta nueva revolución tecnológica, en este sentido se desglosan en varios componentes como se aprecia en la ilustración 5, se debe tener en cuenta que estos deben ser integrados con el fundamento de lograr ambientes y entornos seguros.

- Dispositivos inteligentes
- Medios de interconexión
- Canales de transmisión
- Facilitación
- Plataforma

Ilustración 5. Componentes que integran IoT



Fuente: Los autores

3.4.1 Dispositivos inteligentes

Dentro de este grupo se encierran los elementos inteligentes que permiten el ensamblaje básico de IoT.

3.4.1.1 Sensores

Los sensores son las manos ojos nariz y boca de IoT, estos soldados incansables son la tropa que utilizan las cosas, para llevar a cabo el crítico trabajo de monitorear medir y recolectar datos, en ocasiones este es el primer elemento en el que pensamos cuando nos nombran IoT. Frente a este elemento se encuentran diversos tipos como se visualiza en la Ilustración 6.

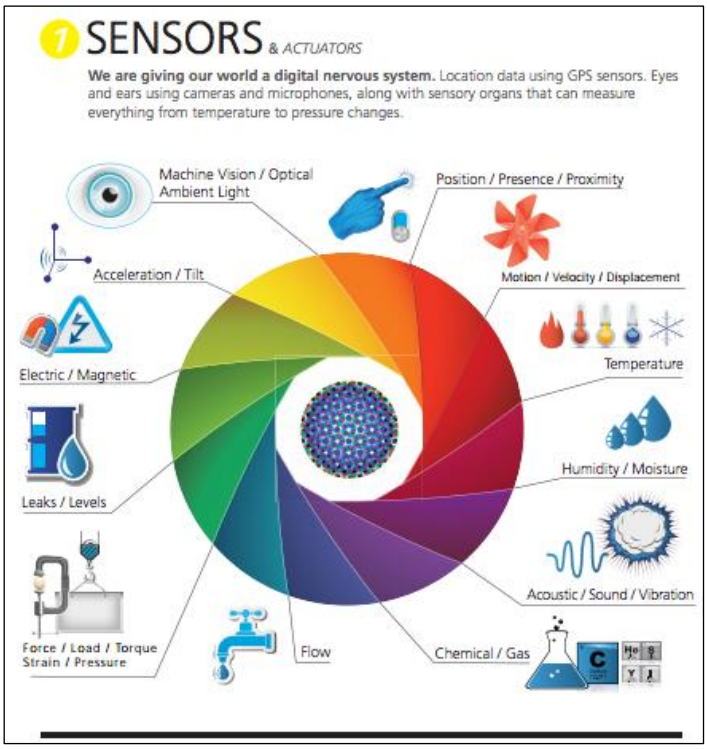
Ilustración 6. Tipos de sensores

Fuente: Pits Team. ¿Qué es un Sensor?. [En línea]. 2015. [Consultado el 31 de octubre de 2017]. Disponible en internet: http://pitsteam.com/site/que-es-un-sensor/

Esos elementos se utilizan comúnmente para responder señales tanto eléctricas ópticas y sonoras, convirtiendo todos los parámetros físicos como (temperatura, movimiento, presión sanguínea, velocidad, luminosidad), como ejemplo tomemos un sensor de calor, el termómetro convierte la temperatura en medidas, posteriormente el espectáculo de vidrio calibrado leerá esos datos.

Lista de los diferentes tipos de sensor. (Ver Ilustración 7).

Ilustración 7. Lista de sensores



Fuente: IoT.eu. Sensors (Infographic). [En línea]. 2015. [Consultado el 27 de octubre de 2017]. Disponible en internet: https://iot.eu.com/sensors-infographic/

Sensores de proximidad

Permite la detección de movimientos y son muy usados para procesos que requieren configuraciones al detalle, a través de estos elementos y aprovechando la proximidad con determinado cliente, se pueden enviar u ofrecer servicios directamente al dispositivo móvil. Sus características también les permite realizar monitoreo sobre determinadas condiciones, por ejemplo establecer disponibilidad de espacios para parqueo sobre sitios de tamaño considerado como centros comerciales, aeropuertos y estadios.

Acelerómetro y giroscópico

Este elemento tiene las funciones para detectar vibraciones, inclinación y aceleración lineal, es muy utilizado dentro de los podómetros que permiten medir el número de pasos que da una persona o medir distancias recorridas. Así mismo tiene aplicabilidad como instrumento para determinar velocidades angulares y se incorpora dentro de dispositivos como el mouse, en juegos y dentro de los procesos de entrenamiento de atletas profesionales.

Sensores de temperatura

Tienen aplicabilidad en casi todos los ambientes IoT, en diversas áreas hacen parte del proceso para analizar entornos y medir temperaturas sobre recursos y elementos para prever situaciones anómalas y establecer comportamientos del suelo, agua y plantas para expandir la producción.

Sensor de humedad

Tiene funciones semejantes al sensor de temperatura, es utilizado para determinar y controlar el desempeño de los dispositivos. Puede tener connotaciones de analógico y digital, frente al primero aplica procedimiento para establecer la humedad relativa del aire haciendo uso de un sistema capacitivo. La estructura de este elemento se encuentra recubierto por vidrio o cerámica, el compuesto aislante que absorbe el agua está elaborado mediante la utilización de un polímero que recibe y suelta el agua a través de la humedad relativa.

Respecto a la parte digital, este hace uso de micro-sensores debidamente calibrados de acuerdo a la humedad que se presente en determinada área, allí mediante un proceso se realiza la conversión de analógico a digital haciendo uso de un chip ubicado dentro del mismo circuito. La capacidad del sensor depende de una máquina que cuenta con un sistema de electrodos elaborados por un polímero, protegiendo al sensor del visor. También se cuentan con sensores de humedad de suelo muy utilizados en ambientes agrícolas durante el todo el proceso plantación y colecta.

Sensor de presión

Tiene funcionalidades dentro de los ambientes agrícolas e industriales, en primera instancia para determinar el flujo de agua que se utiliza o requiere en determinada plantación con lo cual se podrán establecer acciones correctivas, frente a los procesos industriales tiene gran accionar en el área automotriz y aeronáutica para medir fuerza y altitud.

Sensores de nivel

Permiten detectar el nivel sobre determinado fluidos, tiene diversas aplicabilidades, por ejemplo son muy utilizados en las áreas de manejo de residuos y reciclaje, en control de medición de carburantes y procesos agrícolas.

Lo enunciado son los usos más comunes que tienen los sensores dentro del entorno IoT, sin embargo existen otros inmersos en los medios de transporte autónomos los cuales poseen la tecnología de los sensores, allí se encuentran sensores para medir fuerza, tensión, torsión, carga, sensores de movimiento, velocidad, desplazamiento,

posición, vibración y choque. Existe un amplio campo de datos que pueden ser sujeto de análisis por parte de los sensores.[67]

Características de los sensores[68]

- Rango de medida: dominio en la magnitud medida en el que puede aplicarse el sensor.

- Precisión: es el error de medida máximo esperado.

- Offset o desviación de cero: valor de la variable de salida cuando la variable de entrada es nula. Si el rango de medida no llega a valores nulos de la variable de entrada, habitualmente se establece otro punto de referencia para definir el offset.

- Linealidad o correlación lineal.

- Sensibilidad de un sensor: suponiendo que es de entrada a salida y la variación de la magnitud de entrada.

- Resolución: mínima variación de la magnitud de entrada que puede detectarse a la salida.

- Rapidez de respuesta: puede ser un tiempo fijo o depender de cuánto varíe la magnitud a medir. Depende de la capacidad del sistema para seguir las variaciones de la magnitud de entrada.

- Derivas: son otras magnitudes, aparte de la medida como magnitud de entrada, que influyen en la variable de salida. Por ejemplo, pueden ser condiciones ambientales, como la humedad, la temperatura u otras como el envejecimiento (oxidación, desgaste, etc.) del sensor.

- Repetitividad: error esperado al repetir varias veces la misma medida.

3.4.1.2 Placa de desarrollo

- HW Arduino[69]

---

[67] CanalComstor. 6 tipos de sensores para aplicación en la internet de las cosas. [En línea]. 2017. [Consultado 01 de noviembre de 2017]. Disponible en internet: http://blogmexico.comstor.com/6-tipos-de-sensores-para-aplicacion-en-la-internet-de-las-cosas

[68] Fundación Wikimedia. Sensor.[En línea]. 2017. [Consultado 28 de noviembre de 2017]. Disponible en internet: http://es.wikipedia.org/wiki/Sensor#Caracter.C3.ADsticas_de_un_sensor

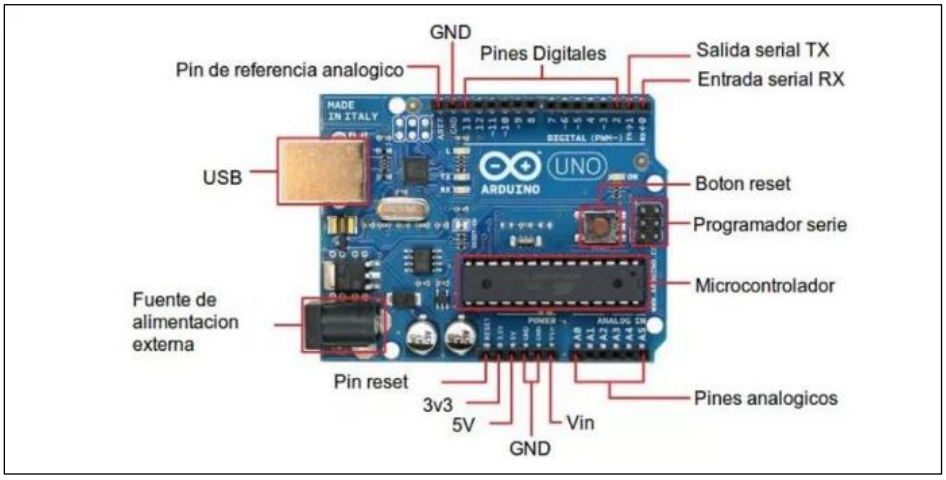
[69] Jecrespom. Que es arduino. [En línea]. [Consultado 21 de octubre de 2017]. Disponible en internet: https://aprendiendoarduino.wordpress.com/2016/09/25/que-es-arduino/

Esta pieza es básicamente una placa que integra un microcontrolador, y es capaz de ejecutar instrucciones que almacena en su memoria, su estructura se basa en bloques funcionales que llevan a cabo tareas específicas tal y como se observa en la ilustración 8.

Características de Arduino para IoT

- Barato y rápido prototipado.
- HW libre y por lo tanto es modificable para que consuma menos y para hacer un HW final de características industriales.
- Disponibilidad de HW de comunicaciones de todo tipo para conectar con Arduino. Nuevas tecnologías de comunicación llegan antes que para elementos comerciales
- Librerías y SW público para su reutilización o adaptación.
- Flexibilidad en la programación.
- Apoyo de la comunidad.

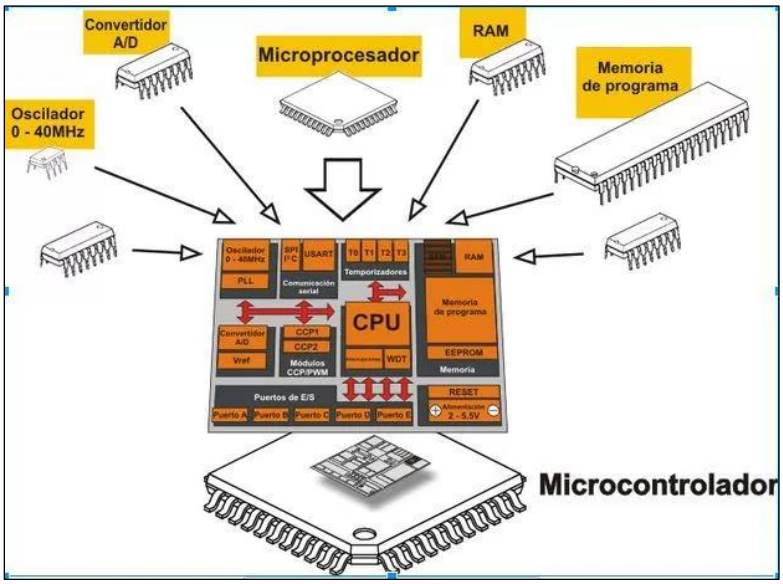
Ilustración 8. Arduino



Fuente: PE, Isaac. Análisis comparativo de las placas Arduino (oficiales y compatibles). [En línea]. 2014. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://comohacer.eu/analisis-comparativo-placas-arduino-oficiales-compatibles/

El microcontrolador integra las tres unidades principales que contienen un sistema informático, la unidad central de procesamiento, la memoria y los periféricos de entrada y salida. (Ver Ilustración 9).

Ilustración 9. Microcontrolador



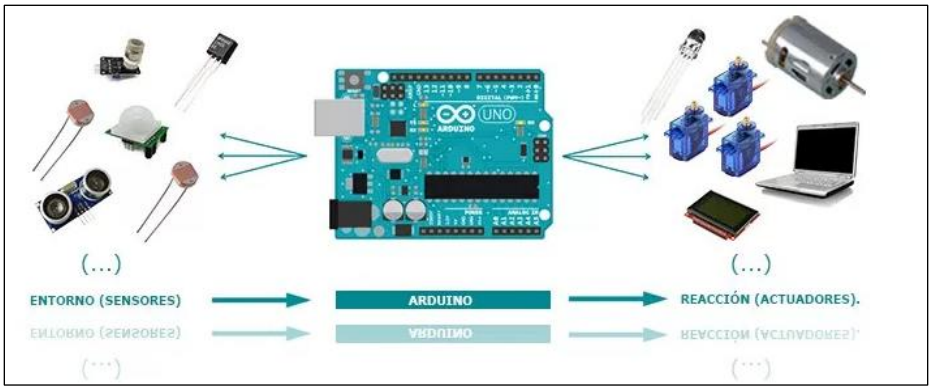
Fuente: CRESPO, José Enrique. Aprendiendo Arduino. [En línea]. 2016. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://aprendiendoarduino.wordpress.com/2016/09/25/que-es-arduino/

Características del Microcontrolador

- Velocidad del reloj u oscilador
- Tamaño de palabra
- Memoria: SRAM, Flash, EEPROM, ROM, etc.
- I/O Digitales
- Entradas Analógicas
- Salidas analógicas (PWM)
- DAC (Digital to Analog Converter)
- ADC (Analog to Digital Converter)
- Buses
- UART
- Otras comunicaciones.

Básicamente un Arduino es utilizado para crear elementos autónomos, pudiendo conectarse e interactuar tanto con elementos de software y hardware, un ejemplo claro del diseño se observa en la Ilustración 10.

Ilustración 10. Diseño básico IoT



Fuente: CRESPO, José Enrique. Aprendiendo Arduino. [En línea]. 2016. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://aprendiendoarduino.wordpress.com/2016/03/28/que-es-arduino-hw-libre/

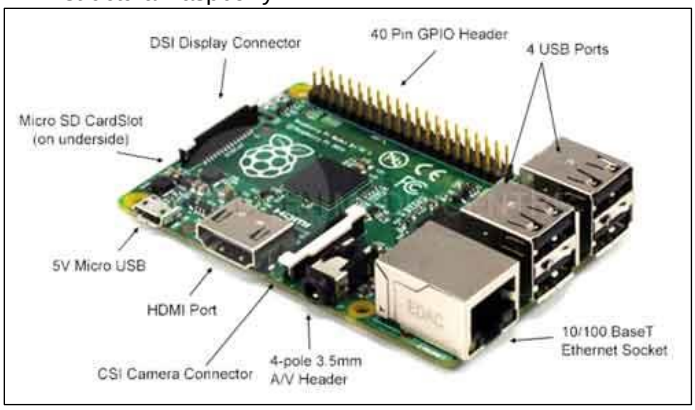
En otras palabras, esta placa permitirá controlar las cosas, por ejemplo, digamos que queremos autorizar la persiana existente en la bodega, el sensor ubicado en la puerta contara el total de personas que entra, asumiendo eso el sensor del bombillo encenderá la luz y mediante un código de acceso por voz la persiana se abrirá, generando una alarma que se le enviara al personal de seguridad, inmediatamente se pondrá en pantalla la imagen de las personas que están dentro, otro sensor ubicado en el estante podrá controlar que objeto fue retirado, todo esto se enviara a la base de datos para ser analizado, como ese ejemplo son muchos los casos que se pueden crear, resumido Arduino = HW + SW + Control

- Raspberry Pi

Esta placa es un mini ordenador de pequeño tamaño, está compuesta por un procesador, un chip gráfico y memoria RAM, además, dispone de puertos USB, puerto LAN, salida de audio para Jack de 3.5 mm, puerto para cámara, HDMI, ranura para micro SD y pines de conexión de entradas y salidas digitales para sensores o actuadores, (Ver ilustración 11). Fue lanzada al mercado en el año 2006 por la fundación Raspberry Pi con la finalidad de promover la enseñanza de informática en las escuelas. Esta placa permite la conexión de periféricos de ordenadores como pantalla, teclado, mouse, impresoras, etc.

Básicamente, Raspberry Pi es un ordenador en miniatura al que se le pueden conectar los mismos periféricos que a cualquier otro ordenador, tales como pantalla, teclado, ratón, pen drive, impresora, altavoces, etc.

Ilustración 11. Estructura Raspberry Pi



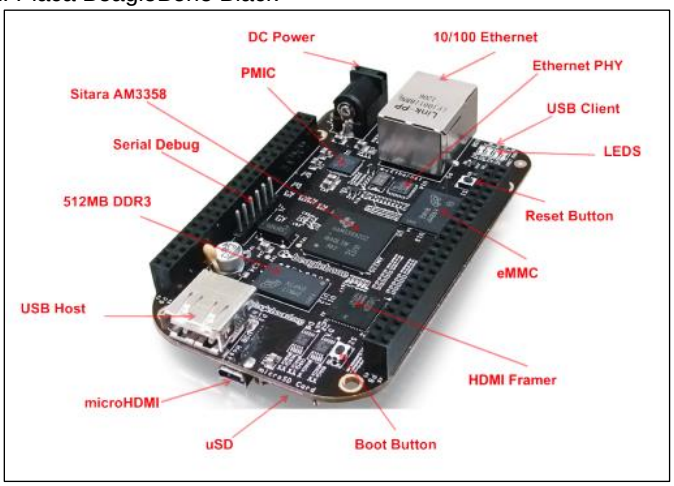
Fuente: LLAMAS, Luis. ¿Qué es Raspberry Pi?. [En línea]. 2017. [Consultado el 31 de octubre de 2017]. Disponible en línea: https://www.luisllamas.es/que-es-raspberry-pi/

- BeagleBone Black

Dispone de las funciones de una computadora básica, con mejores características que la placa Raspberry Pi frente a sus capacidades de procesamiento, periféricos y GPIOs, presenta una desventaja en cuanto a que la placa BeagleBone Black solo cuenta con un puerto USB host, por tanto será necesario la utilización de un Hub USB activo.

La placa cuenta con un procesador de 1 GHz, 512 MB de memoria (DDR3 RAM), almacenamiento de 2 GB con un sistema Linux preinstalado (no se requiere de una tarjeta SD) y más aún, con un conector MicroHDMI para entrada y salida de video y audio, como se observa en la Ilustración 12.

Ilustración 12. Placa BeagleBone Black

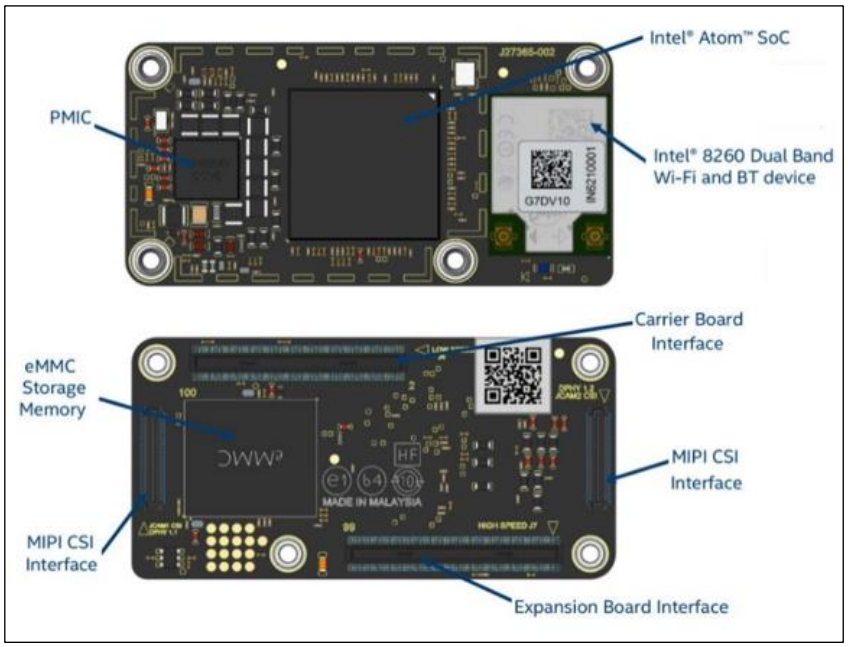


Fuente: Electron Components. BeagleBone Black. [En línea]. SF. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://www.electroncomponents.com/Beagle-Bone-Black-Linux-Original

- Joule

La placa Joule desarrollada por la compañía Intel, cuenta con una cámara sofisticada para la captura y visualización de video a 4K, dispone una alta capacidad de almacenamiento y memoria, así como de interfaces físicas de alta velocidad, incorpora un chip de bajo consumo de reducido tamaño y la habitual placa donde se incorporan los conectores y sensores, incorpora un procesador de cuatro núcleos con arquitectura de 64 bits. Este módulo es utilizado para soluciones IoT, robóticas, realidad virtual y aumentada, micro-servidores y aplicaciones que requieran computación de punta, tal y como se observa en la ilustración 13.

Ilustración 13. Placa Intel Joule

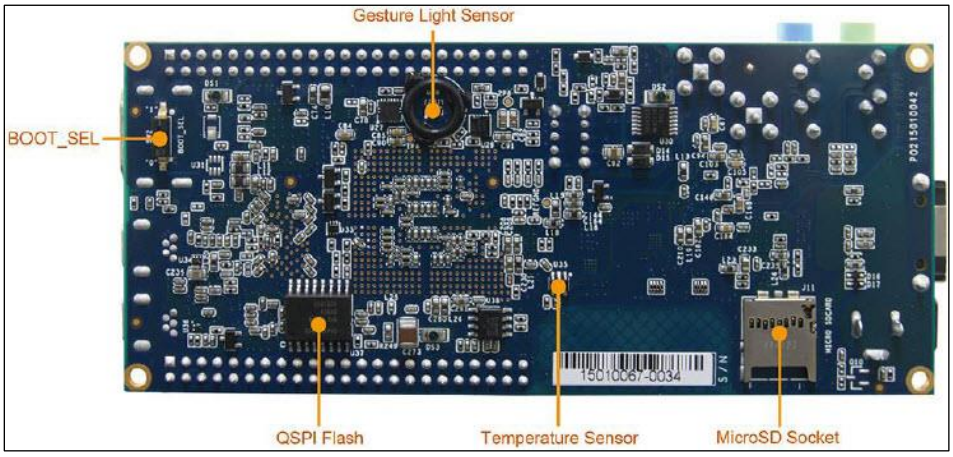


Fuente: WONG, William. A Jewel of a Joule. [En línea]. 2016. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://www.electronicdesign.com/iot/jewel-joule

- Placa DECA

Incorpora varios tipos de tecnologías, diversos protocolos de comunicación y sensores, con ello permite agilizar las pruebas para las aplicaciones IoT, es uno de los primeros chip de la industria, con connotaciones de dispositivo lógico programables no volátiles (PLD) el cual permite integrar un conjunto óptimo de componentes del sistema. (Ver Ilustración 14).

Ilustración 14. Placa Deca



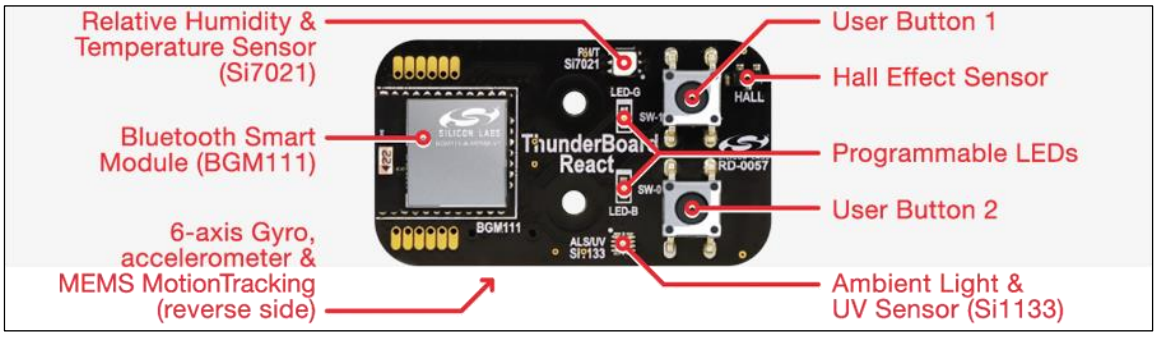
Fuente: ARROW. DECA Diseño de referencia. [En Línea]. SF. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://www.arrow.com/es-mx/reference-designs/deca-development-kit-based-on-the-10m50daf484c6ges-max-10-fpga/178fffd04d89cbb578855555cb159a1a

Adiciona a ello, cuenta con un sensor de temperatura y un sensor de humedad, incorpora otros circuitos integrados lógicos, de audio y de cadena de señales de TI, esta placa de evaluación de hardware permite a los ingenieros reducir el coste y la complejidad, a la vez que interactúa con una multitud de sensores e interfaces.

- Thunderboard React

La placa Thunderboard React ofrece una solución habilitada para Bluetooth Smart y conectada a la nube que le permitirá recopilar datos de sensores a fin de hacer pruebas fácilmente y crear prototipos de aplicaciones de IoT, para mejor claridad se puede observar la ilustración 15.

Ilustración 15. Placa Thunderboard React



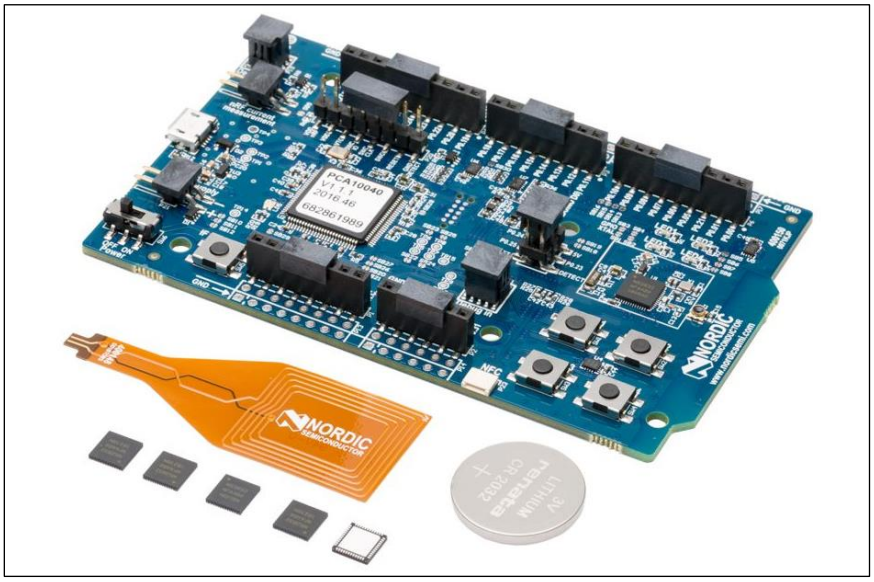
Fuente: WONG, William. A Jewel of a Joule. [En línea]. 2016. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://www.electronicdesign.com/iot/thunderboard-react-races-stem

Como un plus incorpora una aplicación móvil gratuita la cual una vez recopila los datos permite la visualización y control de los led del hardware.

- NRF52-DK

Su diseño proporciona acceso a todas las E/S e interfaces mediante conectores y tiene 4 LED y 4 botones programables por el usuario, esta placa es compatible con la Arduino Uno R3, con lo cual dada su estructura puede usar todos los escudos para Arduino de terceros que sean compatibles. Esta placa está diseñada para conexiones Bluetooth Smart, ANT y aplicaciones inalámbricas de 2,4 GHz, adicional cuenta con un conector para mediciones de RF y una antena NFC enchufable para activar la funcionalidad de etiquetas NFC, esto se puede observar en la ilustración 16.

Ilustración 16. Placa NRF52-DK

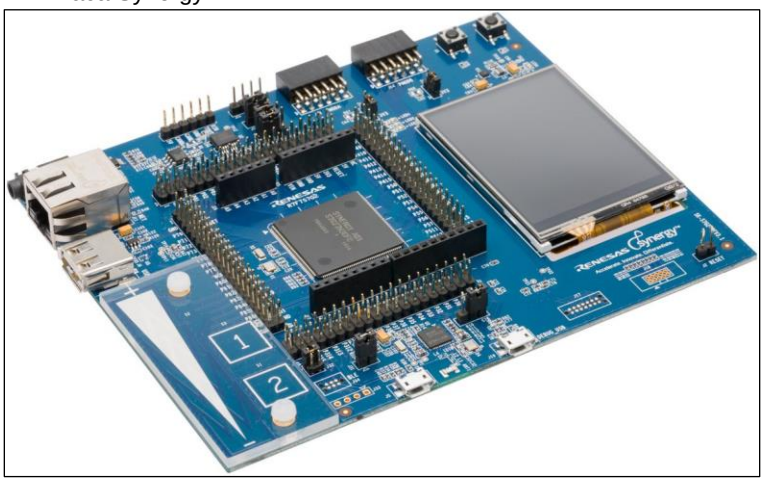


Fuente: ARROW. DECA Diseño de referencia. [En Línea]. SF. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://www.arrow.com/es-mx/products/nrf52-dk/nordic-semiconductor

- Synergy

Proporciona una conectividad segura a través de Ethernet, USB, CAN, y una conectividad inalámbrica a dispositivos de Internet móvil mediante BLE 4.1, dada su estructura puede ser ejercida y adaptada a las necesidades del proceso. Sus características la hacen compatible con arduino uno, las clavijas del conector para todas las interfaces y dispositivos de E/S están disponibles en la placa de desarrollo. (Ver ilustración 17).

Ilustración 17. Placa Synergy



Fuente: ARROW. DECA Diseño de referencia. [En Línea]. SF. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://www.arrow.com/es-mx/products/yssks7g2e30/renesas-electronics

- FONA

Esta placa básicamente es un teléfono celular en un escudo arduino, dentro de su núcleo se encuentra un módulo celular SIM GSM permite la conexión a cualquier red de este tipo a través de SIM 2G, con lo cual permitirá realizar y recibir llamadas de voz, datos entre otros, adicional posee de un motor vibrador dado el caso que se requiera insonorizar, lo cual se puede observar en la ilustración 18.

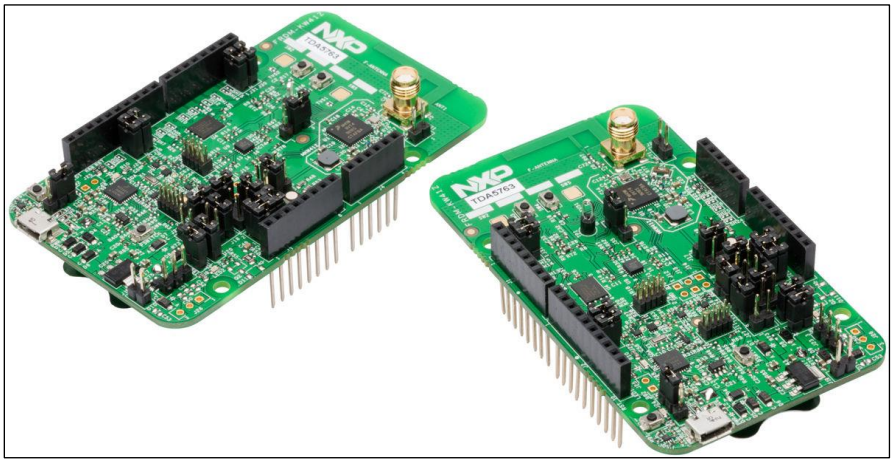
Ilustración 18. Placa Synergy

Fuente: HERNÁNDEZ, María Carlina. Connect the Adafruit FONA to Ubidots. [En línea]. SF. [Consultado el 23 de marzo de 2018]. Disponible en internet: https://ubidots.com/docs/devices/FONA.html#adafruit-fona-minigsm

- Placa de libertad

Esta tecnología pueden admitir múltiples protocolos que se ejecutan de forma simultánea, cuenta con un programador flash en modo de dispositivo de almacenamiento masivo fácil de usar, puerto serial virtual, programación estándar y capacidades de control de ejecución. Integra un chip que habilita consumo bajo de energía cuando se establecen conexiones a través de Bluetooth, para mayor interpretación se puede observar en la ilustración 19.

Ilustración 19. Placa de libertad



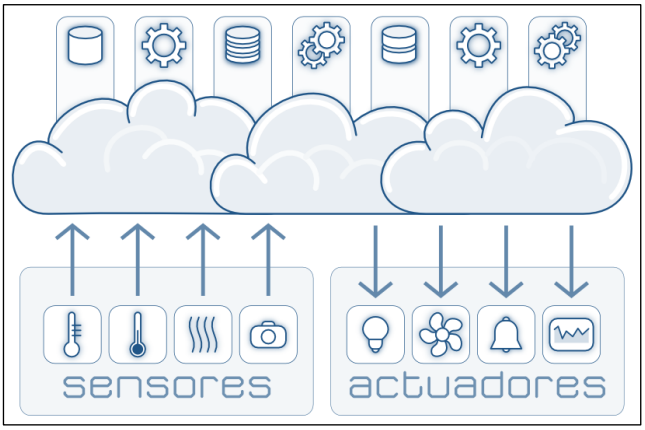
Fuente: ARROW. DECA Diseño de referencia. [En Línea]. SF. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://www.arrow.com/es-mx/products/frdm-kw41z/nxp-semiconductors

3.4.1.3 Actuadores

Estos elementos actúan en respuesta a las lecturas de los sensores para ejecutar alguna acción o a las programaciones estipuladas, tienen la función de convertir una señal eléctrica en una cantidad física correspondiente, que se refleja en movimiento, fuerza, sonido, etc. Los actuadores se pueden clasificar como dispositivos binarios o continuos en función de la cantidad de estados estables que tiene su salida.

Los actuadores no tienen la capacidad de procesar datos, por el contrario el resultado de su accionar se basa en una señal recibida. La distinción entre los sensores y actuadores es que un sensor transforma una acción, energía útil en datos eléctricos. Por el contrario, un actuador transforma los datos eléctricos en una acción, energía útil. (Ver ilustración 20).

Ilustración 20. Función de actuadores



Fuente: VENTURA, Víctor, Qué es la Internet de las Cosas (IoT). [En línea]. 2017. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://polaridad.es/que-es-internet-de-las-cosas-iot/

Dentro de las soluciones relacionadas con IoT se encuentran diversos tipos de actuadores, entre los más comunes se encuentran.[70]

- Servomotores

Este dispositivo incorpora un motor de corriente continua de dos cables, un tren de engranajes, un potenciómetro, un circuito integrado y un eje (espina de salida).

- Motores de paso a paso

Este tipo de dispositivo está compuesto por múltiples bobinas que se organizan en grupos denominados “fases”. Una vez estas fases son energizadas de forma secuencial el motor rotara un paso a vez dado que su estructura de movimientos es por pasos discretos.

- Motores de corriente continua

Es uno de los actuadores de mayor uso dentro de los entornos electrónicos dado su bajo costo, facilidad de uso y adaptación a diversas tareas.

- Actuador lineal

Tiene la función de crear movimientos en línea recta, en contraste con el movimiento circular de un motor eléctrico convencional. Su aplicabilidad ligada a maquinas industriales, dispositivos periféricos, válvulas, amortiguadores, etc.

[70] Yash. basic-iot-actuators. [En línea]. 2017. [Consultado el 07 de marzo de 2018]. Disponible en internet: https://iotbytes.wordpress.com/basic-iot-actuators/

- Relé

Este interruptor opera bajo acción eléctrica, hace uso de una cantidad relativamente pequeña de energía para operar. Esta herramienta en si puede ser utilizada para controlar motores, calefactores, lámparas o circuitos de CA que pueden generar mucha más energía eléctrica.

- Solenoide

Su aplicabilidad se limita principalmente a aplicaciones de encendido y apagado, como enclavamiento, bloqueo y disparo. Se utilizan con frecuencia en electrodomésticos, equipos de oficina, automóviles, máquinas de pinball y automatización de fábrica.

3.4.2 Medios de interconexión

Un dispositivo de puerta de enlace del IoT opera como puente de comunicación entre la nube y los sistemas periféricos, como los dispositivos, sensores, equipos y sistemas del IoT. Así mismo incorpora funciones de traducción de protocolos, procesamiento, almacenamiento, filtrado de datos, seguridad de dispositivos y tiene la capacidad de controlar de forma autónoma los dispositivos de campo, basado en la entrada de datos de los sensores. Si se imagina un ecosistema IoT, una puerta de enlace se encuentra entre los sensores y los dispositivos para hacer posible la comunicación con la nube.[71]

3.4.2.1 Gateway

Permite administrar las conexiones de los dispositivos activos e implementa una semántica para varios protocolos con el objetivo de garantizar que los dispositivos puedan comunicarse de manera segura y eficiente. Actualmente, la Gateway para dispositivos admite los protocolos MQTT, WebSockets, HTTP, AMQP, JMS y OPC.

Estos protocolos diseñados para interacciones IoT son de tipo abierto y permite una conexión rápida de maquina a máquina, allí se mantendrá conexiones de tipo bidireccionales de vida prolongada, permitiendo así que los dispositivos envíen y reciban mensajes en cualquier momento y con una baja latencia. La Gateway para los dispositivos está completamente administrada y se ajusta a escala de forma automática con el fin de admitir más de mil millones de dispositivos sin la necesidad de tener que administrar infraestructuras.

[71] Premier Farnell Limited. Puerta de enlace. [En línea]. 2018. [Consultado el 06 de Marzo de 2018]. Disponible en internet: http://es.farnell.com/internet-of-things-gateway

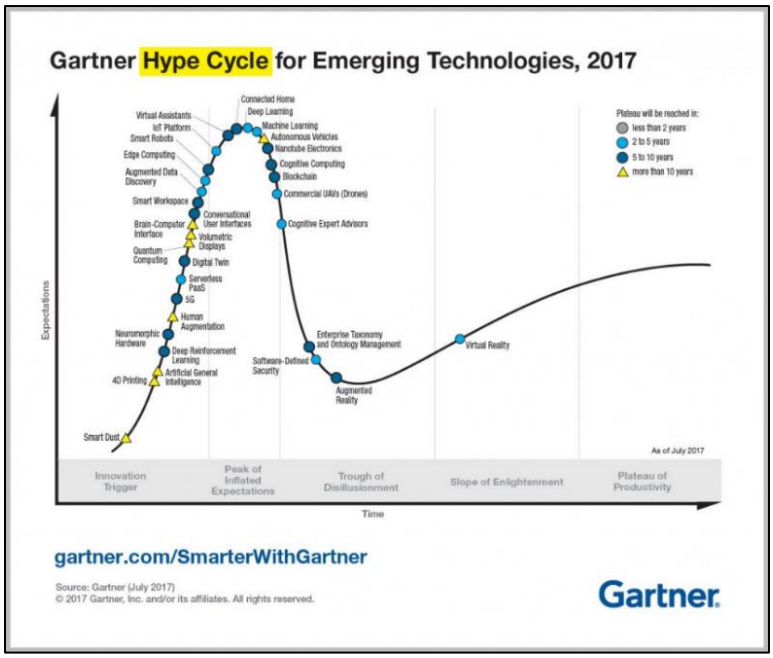
3.4.2.2 Hub

Este dispositivo realiza funciones de puerta de enlace entre los objetos del IoT y el servicio de nube, adicional tiene las características de reducir los inconvenientes de interoperabilidad entre cada objeto conectado.

3.4.3 Canales de transmisión

A pesar que desde hace muchos años surgió el concepto de las cosas de internet, hasta hace poco se lograron verdaderos avances, y los usuarios siguen descifrando como incluir sus dispositivos a la vida cotidiana, todo esto se ha logrado en parte a la conectividad y es que según Gartner[72], se tendrá un consumo en más de 26 mil millones de dispositivos conectados a la Internet de las Cosas antes de 2020, con la finalidad de optimizar procesos en diversos entornos, permitiendo así una mayor disponibilidad y aprovechamiento de tiempo en otros aspectos de la vida, familias, pasatiempos y trabajos. De acuerdo a la Ilustración 21 se especifica el ciclo Gartner Hype.

Ilustración 21. Ciclo Gartner Hype



Fuente: PANETTA, Kasey. Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017. [En línea]. 2017. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

[72] Gartner. Principales tendencias en el ciclo Gartner Hype para tecnologías emergentes. [En línea]. 2017. [Consultado 20 de agosto de 2017]. Disponible enhttps://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Por otra parte y según lo expuesto por Jessica Epley[73], especialista en Desarrollo de Contenido de CommScope, esto no puede ser logrado si la infraestructura de red que soporta todos estos dispositivos no es la adecuada. En los últimos años la necesidad de mayor conexión y el avance tecnológico han presentado grandes desafíos para las infraestructuras de red.

El reto para los operadores es garantizar que las redes sean convergentes, para que los dispositivos IoT puedan funcionar con rapidez y eficacia. La transferencia de todos los datos depende de las redes y, lo que es más importante, de la calidad de dichas redes. A medida que los dispositivos IoT se vuelven más valiosos para acceder a la información, también aumenta el valor de una red de calidad".

Todo esto se vive gracias a la gran dependencia, generada en los consumidores en cualquier parte ya a cualquier hora, según cisco la convergencia de las redes y la seguridad toda en esas entrada un papel primordial en su funcionalidad accesibilidad y uso, se estima que para el añ0 2020 la transición de datos generado por IoT alcanzara un aproximado de 600 zettabits al año, si analizamos las cifras actuales esto sería 275 veces más que los generados actualmente, por consiguiente y en definitiva la red tendrá un papel fundamental para cumplir tan magna misión, a continuación se muestra un listado de las principales redes inalámbricas fundamentales para el correcto funcionamiento de IoT.

Actualmente contamos con redes establecidas, que a lo largo de los años han comprobado su funcionabilidad tecnologías de transmisión inalámbrica de datos, como por ejemplo Wi-Fi, Bluetooth, ZigBee, 2G/3G/4G, etc. A todo esto, se le deben sumar las tecnologías emergentes como Thread, una alternativa en el campo de la domótica, o tecnologías que utilizan la "banda blanca" liberada por la televisión digital terrestre para implementar soluciones de acceso IoT en áreas extensas.

Dependiendo de la aplicación, los factores como el alcance, velocidad de transferencia, seguridad, potencia y autonomía dictarán cuál es la mejor alternativa a la hora de elegir una red inalámbrica u otra. Estas son algunas de las principales tecnologías de comunicación que pueden elegir los desarrolladores:

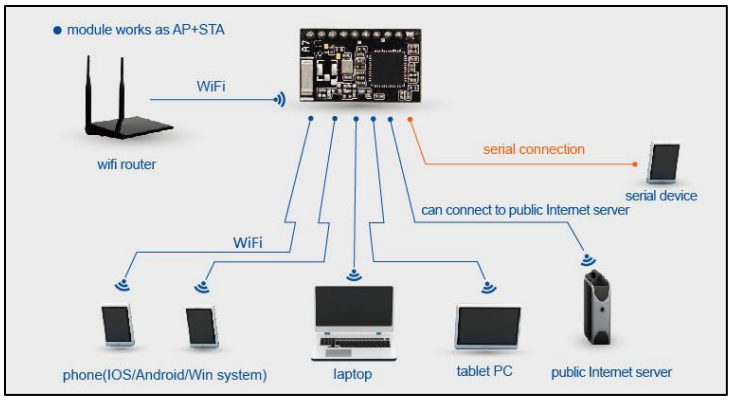
3.4.3.1 Tecnologías tradicionales de conectividad inalámbrica

- **Wifi**. La omnipresencia de WIFI, se ha convertido en la opción de conectividad más elegida por la mayoría de desarrolladores, todo esto dado a que ya existe en domésticos y comerciales: el standard WiFi más habitual utilizado en los hogares y en muchas empresas es el 802.11n, ofreciendo un rendimiento significativo en un rango de cientos de megabits por segundo, muy adecuado

[73] ACIS. Internet de las Cosas: La importancia de la infraestructura convergente de redes. [En linea]. 2017. [Consultado 02 de noviembre de 2017]. Disponible en internet: http://acis.org.co/portal/content/internet-de-las-cosas-la-importancia-de-la-infraestructura-convergente-de-redes

para la transferencia de archivos, pero que consume demasiada potencia para desarrollar aplicaciones IoT, tal y como se observa en la Ilustración 22.

Ilustración 22. AP+STA Mode



Fuente:USR IOT. IoT WiFi Module, Tiny Size. [En linea]. SF. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://www.usriot.com/p/iot-wifi-modules/

- Estándar: Basado en 802.11n
- Frecuencia: 2,4GHz y 5GHz
- Alcance: Aproximadamente 50m
- Velocidad de transferencia: hasta 600 Mbps, pero lo habitual es 150-200Mbps, en función del canal de frecuencia utilizado y del número de antenas (el standard 802.11-ac ofrece desde 500Mbps hasta 1Gbps).

- **Red de telefonía móvil**. Cualquier aplicación IoT que necesite funcionar en grandes áreas puede beneficiarse de las ventajas de la comunicación móvil GSM/3G/4G.

La red de telefonía móvil es capaz de enviar grandes cantidades de datos, especialmente a través de 4G, aunque el consumo de energía y el coste económico de la conexión podrían ser demasiado altos para muchas aplicaciones.

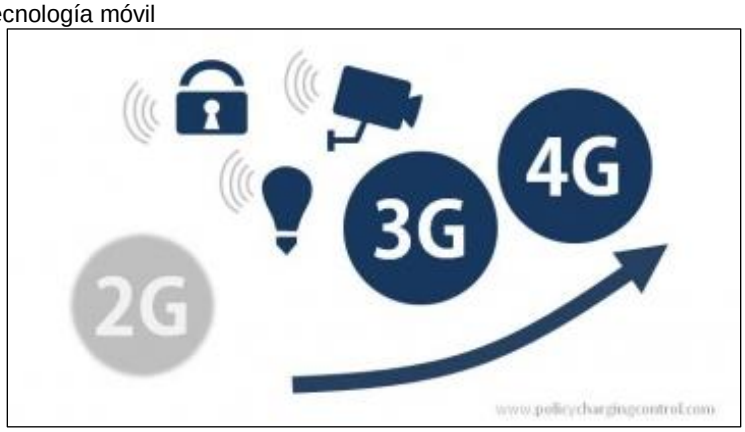
Sin embargo, puede ser ideal para proyectos que integren sensores y que no requieran un ancho de banda muy grande para enviar datos por Internet. (Ver Ilustración 23).

- Estándares: GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)
- Frecuencias: 900 / 1800 / 1900 / 2100

- Alcance: hasta 35km para GSM; hasta 200km para HSPA

- Velocidad de transferencia (descarga habitual): 35-170kps (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600kbps-10Mbps (HSPA), 3-10Mbps (LTE)

Ilustración 23. Tecnología móvil



Fuente: TARA, Neal. M2M Devices on 2G to be Phased Out as 3G and 4G LTE Devices Take Increased Share in the IoT Space. [En línea]. 2014. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://www.thefastmode.com/mobile-devices-and-wearables-trends/2212-m2m-devices-on-2g-to-be-phased-out-as-3g-and-4g-lte-devices-take-increased-share-in-the-iot-space

3.4.3.2 Tecnologías de corto alcance

- **NFC** (Near Field Communication). Es una tecnología que permite dos vías simultáneas de interacción segura entre dispositivos electrónicos, siendo especialmente adecuada para smartphones, permitiendo a los consumidores realizar transacciones de pago, acceder al contenido digital y conectar dispositivos electrónicos, todo ellos sin contacto.

Esencialmente, amplía la capacidad de la tecnología contacless de las tarjetas inteligentes permitiendo conexiones punto a punto y modos de funcionamiento activos y pasivos. (Ver Ilustración 24).

- Estándar: ISO/IEC 18000-3

- Frecuencia: 13.56MHz (ISM)

- Alcance: 10cm

- Velocidad de transf.: 100–420kbps

Ilustración 24. Tecnología NFC

Fuente: Parachute digital. What is Near Field Communication (NFC)?.[En línea]. 2013. [Consultado el 28 de marzo de 2018]. Disponible en internet: http://www.parachutedigitalmarketing.com.au/blog/mobile-marketing-and-apps/what-is-near-field-communication-nfc/

- **Bluetooth.** Este tipo de tecnologías permite la transmisión de datos a un alcance limitado y es una de las más establecidas e importantes dentro del ámbito de la electrónica de consumo. A través de este medio se fundamentara el desarrollo de dispositivos wearable que permitirá la conectividad de los dispositivos IoT, ello se puede observar en la ilustración 25.

Mediante esta herramienta las expectativas apuntan a que será clave, ya que permitirá el establecimiento de conexiones IoT, posiblemente mediante el uso de un smartphone.

Ilustración 25. Conexión a la nube mediante Bluetooth

Fuente: NAIRALAND, Join. New Bluetooth Update Allows For Direct Internet Access For Iot - Phones – Nairaland. [En línea]. 2016. [Consultado el 28 de marzo de 2018]. Disponible en internet: http://www.nairaland.com/2927679/new-bluetooth-update-allows-direct

El nuevo Bluetooth de baja energía, también conocido como Bluetooth LE o Bluetooth Smart, es otro protocolo importante para desarrollar aplicaciones IoT. Se caracteriza por ofrecer un alcance similar al de la tecnología Bluetooth normal pero con un consumo de energía significativamente reducido. Sin embargo, hay que tener en cuenta que Bluetooth LE no está diseñado para transferir archivos y es más adecuado para fragmentos de datos (chunks). Desde el punto de vista de los dispositivos de uso personal y, comparado con otras tecnologías, tiene la gran ventaja del alto grado de integración de esta tecnología en smartphones y dispositivos móviles. Según el Bluetooth Special Interest Group (SIG), se espera que en el año 2018 más del 90 por ciento de los smartphones dispongan de Bluetooth “Smart Ready”.

Los dispositivos que utilizan Bluetooth Smart incorporan el núcleo de Bluetooth en su versión 4.0 (o superior – la última versión de finales de 2014 es la 4.2) que combina transmisión de datos básicos con una configuración de bajo consumo. Es importante destacar que la versión 4.2, gracias a la incorporación del Internet Protocol Support Profile, permite conectarse directamente a internet mediante IPv6/6LoWPAN. Esto facilita el utilizar la infraestructura IP existente para gestionar dispositivos Bluetooth Smart basado en “edge computing”.

  - Estándar: Bluetooth 4.2
  - Frecuencia: 2,4GHz (ISM)
  - Alcance: 50-150m (Smart/LE)
  - Velocidad de transferencia: 1Mbps (Smart/LE)

- **ZigBee**. Es una tecnología inalámbrica más centrada en aplicaciones domóticas e industriales. Los perfiles ZigBee PRO y ZigBee Remote Control (RF4CE) se basan en el protocolo IEEE 802.15.4, una tecnología de red inalámbrica que opera a 2,4GHz en aplicaciones que requieren comunicaciones con baja tasa de envío de datos dentro de áreas delimitadas con un alcance de 100 metros, como viviendas o edificios.

ZigBee/RF4CE tiene algunas ventajas significativas como el bajo consumo en sistemas complejos, seguridad superior, robustez, alta escalabilidad y capacidad para soportar un gran número de nodos. Así, es una tecnología bien posicionada para marcar el camino del control wireless y las redes de sensores en aplicaciones IoT y M2M.

La última versión de Zigbee es la 3.0, ha sido lanzada recientemente y básicamente es la consolidación de ZigBee en un único standard. (Ver ilustración 26).

- Estándar: ZigBee 3.0 basado en IEEE 802.15.4
- Frecuencia: 2.4GHz
- Alcance: 10-100m
- Velocidad de transferencia: 250kbps

Ilustración 26. Tecnología ZigBee

Fuente: LLOYD, Craig. What Are “ZigBee” and “Z-Wave” Smarthome Products?. [En línea]. 2017. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://www.howtogeek.com/250614/what-are-zigbee-and-z-wave-smarthome-products/

- **Thread**. En la actualidad, el protocolo de red más innovador basado en IPv6 es Thread. Diseñado para domótica, está basado en 6LowPAN, y del mismo modo que aquel, no es un protocolo de aplicaciones IoT como Bluetooth o ZigBee. Se diseñó como un complemento WiFi, puesto que aunque la tecnología Wi-Fi funciona muy bien en dispositivos de consumo, tiene limitaciones al utilizar en configuraciones de domótica. (Ver Ilustración 27).

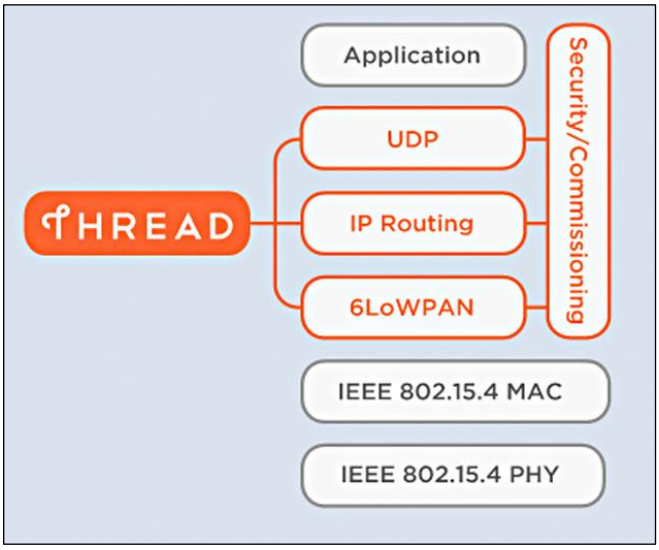
Diseñado para trabajar sobre chips IEEE 802.15.4 ya existentes de fabricantes como Freescale y Silicon Labs, Thread es compatible con redes de topología de malla al utilizar radio transceptores IEEE802.15.4, siendo capaz de manejar hasta 250 nodos con altos niveles de autenticación y cifrado.

Una actualización de software relativamente sencilla permite a los usuarios utilizar thread en dispositivos ya compatibles con IEEE 802.15.4.

- Estándar: Thread, basado en IEEE802.15.4 y 6LowPAN
- Frecuencia: 2,4GHz (ISM)
- Alcance: N/A

- Velocidad de transferencia: N/A

Ilustración 27. Protocolo Thread



Fuente: PARKERSON, Stuart. Thread Consortium Releases New IP-Based Wireless Protocol for IoT. [En línea]. 2015. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://appdevelopermagazine.com/3002/2015/7/23/Thread-Consortium-Releases-New-IP-Based-Wireless-Protocol-for-IoT/

Lanzado a mediados del 2014 por Thread Group, este protocolo sin canon de uso se basa en varios protocolos como IEEE 802.15.4, IPv6 y 6LoWPAN. Es una solución resistente basada en IP para aplicaciones IoT.

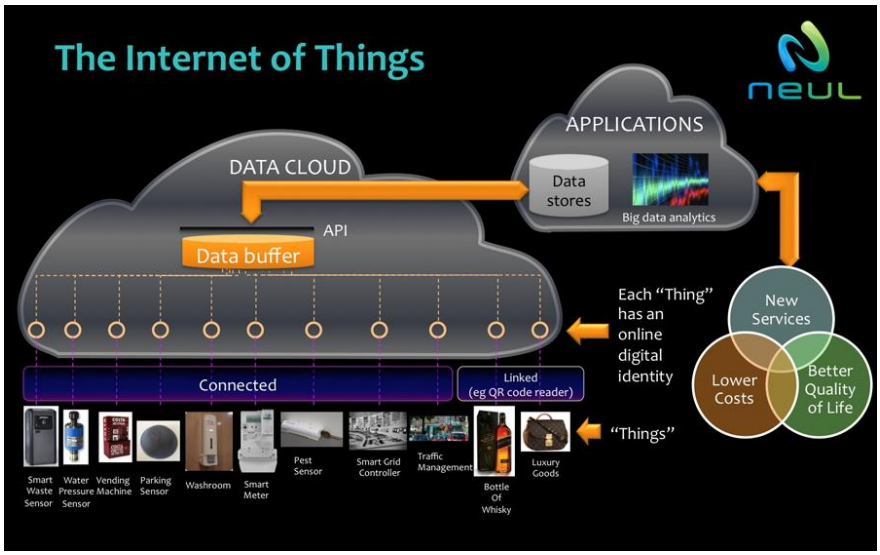
- **Neul**. El concepto de este sistema es similar al de Sigfox y funciona en la banda sub-1GHz. Neul aprovecha pequeños fragmentos de la “banda blanca” de las estaciones de TV para ofrecer alta escalabilidad, amplia cobertura y bajo costes.

Este sistema se basa en el chip Iceni, que se comunica utilizando los “banda blanca” de la radio para acceder al espectro UHF de alta calidad. Ya está disponible debido a la transición analógica a la televisión digital.

La tecnología de comunicaciones que utiliza se llama Weightless, que es una nueva tecnología de red inalámbrica ampliada diseñada para aplicaciones IoT que compite contra las soluciones GPRS, 3G, CDMA y LTE WAN.

La velocidad de transferencia de datos puede ir de unos bits por segundo hasta 100 Mbps en el mismo enlace. Desde el punto de vista del consumo, los dispositivos consumen tan solo de 20 a 30 mA, es decir, de 10 a 15 años de autonomía con 2 pilas AA. (Ver ilustración 28).

Ilustración 28. Internet de las cosas según Neul



Fuente: LAGANE, Christophe. Huawei s'avance dans les objets connectés avec Neul. [En línea]. 2014. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://www.silicon.fr/huawei-savance-les-objets-connectes-neul-96909.html

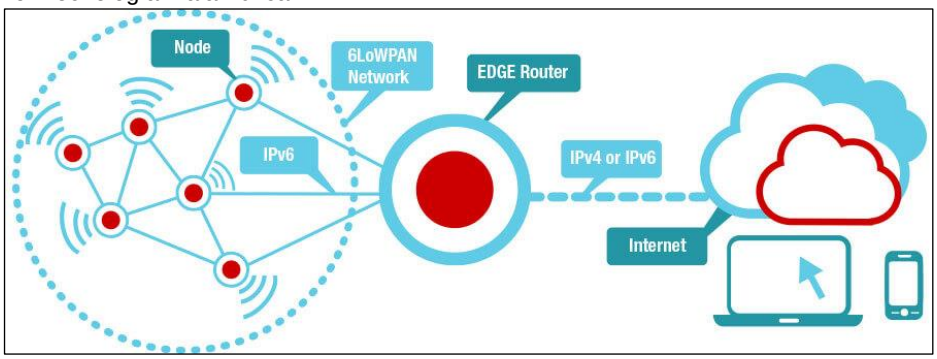
Para poder emplear esta tecnología hay que tener en cuenta la decisión que se haya tomado acerca del uso de las frecuencias de la banda blanda.

En ese sentido, en el Reino Unido, el organismo regulador Ofcom ha decido liberar esa banda para su uso sin licencia.

- Estándar: Neul
- Frecuencia: 900MHz (ISM), 458MHz (UK), 470-790MHz (espacios en blanco)
- Alcance: 10km
- Velocidad de transferencia: Desde unos pocos bps hasta 100kbps

- **6LoWPAN** (IPv6 Low-power wireless Personal Area Network). Es una tecnología inalámbrica basada en IP muy importante. En vez de tratarse de una tecnología de protocolos de aplicaciones IoT, como Bluetooth o ZigBee, 6LowPAN es un protocolo de red que permite mecanismos de encapsulado y compresión de cabeceras. Esta tecnología ofrece libertad de banda de frecuencia y capa física, por lo que se puede utilizar a través de múltiples plataformas de comunicaciones, como Ethernet, Wi-Fi, 802.15.4 y sub-1GHz ISM. (Ver ilustración 29).

Ilustración 29. Tecnología Inalámbrica



Fuente: Texas Instruments. Contiki-6LOWPAN. [En línea]. 2015. [Consultado el 28 de marzo de 2018]. Disponible en internet: http://processors.wiki.ti.com/index.php/Contiki-6LOWPAN

Una característica clave es la introducción de la pila IPv6 (protocolo de internet versión 6), una innovación clave en el avance de IoT en los últimos años, ya que con IPv6 se ofrecen aproximadamente 5 x 1028 direcciones IP a nivel global, permitiendo que cualquier objeto o dispositivo embebido tenga su propia dirección IP única para conectarse a Internet.

Ha sido diseñada especialmente para el hogar y la automatización de edificios proporcionando un mecanismo de transporte básico para producir sistemas de control complejos e interconexión de dispositivos de un modo económico a través de una red inalámbrica de bajo consumo.

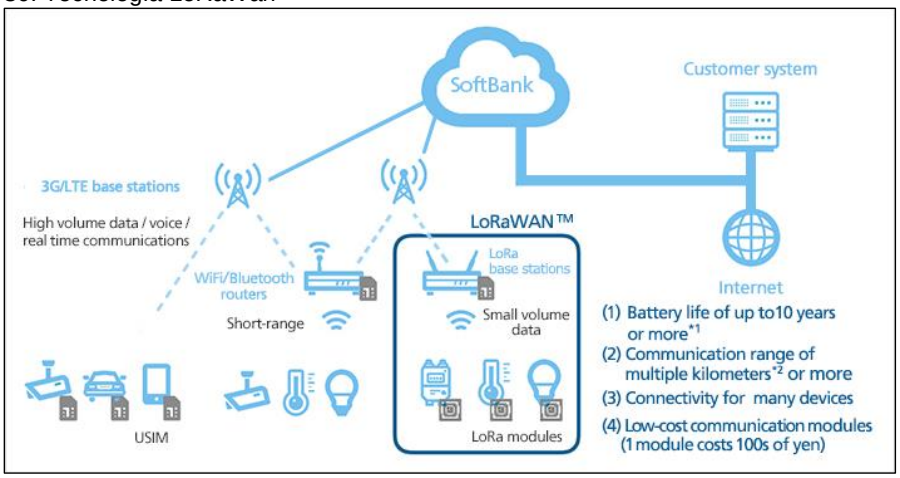
Diseñada para enviar paquetes IPv6 sobre redes IEEE 802.15.4, para luego implementar protocolos superiores como TCP, UDP, HTTP, COAP, MQTT y websockets, 6LowPAN es una red de topología en malla robusta, escalable y auto-regenerativa. Los routers pueden encaminar datos enviados a otros dispositivos, mientras que los hosts permanecen inactivos mucho tiempo.

- Estándar: RFC6282
- Frecuencia: adaptable a múltiples capas físicas como Bluetooth Smart (2.4GHz), ZigBee o comunicación RF de bajo consumo (sub-1GHz)
- Alcance: N/A
- Velocidad de transferencia: N/A

- **LoRaWAN**. Esta tecnología se parece en algunos aspectos a Sigfox y a Neul, está diseñada para implementar redes de área amplia (WAN) con características específicas para soportar comunicaciones móviles, bidireccionales, económicas

y seguras para aplicaciones de IoT, M2M, ciudades inteligentes y aplicaciones industriales, para una mejor interpretación se puede observar la Ilustración 30.

Ilustración 30. Tecnología LoRaWan



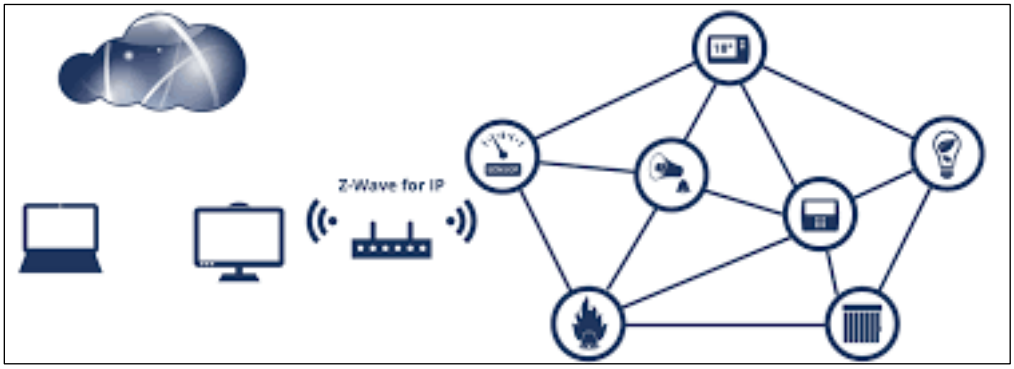
Fuente: SoftBank Corp. SoftBank to Roll Out 'LoRaWAN™' Low Power Wide Área Network. [En línea]. 2016. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://www.softbank.jp/en/corp/group/sbm/news/press/2016/20160912_01/

- Estándar: LoRaWAN
- Frecuencia: Varias
- Alcance: 2-5km (entorno urbano), 15km (entorno rural)
- Velocidad de transferencia: 0,3-50 kbps.

Optimizada para bajo consumo de energía y para ofrecer amplias redes con millones y millones de dispositivos, sus velocidades de transferencia de datos van desde 0,3 kbps hasta 50 kbps.

- **Z-WAVE**. Es una tecnología RF de bajo consumo diseñada inicialmente para productos de domótica como controladores de iluminación y sensores. Optimizado para la comunicación fiable de baja latencia de pequeños paquetes de datos, alcanza velocidades de datos de hasta 100kbit/s, opera en la banda de sub-1 GHz y es robusta frente a interferencias de Wi-Fi y otras tecnologías inalámbricas en el rango 2,4 GHz como Bluetooth o ZigBee. Es totalmente compatible con redes de topología de malla, no necesita un nodo coordinador y es muy escalable, permitiendo controlar hasta 232 dispositivos. (Ver ilustración 31).

Ilustración 31. Tecnología Z-Wave



Fuente: AutoDeus Technologies Private Limited. Z-Wave Technology: The New Standard in Home Automation. [En línea]. SF. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://smartify.in/knowledgebase/z-wave-technology/

Z-Wave utiliza un protocolo más simple que otras tecnologías lo que permite una mayor rapidez en el desarrollo, pero el único fabricante de chips compatibles es la empresa Sigma Design, en comparación con la multitud de empresas que ofrecen productos de otras tecnologías inalámbricas como ZigBee o Bluetooth.

- Estándar: Z-Wave Alliance ZAD12837 / ITU-T G.9959
- Frecuencia: 900MHz (Banda ISM)
- Alcance: 30m
- Velocidad de transferencia: 9,6/40/100kbit/s

3.4.3.3 Nuevas Tecnologías nativas

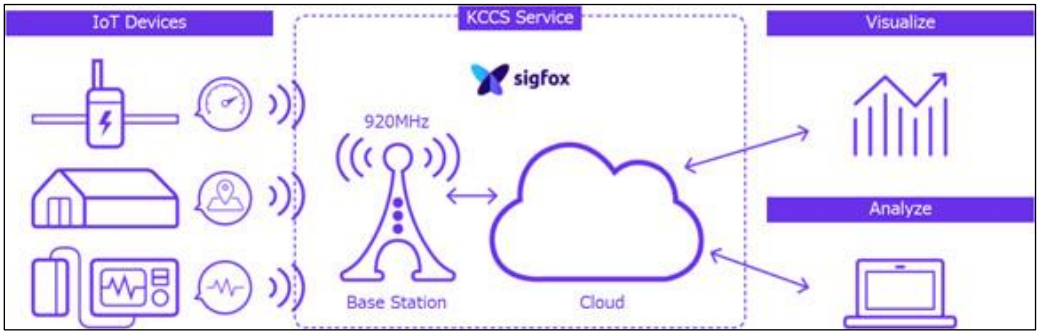
- **SIGFOX**. Una alternativa de amplio alcance es Sigfox, que en términos de alcance está entre Wi-Fi y la comunicación móvil. Utiliza bandas ISM, que se pueden utilizar sin necesidad de adquirir licencias.

Sigfox responde a las necesidades de muchas aplicaciones M2M que funcionan con una batería pequeña y solo requieren niveles menores de transferencia de datos, allí donde WiFi se queda demasiado corto y la comunicación móvil es muy cara y consume demasiada energía.

Sigfox utiliza una tecnología llamada Ultra Narrow Band (UNB) diseñada para funcionar con bajas velocidades de transferencias de 10 a 1.000 bits por segundo. Solo consume 50 microvatios (la comunicación móvil consume 5.000 microvatios) además de poder mantenerse en stand-by 20 años con una batería 2.5Ah (0,2 años

para comunicaciones móviles). Este tipo de tecnología se puede observar en la Ilustración 32.

Ilustración 32. Tecnología Sigfox



Fuente: KYOCERA. KYOCERA Launches Lowest Cost IoT Service in Japan in Partnership with SIGFOX. [En línea]. 2017. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://global.kyocera.com/news/2017/0401_bfko.html

Ya se ha implementado en miles de objetos conectados y la red se está instalando en las principales ciudades de Europa.

Esta tecnología es robusta, energéticamente eficiente y funciona como una red escalable que puede comunicarse con millones de dispositivos móviles a lo largo de muchos kilómetros cuadrados. Así pues, es adecuada para aplicaciones M2M como: contadores inteligentes, monitores médicos, dispositivos de seguridad, alumbrado público y sensores ambientales.

El sistema Sigfox utiliza los transceptores inalámbricos que funcionan en la banda sub-1GHz ofreciendo un rendimiento excepcional, mayor alcance y un consumo mínimo.

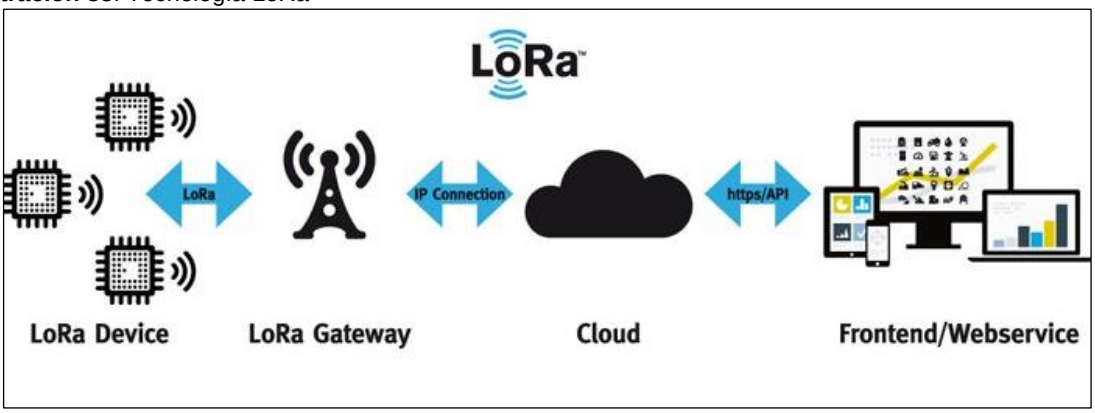
- Estándar: Sigfox
- Frecuencia: 900MHz
- Alcance: 30-50km (ambientes rurales), 3-10km (ambientes urbanos)
- Velocidad de transferencia: 10-1000bps

- **LoRa**. Es un tipo de modulación en radiofrecuencia patentado por Semtech, la cual permite una conexión de red de largo alcance y a bajo consumo[74], dispone de las siguientes características.

    - Alta tolerancia a las interferencias
    - Alta sensibilidad para recibir datos (-168dB)
    - Basado en modulación chirp
    - Bajo Consumo (hasta 10 años con una batería*)
    - Largo alcance 10 a 20km
    - Baja transferencia de datos (hasta 255 bytes)
    - Conexión punto a punto
    - Frecuencias de trabajo: 915Mhz América, 868 Europa, 433 Asia

Por consiguiente estas cualidades la hace ideal para conexiones a grandes distancias y para redes de IoT que se pueden utilizar en ciudades inteligentes, lugares con poca cobertura celular o redes privadas de sensores o actuadores como se observa en la ilustración 33.

Ilustración 33. Tecnología LoRa



Fuente: CRESPO, José Enrique. Aprendiendo Arduino. [En línea]. 2016. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://aprendiendoarduino.wordpress.com/tag/lorawan/

[74] Semtech. Que es LoRa. [En Línea]. 2018. [Consultado el 7 de Marzo de 2018]. Disponible en internet:]https://www.semtech.com/technology/lora/what-is-lora

Como se ha podido observar esas son la 12 tecnología de conectividad que se están utilizando actualmente, cuando se le pregunta a una persona del común normalmente contesta WIFI o bluetooth, en el caso de técnicos e ingenieros, muchos no están familiarizados con las nuevas tecnologías, sin decir de su funcionalidad o forma segura de ponerla en práctica.[75]

3.4.4 Entorno de facilitación

3.4.4.1 La nube inteligente[76]

El principal desafío al que se enfrentan las empresas, es poder mantener el ritmo acelerado y cada vez más innovador, clave principal para convertir a las empresas, con esto automatizándolas llegando a tener resultados óptimos; pero sin lugar a duda nada de esto podrá ser real si no se logra un hibrido entre las privadas y públicas, que permitan combinar la información y obtener resultados reales, solo con la mezcla correcta de con la mezcla correcta de eficiencia, seguridad y elasticidad podrá lograrse tan magno desafío. Esto se puede observar en la Ilustración 34.

Ilustración 34. Nube inteligente

Fuente: IT Business Solutions. Innovación: del IoT a la nube. [En línea]. SF. [Consultado el 28 de marzo de 2018]. Disponible en internet: http://www.itbusiness-solutions.com.mx/innovacion-del-iot-a-la-nube

Ya sea hacer un análisis de Big Data en una nube pública o entregar un servicio seguro a través de una nube privada. Los negocios están comenzando a influenciar

[75] Electrónica S.L.. 11 redes inalámbricas fundamentales para Internet de las Cosas. [En línea]. 2016. [Consultado 05 de noviembre de 2017]. Disponible en internet: https://www.redeweb.com/articulos/software/11-redes-inalambricas-fundamentales-para-internet-de-las-cosas/

[76] IT Business Solutions. Innovación del IoT en la nube: [En línea]. SF. [Consultado 03 de noviembre de 2017]. Disponible en internet: http://www.itbusiness-solutions.com.mx/innovacion-del-iot-a-la-nube

una combinación híbrida de nubes mientras se transforman para recibir al Internet de las Cosas.

IDC proyecta que el próximo año, el mercado de la nube pública registrará un crecimiento del 50% en América Latina, con un aumento también en la necesidad de infraestructura de cómputo en la nube local.

El Internet de las cosas será impulsor principal de las aplicaciones en línea y los servicios en la nube, dando a luz nuevos modelos que podrían amortiguar el acceso directo a los elementos críticos de la IoT, así como convertir las opciones de información y control en servicios de fácil acceso para los usuarios.

El IoT no puede tener éxito como una nube desordenada de sensores con acceso público, pero puede tenerlo como un conjunto de servicios en la nube. La nube no desplazará al IoT, solo lo mejorará.

- Nube de sensores: Este nuevo modelo puede ser la oportunidad más atractiva para un IoT de software como servicio (SaaS), y que cualquier proveedor de nube podría ofrecer.

- Nube de análisis: Este modelo es un conjunto de servicios que analizan datos para llegar a conclusiones útiles más allá de la gestión de los datos del sensor. La nube de análisis IoT es SaaS por naturaleza, y se puede utilizar como procesos de arquitectura orientada a servicios (SOA) o recursos REST.

3.4.5 Plataforma de integración

Representar la información capturada a través de los dispositivos IoT será el punto trascendental y que permitirá al usuario adelantar las actividades de análisis y toma de decisiones. Por consiguiente será primordial disponer de herramientas amigables al usuario ya sean nativas o web, que presenten la información, notificaciones, alarmas y resultados de forma sencilla y precisa. Adicional estas herramientas deben de incorporar o tener la capacidad de administrar los parámetros que permiten establecer las acciones que debe realizar estos dispositivos. En este orden de ideas los entornos que manejaran los usuarios tendrán que llevar a cabo tres funciones esenciales: controlar “cosas”, recoger “datos” y analizar “datos”.

En este sentido, la plataforma pasa a ser la base para que los dispositivos se interconecten y se genere un ecosistema propio, es decir al integrarse al IoT pasa a ser el software que conecta hardware, nodos, redes de datos y finalmente la herramienta que permite al usuario el control del recurso.

Frente a las propiedades que presentan estas herramientas y para ser consideradas como una verdadera plataforma IoT, deben estar enmarcadas dentro de las siguientes características.

3.4.5.1 Conectividad y normalización

Trae diferentes protocolos y diferentes formatos de datos en una sola interfaz de "software" que garantiza la transmisión de datos e interacción precisa con todos los dispositivos

3.4.5.2 Gestión de dispositivos

Asegura que las "cosas" conectadas funcionen correctamente, ejecutando sin problemas parches y actualizaciones para el software y las aplicaciones que se ejecutan en el dispositivo o en las puertas de enlace.

3.4.5.3 Almacenamiento

El almacenamiento escalable de los datos del dispositivo eleva los requisitos para las bases de datos híbridas basadas en la nube a un nuevo nivel en términos de volumen de datos, variedad, velocidad y veracidad.

3.4.5.4 Procesamiento y gestión

Da vida a los datos con desencadenantes de acción de eventos basados en reglas que permiten la ejecución de acciones "inteligentes" basadas en datos de sensores específicos.

3.4.5.5 Analítica

Realiza una gama de análisis complejos desde la agrupación de datos básicos y el aprendizaje automático profundo hasta el análisis predictivo que extrae el mayor valor del flujo de datos de IoT.

3.4.5.6 Visualización

Permite a los humanos ver patrones y observar las tendencias desde tableros de visualización donde los datos se representan vívidamente a través de gráficos lineales, apilados o circulares, modelos 2D o incluso 3D.

3.4.5.7 Herramientas adicionales

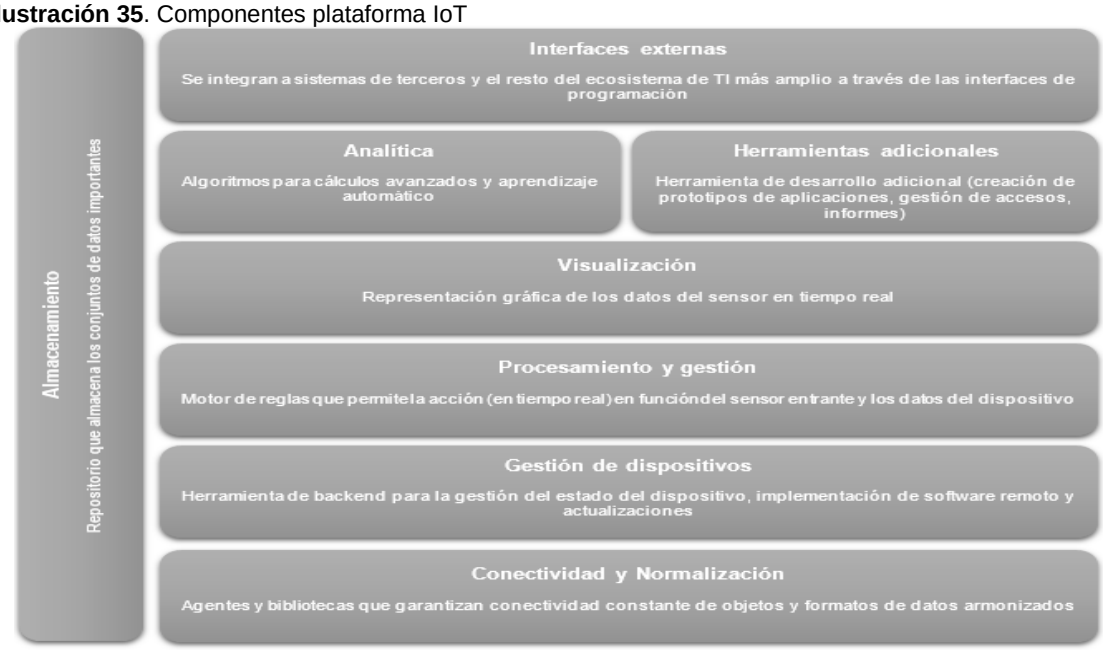
Permiten a los desarrolladores de IoT crear prototipos, probar y comercializar el caso de uso de IoT creando aplicaciones de ecosistema de plataforma para visualizar, administrar y controlar dispositivos conectados.

3.4.5.8 Interfaces externas

Se integran con sistemas de terceros y el resto del ecosistema de TI más amplio a través de las interfaces de programación de aplicaciones (API) incorporadas, los kits de desarrollo de software (SDK) y las puertas de enlace.

La secuencia de lo enunciado se puede apreciar en la ilustración 35.

Ilustración 35. Componentes plataforma IoT



Fuente: SCULLI, Padraig. 5 Things To Know About The IoT Platform Ecosystem. [En linea]. 2016. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://iot-analytics.com/5-things-know-about-iot-platform/

3.5 CLASIFICACIÓN DE ELEMENTOS Y RECURSOS DE INTERNET DE LAS COSAS (IOT)

Para llevar a cabo la clasificación de los elementos y recursos del internet de las cosas, se tienen en cuenta los lineamientos establecidos dentro de la metodología de análisis y gestión de riesgos de sistemas de información MAGERIT, elaborada por el Consejo Superior de Administración Electrónica de España.

Esta herramienta, contiene los instrumentos precisos para la administración de riesgos que se derivan del uso de los recursos tecnológicos, informáticos y de información, así mismo de acuerdo a sus definiciones, brinda las técnicas para la implementación de controles, procedimientos o políticas que minimicen cualquier afectación negativa que se puedan materializar sobre estos elementos.

Partiendo de ello, se lleva a cabo la organización de los elementos que hacen parte de la estructura de IoT, de acuerdo a las características propias que estos presentan.

En la tabla 12, se muestra los elementos de hardware que hacen parte del IoT y que son parte fundamental dentro de la operatividad de IoT.

Tabla 12. [HW] Equipamiento informático (hardware)

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVO	TIPO
[HW] Equipamiento informático (hardware)	[peripheral]	Sensores	Sensores de proximidad
			Acelerómetro y giroscópico
			Sensores de temperatura
			Sensor de humedad
			Sensor de presión
			Sensores de nivel
		Placas de Desarrollo	Raspberry Pi
			Arduino
			BeagleBone Black
			Joule
			Placa DECA
			Thunderboard React
			NRF52-DK
			Synergy
			FONA
			Placa de libertad
		Actuadores	Servomotor
			De paso a paso
			De corriente continua
			Lineales
			Rele
			Solenoide
	[network]	Gateway	
	[network]	Hub	

Fuente: Los autores

En la tabla 13, se muestran los canales de transmisión más empleados para el envío de datos entre dispositivos.

Tabla 13. [COM] Redes de comunicaciones

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVO	TIPO
[COM] Redes de comunicaciones	[wifi]	Conectividad inalámbrica "Tecnología Tradicional"	Wifi
	[mobile]		Red de telefonía móvil
	[wifi]	Tecnología de corto alcance	NFC
			Bluetooth
			ZigBee
			Thread
			Neul
			6LoWPAN
			LoRaWAN
			Z-WAVE
	[wifi]	Nuevas tecnologías	SIGFOX
			LoRa

Fuente: Los autores

En la tabla 14, se muestra el entorno de agrupación que permite la integración de los elementos de IoT.

Tabla 14. [Media] Soportes de información

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVO
[Media] Soportes de información	[vdisk]	Nube inteligente

Fuente: Los autores

En la tabla 15, se muestra el medio que permite el análisis, interpretación y manejo de los datos recolectados a través de los dispositivos inteligentes.

Tabla 15. [SW] Software - Aplicaciones informáticas

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVO	TIPO
[SW] Software - Aplicaciones informáticas	[sub]	Plataforma	Conectividad y normalización
			Gestión de dispositivos
			Almacenamiento
			Procesamiento y gestión
			Analítica
			Visualización
			Herramientas adicionales
			Interfaz externa

Fuente: Los autores

3.6 VULNERABILIDADES DE ELEMENTOS Y RECURSOS DE INTERNET DE LAS COSAS (IOT)

El alto crecimiento que está presentando la tecnología, viene permitiendo la inclusión de una nueva forma de interacción, en donde se emplean e incorporan dispositivos inteligentes, soluciones de comunicación y entornos virtuales conformando así los llamados ecosistemas IoT.

Esta incursión de elementos inteligentes en los diferentes entornos productivos de la sociedad, se convierten en punto de referencia y transformación que marca nuevos retos y desafíos con la seguridad. Por consiguiente, contrarrestar las vulnerabilidades que conciben los dispositivos de IoT, será uno de los temas trascendentales que deberán ser tratados por los fabricantes, integradores, consumidores y de las organizaciones dedicadas a la ciberseguridad, buscando que estos entornos se desarrollen de manera confiable y segura.

3.6.1 Identificación y valoración de amenazas

Dentro de este entorno se estructuran y se les da una valoración a los recursos que integran el ecosistema de IoT con lo cual se permite determinar las acciones adecuadas para mitigar sus deficiencias.

En la tabla 16, se muestran las diferentes amenazas y vulnerabilidades a que se exponen los elementos que hacen parte del IoT y que se enmarcan dentro del tipo de [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE).

Tabla 16. Amenazas y Vulnerabilidades - [HW] Equip. Informático (HARDWARE)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	VULNERABILIDADES
[peripheral]	Sensores	[N1] Fuego	No se disponga de los sistemas de protección y detección
		[N2] Daños por agua	La ubicación de los elementos no sea la adecuada
		[I5] Avería de origen físico o lógico	El dispositivo no se le realicen las inspecciones previas antes de salir al mercado
		[I3] Contaminación mecánica	Los dispositivos sean instalados bajo condiciones inadecuadas según las recomendaciones del fabricante
		[I7] Condiciones inadecuadas de temperatura o humedad	No se disponga de los mecanismos adecuados para la protección de los dispositivos
		[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos
		[E23] Errores de mantenimiento / actualización de equipos (hardware)	Desconocimiento y/o falta de los procedimientos preventivos

Tabla 16. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	VULNERABILIDADES
[peripheral]	Sensores	[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad
		[A11] Acceso no autorizado	Falta de políticas y/o controles
		[A23] Manipulación de los equipos	Ubicación inadecuada de los recursos
		[A25] Robo	Deficiencia de controles de acceso físico
	Placas de Desarrollo	[N1] Fuego	No se disponga de los sistemas de protección y detección
		[N2] Daños por agua	La ubicación de los elementos no sea la adecuada
		[I5] Avería de origen físico o lógico	El dispositivo no se le realicen las inspecciones previas antes de salir al mercado
		[I3] Contaminación mecánica	Los dispositivos sean instalados bajo condiciones inadecuadas según las recomendaciones del fabricante
		[I7] Condiciones inadecuadas de temperatura o humedad	No se disponga de los mecanismos adecuados para la protección de los dispositivos
		[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos
		[E8] Difusión de software dañino	Falta de mecanismos de seguridad sobre el recurso
		[E23] Errores de mantenimiento / actualización de equipos (hardware)	Desconocimiento y/o falta de los procedimientos preventivos
		[E24] Caída del sistema por agotamiento de recursos	Deficiencias en las programación y asignación de tareas
		[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad
		[A11] Acceso no autorizado	Falta de políticas y/o controles
		[A23] Manipulación de los equipos	Ubicación inadecuada de los recursos
		[A25] Robo	Deficiencia de controles de acceso físico
		[A26] Ataque destructivo	Falta de políticas de seguridad solidas
	Actuadores	[I1] Fuego	No se disponga de los sistemas de protección y detección
		[I2] Daños por agua	La ubicación de los elementos no sea la adecuada
		[I5] Avería de origen físico o lógico	El dispositivo no se le realicen las inspecciones previas antes de salir al mercado
		[I7] Condiciones inadecuadas de temperatura o humedad	No se disponga de los mecanismos adecuados para la protección de los dispositivos
		[I8] Fallo de servicios de comunicaciones	Deficiencias en los procedimientos de instalación del recurso
		[A23] Manipulación de los equipos	Ubicación inadecuada de los recursos
		[A25] Robo	Deficiencia de controles de acceso físico

Tabla 16. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	VULNERABILIDADES
[network]	Gateway / Hub	[I1] Fuego	No se disponga de los sistemas de protección y detección
		[I2] Daños por agua	La ubicación de los elementos no sea la adecuada
		[I5] Avería de origen físico o lógico	El dispositivo no se le realicen las inspecciones previas antes de salir al mercado
		[I6] Corte del suministro eléctrico	Falta de procedimientos o mecanismos de inspección en los sistemas de alimentación
		[I7] Condiciones inadecuadas de temperatura o humedad	No se disponga de los mecanismos adecuados para la protección de los dispositivos
		[I8] Fallo de servicios de comunicaciones	Falta de mecanismos de inspección y seguimiento sobre el recurso
		[E2] Errores del administrador	Falta de verificación de los procedimientos y lineamientos establecidos
		[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos
		[E8] Difusión de software dañino	Falta de mecanismos de inspección y seguimiento sobre el recurso
		[E23] Errores de mantenimiento / actualización de equipos (hardware)	Desconocimiento y/o falta de los procedimientos preventivos
		[E25] Pérdida de equipos	Deficiencia de controles de acceso físico
		[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad
		[A6] Abuso de privilegios de acceso	Falta de procedimientos de control frente a la asignación de privilegios
		[A8] Difusión de software dañino	Falta de mecanismos de seguridad sobre el recurso
		[A12] Análisis de tráfico	Falta de políticas de seguridad y seguimiento sobre el recurso
		[A24] Denegación de servicio	Deficiencia en los procedimientos aplicados sobre el recurso

Fuente: Los autores

En la tabla 17, se muestran las diferentes amenazas y vulnerabilidades a que se exponen los elementos que hacen parte del IoT y que se enmarcan dentro del tipo de [COM] Redes de comunicaciones.

Tabla 17. Amenazas y Vulnerabilidades - [COM] Redes de comunicaciones

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	VULNERABILIDADES
[wifi] / [mobile]	Conectividad inalámbrica "Tecnología Tradicional" / Tecnología de corto alcance / Nuevas tecnologías	[I8] Fallo de servicios de comunicaciones	Falta de mecanismos de inspección y seguimiento sobre el recurso
		[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos
		[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad
		[A11] Acceso no autorizado	Falta de políticas y/o controles
		[A14] Interceptación de información (escucha)	Mecanismos de protección deficientes
		[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos
		[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad
		[A11] Acceso no autorizado	Falta de políticas y/o controles
		[A14] Interceptación de información (escucha)	Mecanismos de protección deficientes
		[A24] Denegación de servicio	Deficiencia en los procedimientos aplicados sobre el recurso

Fuente: Los autores

En la tabla 18, se muestran las diferentes amenazas y vulnerabilidades a que se exponen los elementos que hacen parte del IoT y que se enmarcan dentro del tipo de [Media] Soportes de información.

Tabla 18. Amenazas y Vulnerabilidades - [Media] Soportes de información

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	VULNERABILIDADES
[vdisk]	Nube inteligente	[I5] Avería de origen físico o lógico	Deficiencia en la estructuración del entorno
		[I8] Fallo de servicios de comunicaciones	Falta de mecanismos de inspección y seguimiento sobre el recurso
		[I10] Degradación de los soportes de almacenamiento de la información	No se realizan análisis a la estructura de almacenamiento de datos
		[E1] Errores de los usuarios	Falta de habilidades frente al manejo del recurso
		[E2] Errores del administrador	Falta de verificación de los procedimientos y lineamientos establecidos

Tabla 18. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	VULNERABILIDADES
[vdisk]	Nube inteligente	[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos
		[E8] Difusión de software dañino	Falta de mecanismos de seguridad sobre el recurso
		[E14] Escapes de información	Falta de controles frente a los procesos que se realizan sobre el recurso
		[E21] Errores de mantenimiento / actualización de programas (software)	Desconocimiento y/o falta de los procedimientos frente al manejo del entorno
		[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad
		[A5] Suplantación de la identidad del usuario	Manejo inadecuado del recurso
		[A6] Abuso de privilegios de acceso	Falta de procedimientos para el seguimiento de las actividades que se realizan sobre el recurso
		[A7] Uso no previsto	Falta de lineamientos frente al uso del recurso
		[A8] Difusión de software dañino	Falta de mecanismos de inspección y seguimiento sobre el recurso
		[A11] Acceso no autorizado	Falta de políticas y/o controles
		[A18] Destrucción de información	Deficiencia en los mecanismos de protección del entorno
		[A19] Divulgación de información	Falta de controles de auditoria frente a los procesos realizados sobre el recurso
		[A24] Denegación de servicio	Deficiencia en los procedimientos aplicados sobre el recurso

Fuente: Los autores

En la tabla 19, se muestran las diferentes amenazas y vulnerabilidades a que se exponen los elementos que hacen parte del IoT y que se enmarcan dentro del tipo de [SW] Software - Aplicaciones informáticas.

Tabla 19. Amenazas y Vulnerabilidades - [SW] Software - Aplicaciones informáticas

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	VULNERABILIDADES
[sub]	Plataforma	[I8] Fallo de servicios de comunicaciones	Falta de mecanismos de inspección y seguimiento sobre el recurso
		[I10] Degradación de los soportes de almacenamiento de la información	No se realizan análisis a la estructura de almacenamiento de datos
		[E1] Errores de los usuarios	Falta de habilidades frente al manejo del recurso

Tabla 19. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	VULNERABILIDADES
[sub]	Plataforma	[E2] Errores del administrador	Deficiencias en la estructuración del recurso
		[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos
		[E8] Difusión de software dañino	Falta de mecanismos de seguridad sobre el recurso
		[E14] Escapes de información	Falta de controles frente a los procesos que se realizan sobre el recurso
		[E20] Vulnerabilidades de los programas (software)	Deficiencia en la estructuración y adecuación del recurso
		[E21] Errores de mantenimiento / actualización de programas (software)	Desconocimiento y/o falta de los procedimientos frente al manejo del entorno
		[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad
		[A5] Suplantación de la identidad del usuario	Manejo inadecuado del recurso
		[A6] Abuso de privilegios de acceso	Falta de procedimientos para el seguimiento de las actividades que se realizan sobre el recurso
		[A7] Uso no previsto	Falta de lineamientos frente al uso del recurso
		[A8] Difusión de software dañino	Falta de mecanismos de inspección y seguimiento sobre el recurso
		[A11] Acceso no autorizado	Falta de políticas y/o controles
		[A15] Modificación deliberada de la información	La estructura del recurso no disponga de los parámetros de seguridad requeridos
		[A18] Destrucción de información	Falta de mecanismos de barrera que minimice las acciones delictivas
		[A19] Divulgación de información	Falta de controles frente a los procesos que se realizan sobre el recurso
		[A24] Denegación de servicio	Deficiencia en los procedimientos aplicados sobre el recurso
		[A26] Ataque destructivo	El entorno de trabajo no dispone de los mecanismos de seguridad requeridos
		[A30] Ingeniería social (picaresca)	Falta de incorporación de procedimientos para el uso apropiado de los recursos

Fuente: Los autores

Valoración cualitativa

En la tabla 20, se muestra los criterios de valoración y aspectos relacionados con las cualidades que poseen los elementos que integran IoT. (Ver tabla 3. Criterios para las dimensiones).

Tabla 20. Activos y valoración cualitativa

INFORMACIÓN DE LOS ACTIVOS																	
	Nombre del activo de información	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)	¿Es activo de información de terceros o de	¿Activo de información que debe ser	Activo de información que debe ser	Activo de información que puede ser	Activo de información que es muy crítico	Activo de información que es muy crítico	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
													Leve	Importante	Grave		
1	[HW_Sensores]	A	MA	A	MA	MA	X	X	X	X	X	X			X	X	
1	[HW_Sensores]	A	MA	A	MA	MA	X	X	X	X	X	X			X	X	
2	[HW_Placas de desarrollo]	MA	A	MA	M	MA	X	X	X	X	X	X			X	X	
3	[HW_Actuadores]	A	MA	A	M	MA	X	X	X	X	X	X		X		X	
4	[HW_Gateway / Hub]	MA	MA	MA	A	MA	X	X	X	X	X	X			X	X	
5	[COM_Conectividad inalámbrica "Tecnología Tradicional"], [COM_Tecnología de corto alcance], [COM_Nuevas tecnologías]	A	MA	A	A	MA	X	X	X	X	X	X		X			X
6	[MEDIA_Nube Inteligente]	MA	MA	MA	MA	MA	X	X	X	X	X	X			X		X
7	[SW_ Plataforma]	MA	MA	MA	MA	MA	X	X	X	X	X	X			X		X

Fuente: Los autores

Valoración cuantitativa

En la tabla 21, se muestran los valores sobre los riesgos y que constituyen una potencial materialización de las amenazas que afectan directamente a los elementos de IoT. (Ver tabla 6. Criterios valoración del riesgo y tabla 7. Convenciones para la valoración del riesgo).

Esta valoración se enmarca en base a los pilares de la seguridad de la información, Disponibilidad [D], Integridad [I], Confidencialidad [C]. Autenticidad [A] y Trazabilidad [T].

Tabla 21. Valoración cuantitativa

Resumen de Valoración de Riesgos de los Activos								
METODOLOGÍA DE MAGERIT: VALORACIÓN DEL RIESGO								
ACTIVO	**RIESGO**	**FRECUENCIA**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**TOTAL**
[HW_Sensores]	CRITICO	4	25	25	20	20	25	23
[HW_Placas de desarrollo]	CRITICO	4	25	15	25	25	20	22
[HW_Actuadores]	CRITICO	4	25	15	20	20	25	21
[HW_Gateway / Hub]	CRITICO	5	25	20	25	25	25	24
[COM_Conectividad inalámbrica "Tecnología Tradicional"], [COM_Tecnología de corto alcance], [COM_Nuevas tecnologías]	CRITICO	5	25	20	20	20	25	22
[MEDIA_Nube Inteligente]	CRITICO	5	25	25	25	25	25	25
[SW_ Plataforma]	CRITICO	5	25	25	25	25	25	25

Fuente: Los autores

En la tabla 22, se muestra el análisis de las vulnerabilidades y riesgos de los elementos que integran IoT. (Ver numeral 2.3.3 Criterios de valoración).

Tabla 22. Matriz de análisis de riesgos

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
1	[HW_Sensores]	23	[N1] Fuego	No se disponga de los sistemas de protección y detección	3	69	C	1	69	C	I
			[N2] Daños por agua	La ubicación de los elementos no sea la adecuada	4	92	C	1	92	C	I
			[I5] Avería de origen físico o lógico	El dispositivo no se le realicen las inspecciones previas antes de salir al mercado	4	92	C	1	92	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
1	[HW_Sensores]	23	[I3] Contaminación mecánica	Los dispositivos sean instalados bajo condiciones inadecuadas según las recomendaciones del fabricante	3	69	C	1	69	C	I
			[I7] Condiciones inadecuadas de temperatura o humedad	No se disponga de los mecanismos adecuados para la protección de los dispositivos	4	92	C	1	92	C	I
			[E4] Errores de configuración	Ausencia de politicas de apropiación en el uso de los recursos	4	92	C	1	92	C	I
			[E23] Errores de mantenimiento / actualización de equipos (hardware)	Desconocimiento y/o falta de los procedimientos preventivos	4	92	C	1	92	C	I
			[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad	3	69	C	1	69	C	I
			[A11] Acceso no autorizado	Falta de políticas y/o controles	3	69	C	1	69	C	I
			[A23] Manipulación de los equipos	Ubicación inadecuada de los recursos	4	92	C	1	92	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
1	[HW_Sensores]	23	[A25] Robo	Deficiencia de controles de acceso físico	4	92	C	1	92	C	I
2	[HW_Placas de desarrollo]	22	[N1] Fuego	No se disponga de los sistemas de protección y detección	3	66	C	1	66	C	I
			[N2] Daños por agua	La ubicación de los elementos no sea la adecuada	4	88	C	1	88	C	I
			[I5] Avería de origen físico o lógico	El dispositivo no se le realicen las inspecciones previas antes de salir al mercado	3	66	C	1	66	C	I
			[I3] Contaminación mecánica	Los dispositivos sean instalados bajo condiciones inadecuadas según las recomendaciones del fabricante	3	66	C	1	66	C	I
			[I7] Condiciones inadecuadas de temperatura o humedad	No se disponga de los mecanismos adecuados para la protección de los dispositivos	4	88	C	1	88	C	I
			[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos	4	88	C	1	88	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
2	[HW_Placas de desarrollo]	22	[E8] Difusión de software dañino	Falta de mecanismos de seguridad sobre el recurso	4	88	C	1	88	C	I
			[E23] Errores de mantenimiento / actualización de equipos (hardware)	Desconocimiento y/o falta de los procedimientos preventivos	3	66	C	1	66	C	I
			[E24] Caída del sistema por agotamiento de recursos	Deficiencias en las programación y asignación de tareas	3	66	C	1	66	C	I
			[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad	3	66	C	1	66	C	I
			[A11] Acceso no autorizado	Falta de políticas y/o controles	4	88	C	1	88	C	I
			[A23] Manipulación de los equipos	Ubicación inadecuada de los recursos	4	88	C	1	88	C	I
			[A25] Robo	Deficiencia de controles de acceso fisico	4	88	C	1	88	C	I
			[A26] Ataque destructivo	Falta de políticas de seguridad solidas	3	66	C	1	66	C	I
3	[HW_Actuadores]	21	[I1] Fuego	No se disponga de los sistemas de protección y detección	3	63	C	1	63	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
3	[HW_Actuadores]	21	[I2] Daños por agua	La ubicación de los elementos no sea la adecuada	4	84	C	1	84	C	I
			[I5] Avería de origen físico o lógico	El dispositivo no se le realicen las inspecciones previas antes de salir al mercado	3	63	C	1	63	C	I
			[I7] Condiciones inadecuadas de temperatura o humedad	No se disponga de los mecanismos adecuados para la protección de los dispositivos	4	84	C	1	84	C	I
			[I8] Fallo de servicios de comunicaciones	Deficiencias en los procedimientos de instalación del recurso	4	84	C	1	84	C	I
			[A23] Manipulación de los equipos	Ubicación inadecuada de los recursos	3	63	C	1	63	C	I
			[A25] Robo	Deficiencia de controles de acceso físico	4	84	C	1	84	C	I
4	[HW_Gateway / Hub]	24	[I1] Fuego	No se disponga de los sistemas de protección y detección	3	72	C	1	72	C	I
			[I2] Daños por agua	La ubicación de los elementos no sea la adecuada	4	96	C	1	96	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
4	[HW_Gateway / Hub]	24	[I5] Avería de origen físico o lógico	El dispositivo no se le realicen las inspecciones previas antes de salir al mercado	4	96	C	1	96	C	I
			[I6] Corte del suministro eléctrico	Falta de procedimientos o mecanismos de inspección en los sistemas de alimentación	4	96	C	1	96	C	I
			[I7] Condiciones inadecuadas de temperatura o humedad	No se disponga de los mecanismos adecuados para la protección de los dispositivos	4	96	C	1	96	C	I
			[I8] Fallo de servicios de comunicaciones	Falta de mecanismos de inspección y seguimiento sobre el recurso	3	72	C	1	72	C	I
			[E2] Errores del administrador	Falta de verificación de los procedimientos y lineamientos establecidos	4	96	C	1	96	C	I
			[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos	4	96	C	1	96	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
4	[HW_Gateway / Hub]	24	[E8] Difusión de software dañino	Falta de mecanismos de inspección y seguimiento sobre el recurso	4	96	C	1	96	C	I
			[E23] Errores de mantenimiento / actualización de equipos (hardware)	Desconocimiento y/o falta de los procedimientos preventivos	3	72	C	1	72	C	I
			[E25] Pérdida de equipos	Deficiencia de controles de acceso físico	4	96	C	1	96	C	I
			[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad	4	96	C	1	96	C	I
			[A6] Abuso de privilegios de acceso	Falta de procedimientos de control frente a la asignación de privilegios	4	96	C	1	96	C	I
			[A8] Difusión de software dañino	Falta de mecanismos de seguridad sobre el recurso	4	96	C	1	96	C	I
			[A12] Análisis de tráfico	Falta de políticas de seguridad y seguimiento sobre el recurso	4	96	C	1	96	C	I
			[A24] Denegación de servicio	Deficiencia en los procedimientos aplicados sobre el recurso	4	96	C	1	96	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
5	[COM_Conectividad inalámbrica "Tecnología Tradicional"], [COM_Tecnología de corto alcance], [COM_Nuevas tecnologías]	22	[I8] Fallo de servicios de comunicaciones	Falta de mecanismos de inspección y seguimiento sobre el recurso	4	88	C	1	88	C	I
			[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos	3	66	C	1	66	C	I
			[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad	3	66	C	1	66	C	I
			[A11] Acceso no autorizado	Falta de políticas y/o controles	4	88	C	1	88	C	I
			[A14] Interceptación de información (escucha)	Mecanismos de protección deficientes	4	88	C	1	88	C	I
			[A24] Denegación de servicio	Deficiencia en los procedimientos aplicados sobre el recurso	4	88	C	1	88	C	I
6	[MEDIA_Nube Inteligente]	25	[I5] Avería de origen físico o lógico	Deficiencia en la estructuración del entorno	3	75	C	1	75	C	I
			[I8] Fallo de servicios de comunicaciones	Falta de mecanismos de inspección y seguimiento sobre el recurso	3	75	C	1	75	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
6	[MEDIA_Nube Inteligente]	25	[I10] Degradación de los soportes de almacenamiento de la información	No se realizan análisis a la estructura de almacenamiento de datos	3	75	C	1	75	C	I
			[E1] Errores de los usuarios	Falta de habilidades frente al manejo del recurso	4	100	C	1	100	C	I
			[E2] Errores del administrador	Falta de verificación de los procedimientos y lineamientos establecidos	4	100	C	1	100	C	I
			[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos	4	100	C	1	100	C	I
			[E8] Difusión de software dañino	Falta de mecanismos de seguridad sobre el recurso	4	100	C	1	100	C	I
			[E14] Escapes de información	Falta de controles frente a los procesos que se realizan sobre el recurso	4	100	C	1	100	C	I
			[E21] Errores de mantenimiento / actualización de programas (software)	Desconocimiento y/o falta de los procedimientos frente al manejo del entorno	3	75	C	1	75	C	I
			[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad	4	100	C	1	100	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
6	[MEDIA_Nube Inteligente]	25	[A5] Suplantación de la identidad del usuario	Manejo inadecuado del recurso	4	100	C	1	100	C	I
			[A6] Abuso de privilegios de acceso	Falta de procedimientos para el seguimiento de las actividades que se realizan sobre el recurso	4	100	C	1	100	C	I
			[A7] Uso no previsto	Falta de lineamientos frente al uso del recurso	3	75	C	1	75	C	I
			[A8] Difusión de software dañino	Falta de mecanismos de inspección y seguimiento sobre el recurso	4	100	C	1	100	C	I
			[A11] Acceso no autorizado	Falta de políticas y/o controles	4	100	C	1	100	C	I
			[A18] Destrucción de información	Deficiencia en los mecanismos de protección del entorno	3	75	C	1	75	C	I
			[A19] Divulgación de información	Falta de controles de auditoria frente a los procesos realizados sobre el recurso	3	75	C	1	75	C	I
			[A24] Denegación de servicio	Deficiencia en los procedimientos aplicados sobre el recurso	4	100	C	1	100	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
7	[SW_ Plataforma]	25	[I8] Fallo de servicios de comunicaciones	Falta de mecanismos de inspección y seguimiento sobre el recurso	4	100	C	1	100	C	I
			[I10] Degradación de los soportes de almacenamiento de la información	No se realizan análisis a la estructura de almacenamiento de datos	3	75	C	1	75	C	I
			[E1] Errores de los usuarios	Falta de habilidades frente al manejo del recurso	3	75	C	1	75	C	I
			[E2] Errores del administrador	Deficiencias en la estructuración del recurso	4	100	C	1	100	C	I
			[E4] Errores de configuración	Ausencia de políticas de apropiación en el uso de los recursos	4	100	C	1	100	C	I
			[E8] Difusión de software dañino	Falta de mecanismos de seguridad sobre el recurso	4	100	C	1	100	C	I
			[E14] Escapes de información	Falta de controles frente a los procesos que se realizan sobre el recurso	4	100	C	1	100	C	I
			[E20] Vulnerabilidades de los programas (software)	Deficiencia en la estructuración y adecuación del recurso	4	100	C	1	100	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
7	[SW_ Plataforma]	25	[E21] Errores de mantenimiento / actualización de programas (software)	Desconocimiento y/o falta de los procedimientos frente al manejo del entorno	3	75	C	1	75	C	I
			[A4] Manipulación de la configuración	Deficiencia de mecanismos de seguridad	4	100	C	1	100	C	I
			[A5] Suplantación de la identidad del usuario	Manejo inadecuado del recurso	4	100	C	1	100	C	I
			[A6] Abuso de privilegios de acceso	Falta de procedimientos para el seguimiento de las actividades que se realizan sobre el recurso	4	100	C	1	100	C	I
			[A7] Uso no previsto	Falta de lineamientos frente al uso del recurso	3	75	C	1	75	C	I
			[A8] Difusión de software dañino	Falta de mecanismos de inspección y seguimiento sobre el recurso	4	100	C	1	100	C	I
			[A11] Acceso no autorizado	Falta de politicas y/o controles	4	100	C	1	100	C	I

Tabla 22. (Continuación)

No. De amenazas y vulnerabilidades	Nombre del activo de información	Valoración del riesgo	Amenazas metodología magerit	Vulnerabilidades	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad de vulneración)	Criticidad neta	Calificación de gestión	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual	Niveles de aceptación del riesgo
7	[SW_ Plataforma]	25	[A15] Modificación deliberada de la información	La estructura del recurso no disponga de los parámetros de seguridad requeridos	3	75	C	1	75	C	I
			[A18] Destrucción de información	Falta de mecanismos de barrera que minimice las acciones delictivas	3	75	C	1	75	C	I
			[A19] Divulgación de información	Falta de controles frente a los procesos que se realizan sobre el recurso	4	100	C	1	100	C	I
			[A24] Denegación de servicio	Deficiencia en los procedimientos aplicados sobre el recurso	4	100	C	1	100	C	I
			[A26] Ataque destructivo	El entorno de trabajo no dispone de los mecanismos de seguridad requeridos	4	100	C	1	100	C	I
			[A30] Ingeniería social (picaresca)	Falta de incorporación de procedimientos para el uso apropiado de los recursos	3	75	C	1	75	C	I

Fuente: Los autores

4. DETERMINAR CUALES SON LOS RIESGOS A LOS CUALES ESTÁN EXPUESTAS LAS ORGANIZACIONES FRENTE AL AUGE DE INTERNET DE LAS COSAS (IoT) Y LOS MECANISMOS QUE PUEDEN SER ADOPTADOS PARA MINIMIZAR LAS VULNERABILIDADES

El crecimiento que se viene dando sobre los dispositivos que se enmarcan dentro del IoT, es proporcional a los riesgos que estos generan frente a la seguridad de la información y sobre el mismo recurso, las compañías en su afán de sacar al mercado productos diversos, no tienen priorizados los mecanismos de seguridad para la protección de estos medios, pues prevalecen los factores económicos sobre los ambientes seguros.

A partir de ello, la seguridad se traslada a quienes incorporan estas herramientas para el cumplimento de procesos, con lo cual se deberán adoptar mecanismos de protección que eviten cualquier tipo de afectación a nivel del dispositivo como del entorno en el cual realiza sus funciones. Partiendo de ello, existen procedimientos que minimizan la exposición a los delincuentes informáticos.

Los dispositivos enmarcados dentro del IoT tienen un atrayente para los delincuentes informáticos dado su robustez de manejo de información, por tanto presentan una mayor deficiencia que un sistema tradicional, debido a que su incorporación dentro del mercado es muy reciente y las políticas de seguridad son prácticamente inexistentes. Partiendo de ello, estos dispositivos al estar conectados a la red mundial pueden estar expuestos a sufrir afectaciones como:

4.1 LEYES DÉBILES O INEXISTENTES FRENTE A LA PROBLEMÁTICA DE INSEGURIDAD DE LOS DISPOSITIVOS IOT

La Comisión Federal de Comercio de los EE. UU. publicó recientemente un informe que analiza el equilibro entre las preocupaciones de seguridad y privacidad asociadas al desarrollo de los dispositivos de IoT.[77]

La metodología utilizada por HP Fortify a partir de HP Fortify on Demand, el Informe sobre sistemas de seguridad para el hogar de HP probó 10 de los más populares dispositivos de IoT de seguridad para el hogar para detectar vulnerabilidades por medio de técnicas de pruebas de seguridad estándar, que combinan pruebas manuales y herramientas automatizadas. Los dispositivos y sus componentes se

[77] Crece vulnerabilidad en sistemas de seguridad para IoT. [En línea]. 2015. [Consultado el 07 de Noviembre de 2017]. Disponible en internet: http://www.cioal.com/2015/05/22/hp-da-a-conocer-vulnerabilidad-en-sistemas-de-seguridad-para-iot/

evaluaron con base en la lista OWASP Internet of Things Top 10 y en las vulnerabilidades específicas de cada categoría

4.2 ATAQUES A LOS QUE SON SUSCEPTIBLES UN IOT NUEVO

Una representación de la susceptibilidad que presentan los dispositivos IoT frente a los delincuentes informáticos se puede analizar en la Ilustración 36.

Ilustración 36. Ataques a los IoT

Fuente: Mercado. Internet de las Cosas, con foco en seguridad. [En línea]. 2017. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://www.mercado.com.ar/notas/8024928

4.2.1 Ataque DDoS

Este tipo de ataque, tiene como fundamento generar indisponibilidad de los recursos mediante la saturación de procesos. Sus siglas traducen Distributed Denial of Service y literalmente se trata de la denegación del servicio mediante el ataque desde muchos ordenadores a un servidor.

Para explicar cómo funciona un ataque DDoS mediante IoT, se utilizara la siguiente analogía, supongamos que el servidor es una ventanilla de atención al usuarios pertenecientes a una empresa, donde se reciben Peticiones quejas y reclamos, con una eficacia capaz de atender las PQR con gran agilidad y de un momento a otro personas que no son de la empresa empiezan a enviar de forma masiva Peticiones Quejas y Reclamos poniendo lenta la atención en la ventanilla hasta el punto de paralizar por completo el servicio.

Desglosemos mejor que fue lo que sucedió

- La ventanilla = Servidor

- Usuarios de la empresa = tráfico normal

- Usuarios ajenos a la empresa= Cosas infectadas “cafeteras, cámaras IP, DVRs” s como muchos otros pertenecientes a IoT que tienen un problema, su seguridad es poca o nula y son utilizados por el atacante para saturar el servicio

4.2.2 Suplantación de identidad

Empleando las páginas, mensajes de correo y mensajes por WhatsApp que son falsos, pero que el usuario cae porque le ofrece algo, los atacantes buscaran engañar a los usuarios haciéndoles creer que están accediendo a sitios seguros, cuando realmente están siendo engañados, con la finalidad de obtener información confidencial.

Todo esto se presenta gracias a que cada día es más común ver dispositivos Smart tales como Impresoras, televisores neveras, un tostador o una tetera conectada a internet, oportunidad que los criminales no desperdician y por eso desarrollan códigos maliciosos para infectar esos equipos y la red a la que están conectados.

4.2.3 Aplicaciones maliciosas

Existe gran diversidad de aplicaciones en el mercado que no cumplen con los parámetros de seguridad básicos, muchas de ellas disponen de códigos binarios que no cuentan con los mecanismos de protección, haciéndolas vulnerables de acceso y modificación.

A parte de las aplicaciones que no cuentan con parámetros de seguridad, están las que se aprovechan de los privilegios dados por los usuarios confiados, que sin saber le están dando permisos amplios a un tercero por medio de la aplicación descargada, y por último están las aplicaciones de proveedores de servicios los cuales se aprovechan de su imagen de seguridad para por medio de sus aplicaciones recolectar datos, para ser utilizados en marketing.

4.2.4 Interfaces web deficientes

Los dispositivos IoT incorporan funcionalidades web mediante las cuales se permite su administración, por tanto pueden existir deficiencias en sus estructuras de código lo cual permite a un atacante afectar dicho recurso de forma remota.[78]

[78] OWASP. Top 10 2014-I1 Insecure Web Interface. [En línea]. 2015. [Consultado octubre 3 de 2017]. Disponible en internet: https://www.owasp.org/index.php/Top_10_2014-I1_Insecure_Web_Interface

4.2.5 Débil autenticación

Los procesos de configuración que se aplican a estos dispositivos no disponen de los métodos ni de la robustez requerida, en muchos casos es común que estos elementos operen con sus configuraciones de fábrica, dejando una puerta abierta para su vulneración.[79]

4.2.6 Canales de comunicación inseguros

Los dispositivos IoT en su gran mayoría disponen de mecanismos que permiten determinar su operatividad, estos servicios de diagnóstico involucra la utilización de puertos que pueden convertirse en agujeros de seguridad, aquí influye las pruebas previas realizadas por el fabricante que como es muy común por el afán de vender no se le presta la importancia requerida.

4.2.7 No cifrado

Una de las características fundamentales de los dispositivos IoT, es el flujo de información que estos manejan y transmiten, por tanto los mecanismos de cifrado deberán ser parte de los mecanismos de seguridad que evite que los datos que viaja a través de ellos no sean interpretados por terceros.

4.2.8 La privacidad

Disponer de mecanismos de seguridad y de una cultura de buenas prácticas, frente a la accesibilidad de los dispositivos del IoT, así como la aplicación de técnicas de cifrado cuando estos se encuentran en un estado de reposo influirá en la minimización de vulnerabilidades.

4.2.9 Entornos de nube virtual

Una de las características de los dispositivos IoT es el entorno virtual que estos utilizan para determinadas funciones, por tanto estas acciones se pueden convertir en una debilidad de seguridad, la cual será aprovechada por algún atacante para vulnerar el dispositivo.

4.2.10 Interfaz de administración móvil.

La mayor parte de los procesos y/o actividades que se realizan a diario, tienen una relación directa con el uso de dispositivos móviles, partiendo de ello, mediante estos

[79] OWASP. Top 10 2014-I2 Insufficient Authentication/Authorization. [En línea]. 2015. [Consultado octubre 3 de 2017]. Disponible en internet: https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization

mecanismos se pueden administrar los dispositivos del IoT que dispongan de estos entornos, allí también se abrirá otra brecha de seguridad, dado que se dispondrá de una interfaz adicional para el control de ellos.

4.2.11 Escasa seguridad

Algunos dispositivos de acuerdo a las funciones para la cual fueron diseñados, no proporcionan ambientes seguros robustos, es decir estarían expuestos a sufrir alguna vulneración, allí prevalece la operatividad frente a la seguridad dado los costos que tendrían aplicar medios de protección avanzada.

4.2.12 Actualización del firmware

Uno de los aspectos que más genera susceptibilidad dadas las consecuencias que pueden generar en el dispositivo si estos no se realizan de la forma adecuada, una mala aplicación podría ser aprovechada por los atacantes si no se tienen en cuenta los parámetros determinados por el fabricante, mediante este proceso los delincuentes podrían vulnerar la seguridad al transmitir alguna aplicación maliciosa.

4.2.13 Renovación tecnológica

Todo dispositivo tecnológico es sujeto a renovación por determinas condiciones, en este sentido aquellos que son removidos de su actividad en algunos casos son puestos a la venta mediante canales electrónicos, allí juega un papel muy importante el tratamiento de los mismos antes de ser entregados a terceros dado que durante su operatividad recolectaron información confidencial la cual deberá ser retirada previamente, por tanto a estos dispositivos deberán incorporar mecanismos de restauración a fabrica que evite que información valiosa la tenga un desconocido.

4.2.14 Estructurar segmentación de red específica para los dispositivos

Las deficiencias de seguridad que presentan los recursos del IoT, pueden desencadenar una afectación total sobre las demás herramientas tecnológicas, informáticas y de información que posea la organización, esto puede llegar a un punto de dejar inoperativa a la organización. Partiendo de ello, una de las estrategias para salvaguardar estos recursos consiste en establecer un segmento de red independiente para los elementos del IoT.

4.2.15 Robustez de credenciales

Es uno de las factores que no se les presta la atención requerida, en ocasiones se manejan las configuraciones por defecto que proporciona el fabricante, sin analizar que es la primera línea a vulnerar por el atacante, por tanto el establecer

mecanismos de autenticación robusta para acceder al recurso, así mismo que estas no sean unificadas para todos los dispositivos.

4.2.16 Actualización del dispositivo

A medida que los atacantes adoptan nuevos mecanismos para vulnerar los recursos o identifican deficiencias dentro de ellos, en gran parte son materializados dada la falta de implementación de procesos automatizados que permitan mantener parcheados el software del dispositivo, allí la importancia de establecer políticas para la actualización de estos recursos.

4.2.17 Restricción de uso de dispositivos personales

La organización debe limitar el uso de dispositivos del IoT de connotaciones personales o establecer entornos en los cuales puedan ser utilizados sin que interactúen dentro del segmento de producción.

4.2.18 Conecte solo lo que necesite

Determinar hasta qué punto el dispositivo o su estructura operativa requiere mantener una conexión con la red mundial de forma continua, para ello se debe evaluar las características y funcionalidades que este ofrece, dependiendo de ello tome las acciones requeridas.

4.2.19 Protocolos de comunicación

La mayor parte de dispositivos disponen de protocolos que permiten a dichos elementos establecer una comunicación mediante el descubrimiento y detección entre sí, estos mecanismos sin las medidas pertinentes se convierten en objeto de ataque por los delincuentes informáticos, donde su accionar puede trascender a los demás recursos aprovechando la deficiencia de este protocolo. Por tanto la inhabilitación de este servicio es la medida más efectiva para contrarrestar la deficiencia de seguridad.

4.2.20 Seguimiento del recurso

Las organizaciones deben de disponer de políticas para la inspección de los dispositivos que se integran a la infraestructura de red y establecer acciones para controlar el tráfico que sobre ella se aplica. Una constante verificación en la operatividad y configuración de estas herramientas, minimizan el accionar delictivo, con ello se tendrá un ambiente seguro prevaleciendo la integridad, confidencialidad y disponibilidad de todos los recursos de la compañía.

4.2.21 Entornos y servicios de la nube

La gran mayoría de dispositivos del IoT operan bajo entornos dispuestos en ambientes de nube virtual, esto permite que establezcan una comunicación para cumplir con las funciones para lo cual fueron diseñados o realizar alguna tarea específica. Este factor debe ser debatido y analizado antes de incorporar estas herramientas, y establecer el alcance de protección que proporcionaran frente a los recursos que maneje.

4.2.22 Conozca los dispositivos

Los dispositivos del IoT tienen integración de diversos fabricantes y desarrolladores para su construcción, esto los convierte en un factor de riesgo potencial y objetivo principal de los delincuentes informáticos. Por tanto el determinar y conocer al detalle las estructuras, entornos, mecanismos de seguridad y la forma en cómo opera cada dispositivo evitara situaciones de vulnerabilidad sobre los recursos de la organización.

4.3 PRODUCCIÓN EN MASA DE IOT

Como ya es sabio el gigante asiático es, es el productor en masa más grande del mundo, cosa que hace felices a las personas por sus bajos precios, pero vulnerables a muchos debido la falta de estándares lo cual supone una amenaza para IoT.

Pero la otra cara de la moneda es que IoT conlleva ciertos riesgos que todavía no se comprenden del todo. Enzo Taibi, socio de Consultoría en IT de PwC Argentina comenta: "Muchos ejecutivos creen que el ecosistema IoT propiciará el crecimiento económico, a partir de la transformación de los modelos de negocios y la innovación en productos y servicios. Pero los riesgos asociados también podrían amenazar la seguridad de los datos, atravesando virtualmente todas las industrias y haciéndolas más vulnerables a interferencias maliciosas con graves consecuencias".

Las empresas recopilan y analizan una gama cada vez más amplia de información, y su compilación puede proporcionar información personal sensible sobre los consumidores, habilitando situaciones que podrían comprometer la ética de su uso. Las empresas que extraen datos personales con fines no transparentes o que comparten datos personales con terceros sin la debida notificación corren el riesgo de incurrir en prácticas que violan las normas de protección y seguridad del consumidor.

Según Diego Taich, director de Consultoría en IT de PwC Argentina "Para acompañar el avance de IoT será crucial un programa integrado de seguridad informática. Las empresas que alineen el desarrollo e implementación de productos

y sistemas de IoT con estándares de seguridad informática y protección de datos contarán con una significativa ventaja para materializar los beneficios de esa tecnología".

El gran desafío es la complejidad del ecosistema IoT, que impide que la mayoría de las empresas elaboren un marco de seguridad y privacidad. A diferencia de los equipos de TI, los dispositivos conectados no fueron diseñados pensando en la seguridad, y muchos de ellos no poseen capacidades esenciales como encriptación o autenticación.

El estudio Global State of Information Security -que PwC realizó con la participación de más de 10.000 ejecutivos de TI en 133 países- concluye que las empresas están comenzando a ocuparse de la seguridad de IoT, aunque todavía queda mucho por mejorar. Un 35% de los encuestados informaron que su organización posee una estrategia de seguridad IoT en marcha, y un 28% confirmó que avanzaron en su implementación.

La mayor parte de estas organizaciones pertenecen a los sectores de telecomunicaciones (78%), tecnología (73%) y automotriz (69%). Al mismo tiempo, el 46% de los entrevistados planea invertir en seguridad de IoT durante los próximos doce meses, fundamentalmente en el sector de automotriz (55%), productos industriales (55%) y tecnología (53%).

"Creemos que las tecnologías de seguridad existentes se van a extender rápidamente para administrar y proteger el flujo de datos en las redes de IoT. Nuestra recomendación es que las organizaciones abran el diálogo con sus socios tecnológicos, para desarrollar, a partir de las herramientas actuales, un camino hacia la identificación, la seguridad y la gestión de los datos producidos o procesados por IoT", concluye Taibi.

La nueva revolución tecnológica el “IoT”, ya hace parte de innumerables procesos que se desarrollan al interior de las organización y en el entorno cotidiano, cada día el crecimiento y conectorización de elementos que se utilizaban para determinadas labores de forma rudimentaria, pasaron a un ambiente autónomo que basado en el uso de sensores y recolección de parámetros llevan a cabo una acción específica de forma automática. Ante ello, el incremento de estos dispositivos conectados a la red mundial, es proporcional a la preocupación frente a la privacidad y seguridad de los datos que recolectan dichos recursos, estos ataques se pueden catalogar dentro del grupo de tipo físico, de software, de red o cifrado.

4.3.1 Riesgos de tipo físico

Se fundamenta en vulnerar el hardware afectando los sensores que posee el sistema IoT o en su defecto se imparten acciones para limitar la operatividad y

efectividad del recurso. Para llevar a cabo la afectación, el atacante requerirá establecer un acercamiento a la ubicación del dispositivo, así mismo si el accionar es efectivo, se podrá alterar los dispositivos sensores centralizados y obtener el control de los mismos, con lo que se permitirá la extracción de datos y códigos. También podrán replicar e inyectar dentro del recurso, sensores maliciosos que operaran en conjunto con los reales, teniendo un control total de todo lo que se transmite.

Por otra parte, este tipo de inyección maliciosa puede llegar al punto de dañar físicamente el dispositivo e interrumpir sus servicios, tomando el control del sistema este tiene un alcance de afectación sobre los recursos que son controlados por los dispositivos IoT, sus almacenes de datos e infraestructura sobre la cual operan.

Otro aspecto de la afectación, contempla la alteración de los procesos a través del cual los usuarios quedan a merced de los atacantes, quienes con los métodos de afectación buscaran satisfacer sus propósitos delictivos.

Frente a la forma en que operan los dispositivos, incorporan estados de suspensión para alargar la duración de su mecanismo de energía, allí los delincuentes toman y forzan estos medios para provocar un estado de cesación de actividades, con lo cual se trasladara el consumo de energía a los sensores principales que terminaran por apagarse.

4.3.2 Riesgos a nivel de software

Su principal accionar está fundamentado en la utilización de herramientas de software y es mediante ello que se generan la mayor cantidad de riegos sobre los dispositivos IoT, una vez son ejecutados tienen el alcance de explotar la totalidad del sistema, sustraer datos relevantes, modificar información, interrumpir la operatividad y hasta el punto de causar daño al dispositivo.

Esta afectación vulnerara tanto el recurso como al usuario que interactúa con el dispositivo, esto dado que se pueden emplear ataques en los cuales se engañe al victimario, para que este proporcione información confidencial, por otra parte estarán las acciones donde se incorporen el uso de programas maliciosos, troyanos, virus, gusanos con la finalidad de afectar datos, alterar procesos del sistema, extraer información o monitorear el flujo de transacciones que se llevan a cabo.

4.3.3 Riesgos a nivel de red

Dentro de este ámbito, el objetivo del atacante es afectar el recurso a través de la capa de red del dispositivo IoT el cual lo puede llevar a cabo de forma remota, este es uno de los riesgos más notables para dichos recursos. A través de la utilización de herramientas de vulneración se desbordará la capacidad de recepción de

solicitudes provocando la saturación y posterior denegación de servicios. Así mismo se emplean aplicaciones para rastrear el tráfico que generan los dispositivos, buscando deducir patrones de comunicación entre estos elementos.

- **Vulneración de accesos, suplantación de identidad y clonación**. Los ataques llevados cabo mediante la afectación y descubrimiento de la fuente de comunicación RFDI que poseen estos dispositivos, incorporan técnicas de clonación, spoofing y accesos no autorizados. A través de cada una de ellas se aplican acciones diversas, para el caso de la clonación se genera cuando el atacante reproduce la información de etiquetas reales para obtener acceso al sistema IoT, empleando el spoofing se suplanta la comunicación RFDI para interpretar y capturar datos transmitidos, y por último los delincuentes buscaran vulnerar el acceso aprovechando las deficiencias de seguridad del recurso teniendo el control para alterar, eliminar y modificar datos.

- **Esquemas de sumidero**. Este ataque tiene el fundamento en vulnerar la confidencialidad de los datos que transmiten los dispositivos, allí mediante la afectación de los nodos atraerán el tráfico de paquetes para posterior truncamiento del servicio de red e impedir que estos llegue a su destino.

  También buscaran atraer a nodos vecinos mediantes aquellos que han sido comprometidos, permitiendo que el tráfico pueda ser modificado, reenviado o eliminado según criterios del atacante, afectando la confidencialidad del recurso y su entorno.

- **Man-in-the-Middle**. Esta intrusión se ejecuta mediante el uso de los protocolos de comunicación de red que utilizan los dispositivos IoT, donde se interfiere la conexión entre los dos nodos y se engaña al otro punto haciéndole creer que es una instrucción legitima, una vez se efectúa el ataque el ente ejecutor tendrá opciones para controlar, supervisar y escuchar las comunicaciones entre determinado nodo quedando a merced de cualquier afectación.

4.3.4 Riesgos a nivel de cifrado

Los esquemas de cifrado que poseen los dispositivos IoT, también hacen parte de los objetivos a vulnerar, este método pretende no atacar directamente al algoritmo de cifrado si no que buscara afectar al medio de implementación de dicho mecanismo de protección. También se emplean técnicas en las cuales se tratara de descifrar las claves del cifrado tomando los parámetros que utiliza para su construcción y el estado que adopta el dispositivo durante el proceso.

Adicional a ello, estos esquemas de cifrado también pueden estar sujetos a ser afectados por ataques Man-in-the-Middle, en el cual se intercepta la comunicación

entre los nodos descifrando los paquetes a través de las claves compartidas donde el usuario asume que esta interactuando con ambientes legítimos.

4.4 RIESGOS DE LOS ELEMENTOS QUE COMPONEN IOT

En la tabla 23, se muestran los diferentes riesgos a que se exponen los elementos que hacen parte del IoT y que se enmarcan dentro del tipo de [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE), así mismo se puede ver la representación en el anexo 1.

Tabla 23. Riesgos - [HW] EQUIP. INFORMÁTICO (HARDWARE)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
[peripheral]	Sensores	[N1] Fuego	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[N2] Daños por agua	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[I5] Avería de origen físico o lógico	Interrupción de los procesos, perdidas económicas
		[I3] Contaminación mecánica	No se obtengan datos precisos, daños de dispositivo, interrupción de procesos
		[I7] Condiciones inadecuadas de temperatura o humedad	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[E4] Errores de configuración	Inoperatividad del dispositivo, no disponibilidad del servicio
		[E23] Errores de mantenimiento / actualización de equipos (hardware)	Daño en dispositivo, no disponibilidad de servicios
		[A4] Manipulación de la configuración	Interrupción de los procesos, perdidas económicas
		[A11] Acceso no autorizado	No disponibilidad de servicio, pérdidas económicas
		[A23] Manipulación de los equipos	Daño en dispositivo, no disponibilidad de servicios
		[A25] Robo	Interrupción de los procesos, perdidas económicas
	Placas de Desarrollo	[N1] Fuego	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[N2] Daños por agua	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[I5] Avería de origen físico o lógico	Interrupción de los procesos, perdidas económicas
		[I3] Contaminación mecánica	Deficiencia en la operatividad, daños de dispositivo, interrupción de procesos

Tabla 23. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
[peripheral]	Placas de Desarrollo	[I7] Condiciones inadecuadas de temperatura o humedad	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[E4] Errores de configuración	Inoperatividad del dispositivo, no disponibilidad del servicio
		[E8] Difusión de software dañino	Daño de dispositivo, interrupción de procesos
		[E23] Errores de mantenimiento / actualización de equipos (hardware)	Daño en dispositivo, no disponibilidad de servicios
		[E24] Caída del sistema por agotamiento de recursos	No disponibilidad de servicios, perdidas económicas
		[A4] Manipulación de la configuración	Interrupción de los procesos, perdidas económicas
		[A11] Acceso no autorizado	No disponibilidad de servicio, pérdidas económicas
		[A23] Manipulación de los equipos	Daño en dispositivo, no disponibilidad de servicios
		[A25] Robo	Interrupción de los procesos, perdidas económicas
		[A26] Ataque destructivo	Daño en dispositivo, perdidas económicas
	Actuadores	[I1] Fuego	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[I2] Daños por agua	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[I5] Avería de origen físico o lógico	Interrupción de los procesos, perdidas económicas
		[I7] Condiciones inadecuadas de temperatura o humedad	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[I8] Fallo de servicios de comunicaciones	Interrupción de los procesos, perdidas económicas
		[A23] Manipulación de los equipos	Daño en dispositivo, no disponibilidad de servicios
		[A25] Robo	Interrupción de los procesos, perdidas económicas
[network]	Gateway / Hub	[I1] Fuego	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[I2] Daños por agua	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[I5] Avería de origen físico o lógico	Interrupción de los procesos, perdidas económicas
		[I6] Corte del suministro eléctrico	Daño de dispositivo, interrupción del servicio, perdidas económicas

Tabla 23. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
network	Gateway / Hub	[I7] Condiciones inadecuadas de temperatura o humedad	Daños de dispositivo, pérdidas económicas, no disponibilidad de servicios
		[I8] Fallo de servicios de comunicaciones	Interrupción de los procesos, perdidas económicas, perdida de datos
		[E2] Errores del administrador	Perdida de datos, afectación del servicio
		[E4] Errores de configuración	Inoperatividad del dispositivo, no disponibilidad del servicio
		[E8] Difusión de software dañino	No disponibilidad del servicio, perdida de datos
		[E23] Errores de mantenimiento / actualización de equipos (hardware)	Daño en dispositivo, no disponibilidad de servicios
		[E25] Pérdida de equipos	Perdidas económicas, interrupción del servicio
		[A4] Manipulación de la configuración	Interrupción de los procesos, perdidas económicas
		[A6] Abuso de privilegios de acceso	Perdida de datos, alteración del proceso
		[A8] Difusión de software dañino	Daño de dispositivo, interrupción de procesos
		[A12] Análisis de tráfico	Perdida de datos, vulneración de información confidencial
		[A24] Denegación de servicio	Interrupción del proceso, perdidas económicas

Fuente: Los autores

En la tabla 24, se muestran los diferentes riesgos a que se exponen los elementos que hacen parte del IoT y que se enmarcan dentro del tipo de [COM] Redes de comunicaciones, así mismo se puede ver la representación en el anexo 2.

Tabla 24. Riesgos - [COM] Redes de comunicaciones

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
[wifi] / [mobile]	Conectividad inalámbrica "Tecnología Tradicional" / Tecnología de	[I8] Fallo de servicios de comunicaciones	Interrupción de los procesos, perdidas económicas, perdida de datos
		[E4] Errores de configuración	Inoperatividad del dispositivo, no disponibilidad del servicio
		[A4] Manipulación de la configuración	Interrupción de los procesos, perdidas económicas
		[A11] Acceso no autorizado	No disponibilidad de servicio, pérdidas económicas

Tabla 24. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
[wifi] / [mobile]	Conectividad inalámbrica "Tecnología Tradicional" / Tecnología de	[A14] Interceptación de información (escucha)	Perdida de datos, afectación del servicio
		[A24] Denegación de servicio	Interrupción del proceso, perdidas económicas

Fuente: Los autores

En la tabla 25, se muestran los diferentes riesgos a que se exponen los elementos que hacen parte del IoT y que se enmarcan dentro del tipo de [Media] Soportes de información, así mismo se puede ver la representación en el anexo 3.

Tabla 25. Riesgos - [Media] Soportes de información

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
[vdisk]	Nube inteligente	[I5] Avería de origen físico o lógico	Interrupción de los procesos, perdidas económicas
		[I8] Fallo de servicios de comunicaciones	Interrupción de los procesos, perdidas económicas, perdida de datos
		[I10] Degradación de los soportes de almacenamiento de la información	Interrupción de los procesos, perdida de datos
		[E1] Errores de los usuarios	Alteración de datos, afectación del servicio, perdida de datos
		[E2] Errores del administrador	Interrupción del servicio, daño del entorno de almacenamiento, perdida de datos
		[E4] Errores de configuración	No disponibilidad del servicio, afectación de datos, perdida de datos
		[E8] Difusión de software dañino	Interrupción de procesos, perdida de datos
		[E14] Escapes de información	Perdidas económicas, afectación del entorno, exposición del recurso
		[E21] Errores de mantenimiento / actualización de programas (software)	Exposición del recurso, afectación del servicio, perdida de datos
		[A4] Manipulación de la configuración	Interrupción de los procesos, perdidas económicas
		[A5] Suplantación de la identidad del usuario	Afectación del entorno, perdida de datos, interrupción de procesos
		[A6] Abuso de privilegios de acceso	Perdida de datos, alteración del proceso
		[A7] Uso no previsto	Daño del entorno de trabajo, interrupción del servicio, perdida de datos, perdidas económicas
		[A8] Difusión de software dañino	Daño de dispositivo, interrupción de procesos

Tabla 25. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
[vdisk]	Nube inteligente	[A11] Acceso no autorizado	No disponibilidad de servicio, pérdidas económicas
		[A18] Destrucción de información	Perdidas económicas, afectación del entorno
		[A19] Divulgación de información	Exposición del recurso, perdidas económicas
		[A24] Denegación de servicio	Interrupción del proceso, perdidas económicas

Fuente: Los autores

En la tabla 26, se muestran los diferentes riesgos a que se exponen los elementos que hacen parte del IoT y que se enmarcan dentro del tipo de [SW] Software - Aplicaciones informáticas, así mismo se puede ver la representación en el anexo 4.

Tabla 26. Riesgos - [SW] Software - Aplicaciones informáticas

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
[sub]	Plataforma	[I8] Fallo de servicios de comunicaciones	Interrupción de los procesos, perdidas económicas, perdida de datos
		[I10] Degradación de los soportes de almacenamiento de la información	Interrupción de los procesos, perdida de datos
		[E1] Errores de los usuarios	Alteración de datos, afectación del servicio, perdida de datos
		[E2] Errores del administrador	Interrupción del servicio, daño del entorno de almacenamiento, perdida de datos
		[E4] Errores de configuración	No disponibilidad del servicio, afectación de datos, perdida de datos
		[E8] Difusión de software dañino	Interrupción de procesos, perdida de datos
		[E14] Escapes de información	Perdidas económicas, afectación del entorno, exposición del recurso
		[E20] Vulnerabilidades de los programas (software)	Perdidas de datos, afectación del servicio
		[E21] Errores de mantenimiento / actualización de programas (software)	Exposición del recurso, afectación del servicio, perdida de datos
		[A4] Manipulación de la configuración	Interrupción de los procesos, perdidas económicas
		[A5] Suplantación de la identidad del usuario	Afectación del entorno, perdida de datos, interrupción de procesos
		[A6] Abuso de privilegios de acceso	Perdida de datos, alteración del proceso

Tabla 26. (Continuación)

CÓDIGO DE ACTIVO	ACTIVO	AMENAZAS	RIESGOS
[sub]	Plataforma	[A7] Uso no previsto	Daño del entorno de trabajo, interrupción del servicio, perdida de datos, perdidas económicas
		[A8] Difusión de software dañino	Daño de dispositivo, interrupción de procesos
		[A11] Acceso no autorizado	No disponibilidad de servicio, pérdidas económicas
		[A15] Modificación deliberada de la información	Perdidas económicas, afectación de procesos
		[A18] Destrucción de información	Perdidas económicas, afectación del entorno
		[A19] Divulgación de información	Exposición del recurso, perdidas económicas
		[A24] Denegación de servicio	Interrupción del proceso, perdidas económicas
		[A26] Ataque destructivo	Perdidas económicas, afectación del entorno
		[A30] Ingeniería social (picaresca)	Perdida de datos, afectación del entorno

Fuente: Los autores

4.5 MECANISMOS PARA MINIMIZAR LAS VULNERABILIDADES DE LOS ELEMENTOS QUE COMPONEN IOT

Estas acciones contribuyen a disponer de entornos de producción bajo estándares de seguridad, minimizando la materialización de afectaciones.

En la tabla 27, se muestran algunas pautas para minimizar las vulnerabilidades sobre los dispositivos inteligentes.

Tabla 27. Seguridad para dispositivos inteligentes

	ESTRATEGIAS DE SEGURIDAD
Dispositivos inteligentes	Desactivación de la conectividad de dispositivos externos por ejemplo, unidades USB y permitiendo su uso sólo previa aprobación, revisión, análisis y sobre la base de lo necesario
	Deshabilitar el acceso directo de Internet del dispositivos sensibles o puntos finales
	Asegurar que los servicios que no sean requeridos estén deshabilitados o bloqueados "puertos abiertos, protocolos inseguros"
	Habilite mecanismos de inicio seguro mediante el uso de llaves cifradas y firmware seguro
	Soporte de autenticación del dispositivo al conectar

Tabla 27 (Continuación)

	ESTRATEGIAS DE SEGURIDAD
Dispositivos inteligentes	Aplicar parches regulares al software del dispositivo
	Ejecute actualizaciones de firmware de forma segura y autenticada
	Aplique listas blancas de conexiones en lugar de listas negras
	Adopte mecanismos de intercambio de claves seguras

Fuente: Los autores

En la tabla 28, se muestran algunas pautas para minimizar las vulnerabilidades en los medios de interconexión y canales de transmisión.

Tabla 28. Seguridad para medios de interconexión y canales de transmisión

MEDIOS DE INTERCONEXIÓN Y CANALES DE TRANSMISIÓN	ESTRATEGIAS DE SEGURIDAD
Seguridad en el Gateway	Asegúrese de que la puerta de enlace IoT / M2M esté protegida contra intrusiones y malware mediante el uso de mecanismos apropiados, como ACL, IPS, filtrado, etc.
Seguridad física y de red	Las instalaciones deberían tener una seguridad física adecuada, como guardias de seguridad, tarjetas de acceso, registros de visitantes, cámaras CCTV, zonas seguras, etc. para prevenir accesos no autorizados
	Deben aprovecharse los mecanismos de seguridad apropiados para aislar información sensible con segmentos como IDS / IPS, firewalls, red ACL, etc.
	El proveedor de servicios debe contar con certificaciones de aseguramiento tales como ISO 27001, sellos de privacidad, etc.
Seguridad de acceso remoto	Permitir una sólida autenticación por ejemplo la autenticación multifactor (MFA), para el acceso remoto a los usuarios privilegiados como los administradores, personal de mantenimiento, para iniciar sesión de forma segura desde fuera de la red
	El uso de canales de comunicación seguros, tales como VPNs-S2S, C2S para acceso a empleados regulares a la red de la empresa desde las sucursales, estos accesos de deshabilitan cuando ya no se requiera.
Seguridad de las comunicaciones inalámbricas	El uso de configuraciones seguras cuando se comunican a través de las redes inalámbricas; dispositivos/sensores por la puerta de enlace.
	Cumplimiento de las autenticaciones y cifrados.

Fuente: Los autores

En la tabla 29, se muestran algunas pautas para minimizar las vulnerabilidades en los entornos de facilitación.

Tabla 29. Seguridad para entornos de facilitación

ENTORNO DE FACILITACIÓN	ESTRATEGIAS DE SEGURIDAD
Seguridad de la nube	Los entornos virtuales necesitan seguridad y cuidado, por ejemplo: dureza del software huésped, parches, actualizaciones, etc.
	El acceso a los entornos virtuales, las aplicaciones en ella necesitan tener fuerte mecanismos de control
	La seguridad de datos en la nube debe tener tecnologías apropiadas y algoritmos de cifrados acordes al proceso a realizar, incluyendo fuertes algoritmos de administración de claves.
	Soluciones de continuidad del negocio y recuperación ante desastres deben diseñarse como instantáneas para los entornos virtuales y los datos de la misma, aprovechando los respaldos externos, teniendo máquinas virtuales en modo de espera en otros servicios de la nube, dentro de la misma región del proveedor.
	Protección del entorno web frente a instancias en la nube con IDS/IPS, firewall basados en host, etc. Para inspeccionar trafico malicioso detección/prevención
	Monitoreo de acceso a los recursos especialmente para usuarios con privilegios y administración de sesiones integrando los múltiples registros con soluciones SIEM (Información de Seguridad y administración de Eventos) para la correlación y análisis de incidentes de seguridad.

Fuente: Los autores

En la tabla 30, se muestran algunas pautas para minimizar las vulnerabilidades en las plataformas de integración.

Tabla 30. Seguridad para plataformas de integración

PLATAFORMA DE INTEGRACIÓN	ESTRATEGIAS DE SEGURIDAD
Seguridad de las aplicaciones	Aplicaciones (pueden ser web, móvil, nube, etc.) deben ser desarrolladas con los lineamientos seguros de codificación teniendo en cuenta el estandar estándar de las industrias como OWASP, SAFEcode, SANS Institute/CWE, etc., para minimizar el riesgo de ataques a las aplicaciones.
	Ejemplo prevención del SQL inyección, XSS, fuga de datos, sesión de repetición, ataques de desbordamiento de buffer, etc.
	Aprovechamiento de las mejores prácticas tales como restricción de archivo, validación de entrada, etc.
	Pruebas de pent-test (dinámicas, estáticas, hibridas) para detectar vulnerabilidades en las aplicaciones y tomar acciones correctivas para solucionarlas.
	Utilizar código firmado para asegurar a los clientes sobre la autenticidad del software, así como el no-repudio.

Tabla 30. (Continuación)

PLATAFORMA DE INTEGRACIÓN	ESTRATEGIAS DE SEGURIDAD
Monitoreo de la integridad	La estructura de archivos críticos deben ser monitoreados para detectar cualquier alteración o cambio no autorizado, por ejemplo: archivo de configuración, el tráfico debe ser monitoreado para detectar cualquier cambio deliberado o accidental.
	Adopción de procedimientos que serán una herramienta para monitorear la integridad del recurso y prevenir o alertar lo expuesto con anterioridad.
	Robustecer los procesos de aprobación de cambios y revisión.

Fuente: Los autores

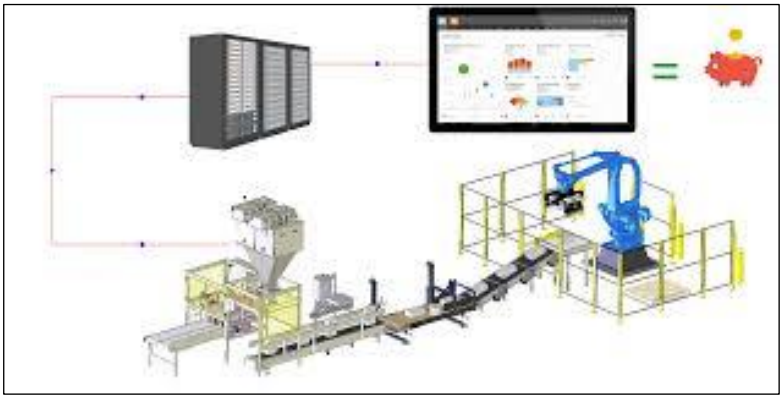
5. CONTROLES PARA EL BUEN USO DE LAS HERRAMIENTAS QUE ESTÁN DENTRO DE INTERNET DE LAS COSAS (IoT).

Disponer de controles frente al uso de los dispositivo IoT, proporcionan ambientes de seguridad al momento de realizar alguna interacción tanto a nivel de los usuarios como entre cada elemento, ello generara un protección en todos los entornos, minimizando vulnerabilidades y otorgar una mayor integridad, disponibilidad y confidencialidad de los recursos asociados.

5.1 CONTROL EN LA MANUFACTURA INTELIGENTE.

Aunque el concepto es viejo y algunos lo confunden con la revolución industrial, la automatización poco tiene que ver con esto, ya que se trata del servicio o función de una máquina o una parte de ella pueden mejorar antes de que se presente una falla, eliminando así los costosos tiempos de inactividad y eventualidades no previstas, para mayor interpretación se puede observar la Ilustración 37.

Ilustración 37. Manufactura inteligente



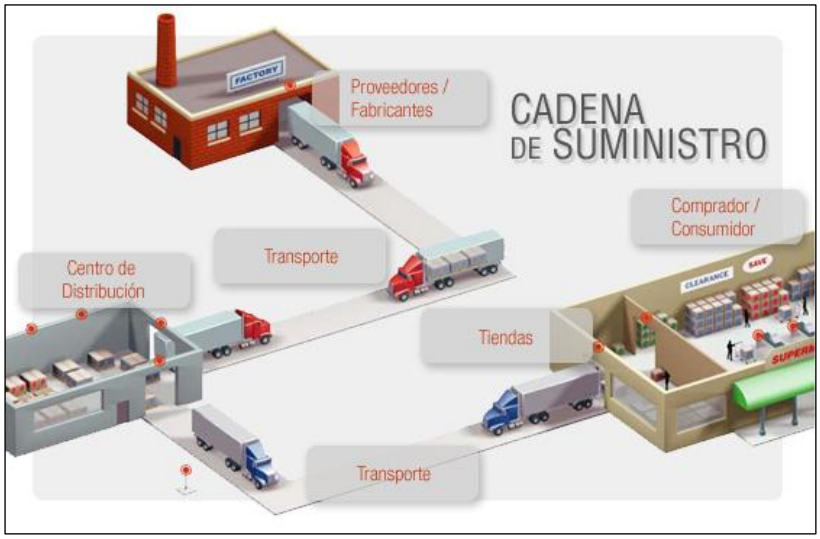
Fuente: Grupo Gersa Monterrey. Manufactura Inteligente. [En linea]. SF. [Consultado el 31 de octubre de 2017]. Disponible en internet: http://gersa.com.mx/es/productos-y-soluciones/manufactura-inteligente/

El servicio o función de una máquina o una parte de ella pueden mejorar antes de que se presente una falla, eliminando así los costosos tiempos de inactividad y eventualidades no previstas.

5.2 CONTROL EN LAS CADENAS INTELIGENTES DE SUMINISTRO.

Proporcionando información en tiempo real de la oferta, demanda y envíos a los clientes. Las entregas pueden ser rastreadas y recuperadas si son extraviadas o robadas. (Ver ilustración 38).

Ilustración 38. Cadenas inteligentes de suministro



Fuente: NAVARRO, Javier. Qué es la cadena de suministro: entendiendo mejor el concepto. [En línea]. 2015. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://www.deustoformacion.com/blog/empresa/que-es-cadena-suministro-entendiendo-mejor-concepto

5.3 CONTROL INFRAESTRUCTURAS INTELIGENTES.

Las oficinas inteligentes contribuyen a generar ahorros de energía, mejorar el auto sustentabilidad y potenciar la colaboración entre los empleados, un ejemplo claro se puede observar en la Ilustración 39.

Ilustración 39. Infraestructuras inteligentes

Fuente: Kuzu Decoletaje. La Internet de las Cosas (IoT) y el futuro de la industria. [En línea]. 2017. [Consultado en internet el 23 de marzo de 2018]. Disponible en internet: http://kuzudecoletaje.es/la-internet-de-las-cosas-iot-y-el-futuro-de-la-industria/

El auge de las tecnologías de la información a través del tiempo, ha permitido que estas sean parte esencial para el desarrollo de los procesos al interior de las organizaciones, siendo eje central para el cumplimiento de objetivos y satisfacción de los usuarios; este mercado tecnológico accesible por cualquier ciudadano también abrió la brecha para la exposición de recursos vitales y confidenciales como lo es la información, la cual es aprovechada por los delincuentes informáticos, para retener datos y obtener algún beneficio económico por su devolución, donde este último no siempre se lleva a cabo. A raíz de ello, las instituciones se han concientizado para brindarles a dichas organizaciones de los mecanismos normativos, metodológicos y legales, con el fin de que se implementen dentro de ellas políticas sólidas que minimicen la exposición de los activos tanto a nivel interno como externo.

Partiendo de ello, estas exposiciones de seguridad que se presentan dentro de las organizaciones y en especial con las que involucran a los dispositivos del IoT, es primordial establecer un marco de controles y/o procedimientos estructurados que permitan asegurar la disponibilidad, integridad y confidencialidad de los recursos de información que son recopilados y manejados a través de estas herramientas.

Bajo estas premisas, se debe tener presente las metodologías diseñadas para controlar y mitigar los riesgos, entre este tipo de modelos se encuentran:[80]

- **OCTAVE**. Esta metodología tiene como fundamento el estudio de los riesgos organizacionales específicamente en los aspectos que surgen en el día a día, un aspecto básico de este método es que se preocupa por el uso que se le da a los recursos tecnológicos e informáticos. Su punto de partida inicia con la identificación de los activos que tiene injerencia con la información.

- **MAGERIT**. Se fundamenta en el uso aplicado sobre las tecnologías de la información, para lo cual dispone de un método para analizar las actividades realizadas sobre estas herramientas y a partir de ello aplicar los controles de acuerdo a las situaciones presentadas para lograr su mitigación.

- **MEHARI**. Tiene como base realizar el estudio de los riesgos bajos los principios de la confidencialidad, integridad y disponibilidad.

- **NIST SP 800 – 30**. Establece un conjunto de criterios en los cuales establece una serie de recomendaciones y acciones en busca de realizar una gestión adecuada de los riesgos.

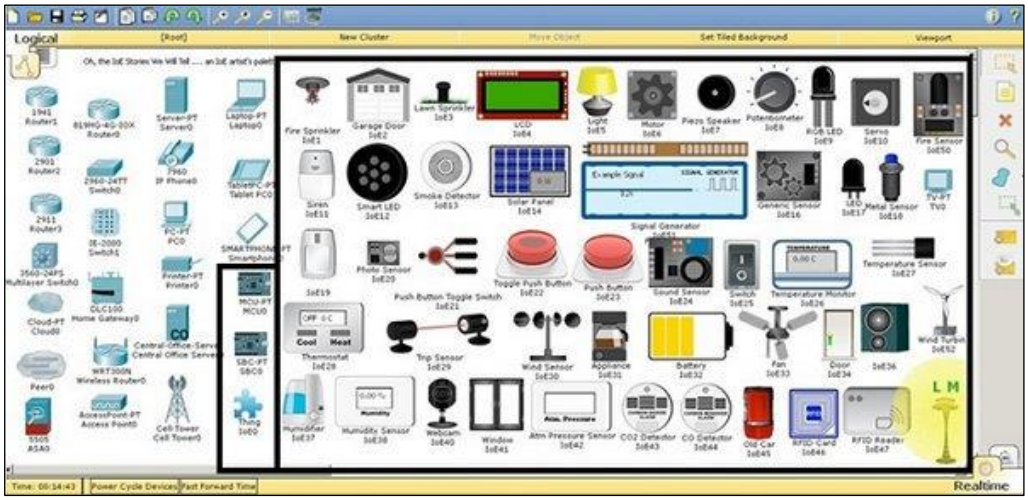
[80] HUERTA, Antonio. Introducción al análisis de riesgos – Metodologías (II). [En línea]. 2012. [Consultado el 31 de octubre de 2017]. Disponible en internet:https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

- **CORAS**[81]. Se fundamenta en los procesos donde la seguridad de los sistemas es crítica, a partir de sus procesos se detectan deficiencias de seguridad, debilidades, redundancia y se identifican vulnerabilidades, todo ello basado en sus siete fases presentación, análisis de alto nivel, aprobación, identificación de riesgos, estimación de riesgo, evaluación de riesgo y tratamiento del riesgo.

Para comprender la gran problemática que se teje tras el IoT en las organizaciones, debemos empezar por enumerar la aplicabilidad de IoT en la empresa, ya que en este mundo de la automatización, las cosas siempre han estado, al servicio de que las ha requerido, llevándonos a preguntar ¿Cuáles con los alcances de IoT empresarial? Básicamente se puede listar todo un abanico de posibilidades, donde sobresalen las siguientes:

Un claro ejemplo de solución se da en la utilización, de la herramienta Packet Tracer como se observa en la ilustración 40, un software que nos permite la simulación de redes en este caso donde se identifica de antemano IoT, con esto pudiendo anticiparnos a los posibles riesgos que se generan al instalar tecnología sin protección, o que por motivos de fabricación en masa, no cumplen los protocolos de seguridad necesarios. (Ver ilustración 41).

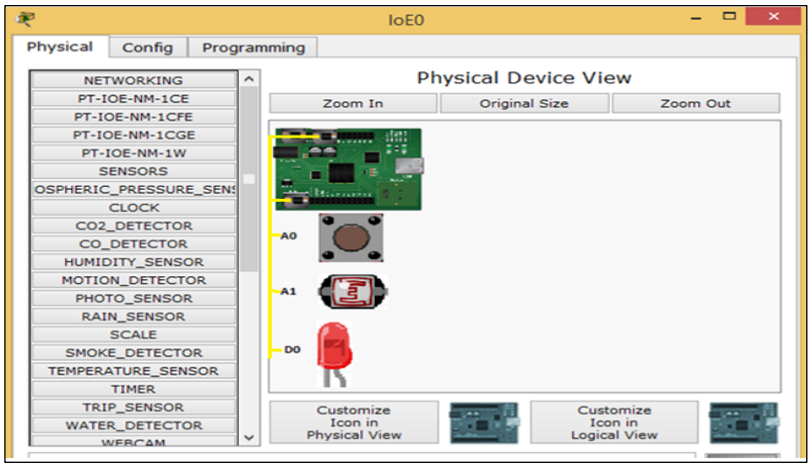
Ilustración 40. Simulación de redes



Fuente: BAUTISTA, Ángelo. CISCO Plus(+) Tecnología en Redes de Computadores. [En línea]. 2016. [Consultado el 27 de marzo de 2018]. Disponible en internet: https://ciscoplus.wordpress.com/2016/06/

[81] ALEMÁN, Helena; RODRÍGUEZ, Claudia. Metodologías Para el Análisis de Riesgos en los SGSi. [En línea]. 2015. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Ilustración 41. Dispositivos IoT



Fuente: Cisco Systems. What's new in Cisco Packet Tracer 7.0. [En linea]. 2018. [Consultado el 23 de marzo de 2018]. Disponible en internet: http://www.packettracernetwork.com/features/packettracer-7-newfeatures.html

5.4 CREAR UN SERVIDOR IOT

5.4.1 Qué es un servidor IoT y para qué sirve

La creación de un servidor que pueda receptar toda la información generada por IoT dentro de la organización, se convierte en uno de los factores clave de la transformación digital que progresivamente da soluciones prácticas, para enfrentar los problemas de seguridad a los que nos enfrentarnos los próximos años, con el crecimiento de la utilización y puesta en marcha de IOT

El servidor cumple una tarea fundamental a la hora de asegurar y convertir los datos emitidos por la infraestructura inteligente, puesto que es el sistema encargado de la información para el correcto funcionamiento de la organización.

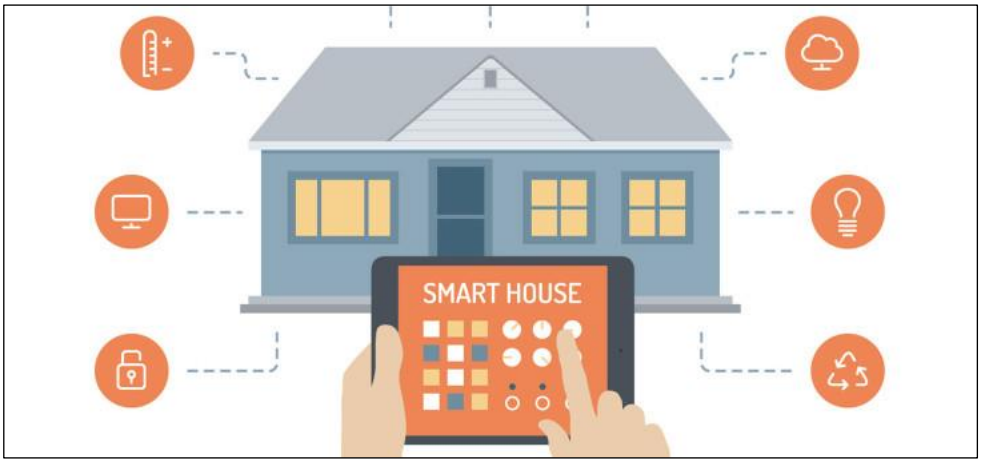
De ahí que se constituya un ámbito inmerso en la evolución y que trata de perfeccionarse poco a poco y llegar a una de las más novedosas fases, como el servidor cloud o los servidores en la nube. Unas herramientas indispensables para mejorar la competitividad y gestión de las corporaciones.

5.4.2 Domotización como solución

La posibilidad de controlar todo desde un solo punto, es excelente solución de logística, pero para que sea una solución fiable se deben de comprender políticas de seguridad en la creación de una aplicación propia, dado que las organizaciones tiene problemáticas diferentes y se hace necesario que el manejo de sus datos se

realice de forma personalizada, cerrándole las puertas a los delincuentes que desean dichos datos de forma ansiosa, como se observa en la ilustración 42.

Ilustración 42. Domotización



Fuente: Vemedia. ¿Qué es domótica? – Su definición, concepto y definición. [En línea]. 2015. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://conceptodefinicion.de/domotica/

A continuación, se presenta un proceso de domótica, en el cual aparte de bajos costos, se puede apreciar como es la correcta configuración y seguimiento de protocolos dentro de IoT.

En la tabla 31, se muestran los costos de los elementos que se emplean para un proceso de domótica.

Tabla 31. Costos

Placa	Arduino Mega 2560R3	22 USD
Interconectividad	Shield Enthernet	15 USD
computadora	Rasberry Pi A	30 USD
Memoria	Tarjeta SD 16 GB	6 USD3
TOTAL		133 USD

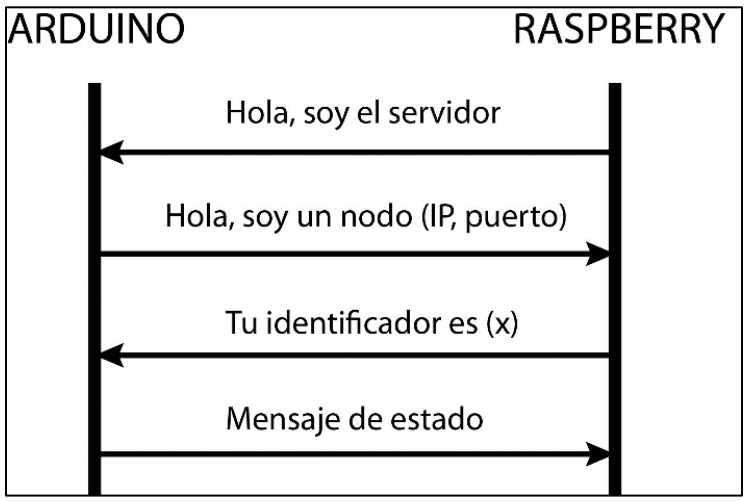
Fuente: Los autores

5.4.3 Esquema de comunicación del protocolo

En este proceso se puede evidenciar como el servidor, será el encargado de enviar los mensajes a través de la red, con esto logrando que los nodos IOT descubran donde está situado el servidor, el mensaje es enviado con intervalos de tiempo, permitiendo que el servicio esta constante mente actualizado, de esta forma si en algún momento se recibe un mensaje que no pertenezca a la interconexión

establecida, se generará una alarma invitando a identificarse nuevamente Una vez el nodo obtiene el identificador, ya puede empezar a realizar los envíos necesarios o escuchar un puerto determinado. Este esquema de comunicación se interpreta de acuerdo a la Ilustración 43.

Ilustración 43. Esquema de comunicación



Fuente: Los autores

6. MANUAL DE PROCEDIMIENTOS PARA LA UTILIZACIÓN EN FORMA MÁS SEGURA DE INTERNET DE LAS COSAS (IoT), QUE LE PERMITA A USUARIOS, INTERACTUAR CON ESTAS TECNOLOGÍAS REDUCIENDO SUSTANCIALMENTE LOS PROBLEMAS DE VULNERABILIDAD.

La protección de una infraestructura de Internet de las cosas precisa de una estrategia de seguridad rigurosa y detallada. La eficacia de esta estrategia se basa en la protección de los datos en la nube, la protección de la integridad de los datos en su tránsito por la red pública de Internet y el aprovisionamiento de dispositivos de forma segura. Cada capa genera mayor garantía de seguridad en toda la infraestructura.[82]

6.1 INTEGRADOR/FABRICANTE DE HARDWARE IOT

Estos son los procedimientos recomendados para los fabricantes de hardware de IoT e integradores de hardware.

- **Acotar el hardware a unos requisitos mínimos**: el diseño del hardware debe incluir únicamente las características mínimas necesarias para su funcionamiento. Un ejemplo es la inclusión de puertos USB únicamente si es necesario para el funcionamiento del dispositivo. Estas características adicionales abren el dispositivo para vectores de ataques no deseados, los cuales deben evitarse.

- **Crear hardware a prueba de manipulaciones**: mecanismos integrados para detectar la alteración física del hardware; por ejemplo, abrir la cubierta del dispositivo o quitar una parte de este. Estas señales de alteración pueden formar parte de la transmisión de datos que se carga en la nube y que podría alertar a los operadores sobre estos eventos.

- **Basarse en hardware seguro**: si COGS (Costo de Bienes Vendidos) lo permite, cree características de seguridad como el almacenamiento seguro y cifrado, o la funcionalidad de arranque basada en TPM (Módulo de plataforma segura). Estas características crean dispositivos más seguros y ayudan a proteger la infraestructura de IoT general.

- **Aplicar las actualizaciones de manera segura**: las actualizaciones del firmware son inevitables durante la vigencia del dispositivo. La creación de dispositivos con rutas de acceso seguras para las actualizaciones y la garantía

[82] Microsoft. Practicas recomendadas de seguridad en IoT. [En línea]. 2017. [Consultado el 15 de noviembre de 2017]. Disponible en internet: https://docs.microsoft.com/es-es/azure/iot-hub/iot-hub-security-best-practices

criptográfica de la versión del firmware permitirá la protección del dispositivo durante y después de las actualizaciones.

6.2 DESARROLLADOR DE SOLUCIONES DE IOT

Estos son los procedimientos recomendados para los desarrolladores de soluciones de IoT:

- **Seguir una metodología de desarrollo de software seguro**: el desarrollo de software seguro requiere pensar bien la seguridad, desde la concepción del proyecto hasta su implementación, prueba y desarrollo. Esta metodología influye en la elección de plataformas, idiomas y herramientas. El Ciclo de vida de desarrollo de seguridad de Microsoft proporciona un enfoque paso a paso para la creación de software seguro.

- **Elegir software de código abierto con cuidado**: el software de código abierto brinda la oportunidad de desarrollar soluciones con rapidez. Al elegir software de código abierto, tenga en cuenta el nivel de actividad de la comunidad para cada componente de código abierto. Una comunidad activa garantiza la compatibilidad con el software; se detectarán problemas, a los que se hará frente. La otra opción es que no se admita software de código abierto complejo e inactivo, y así lo más probable es que no se detecten problemas.

- **Integrar con cuidado**: muchas de las brechas de seguridad del software aparecen en el límite de las bibliotecas y las API. Es posible que la funcionalidad que puede no requerirse para la implementación actual siga estando disponible a través de un nivel de API. Para garantizar la seguridad general, asegúrese de comprobar que no existen errores de seguridad en todas las interfaces de los componentes que se están integrando.

6.3 IMPLEMENTADOR DE SOLUCIONES DE IOT

A continuación se muestran los procedimientos recomendados para los implementadores de soluciones de IoT:

- **Implementar hardware de forma segura**: las implementaciones de IoT pueden requerir la implementación de hardware en ubicaciones no seguras, por ejemplo, espacios públicos o configuraciones regionales no supervisadas. En este tipo de situaciones, asegúrese de que la implementación de hardware sea lo más resistente posible a las manipulaciones. Si hay puertos USB o de otro tipo disponibles en el hardware, asegúrese de que estos se tratan de forma segura. Muchos vectores de ataques pueden usarlos como punto de entrada.

- **Mantener seguras las claves de autenticación**: durante la implementación, cada dispositivo requiere identificadores de dispositivo y claves de autenticación asociadas generadas por el servicio en la nube. Mantenga seguras estas claves físicamente incluso después de la implementación. Un dispositivo malintencionado puede usar cualquier clave en peligro para su enmascaramiento como dispositivo existente.

6.4 OPERADOR DE SOLUCIONES DE IOT

Estos son los procedimientos recomendados para los operadores de soluciones de IoT:

- **Mantener el sistema actualizado**: asegúrese de que los sistemas operativos y todos los controladores de los dispositivos están actualizados con las versiones más recientes. Si activa las actualizaciones automáticas en Windows 10 (IoT u otras SKU), Microsoft mantiene el equipo actualizado, ofreciendo a los dispositivos de IoT un sistema operativo seguro. En el caso de otros sistemas operativos (como Linux), el hecho de mantenerlos actualizados garantiza también su protección contra ataques malintencionados.

- **Proteger contra la actividad malintencionada**: si el sistema operativo lo permite, instale las funcionalidades antivirus y antimalware más recientes en el sistema operativo de todos y cada uno de los dispositivos. Esto puede ayudar a mitigar las amenazas más externas. Puede proteger los sistemas operativos más modernos contra amenazas realizando los pasos adecuados.

- **Auditar con frecuencia**: la auditoría de los problemas relacionados con la seguridad de la infraestructura de IoT es clave a la hora de responder a incidentes de seguridad. La mayoría de los sistemas operativos proporciona un registro de eventos integrado que se debe revisar con frecuencia para asegurarse de que no se haya producido ninguna infracción de seguridad. La información de la auditoría se puede enviar como transmisión independiente de telemetría al servicio en la nube, donde puede analizarse.

- **Proteger físicamente la infraestructura de IoT**: los peores ataques contra la seguridad de la infraestructura de IoT se inician mediante el acceso físico a los dispositivos. La protección contra el uso malintencionado de puertos USB y otros accesos físicos es una importante práctica de seguridad. Una clave para descubrir las infracciones que pudieran haberse producido es registrar el acceso físico, como el uso del puerto USB. Una vez más, Windows 10 (IoT y el resto de SKU) habilita el registro detallado de estos eventos.

- **Proteger las credenciales en la nube**: es posible que las credenciales de autenticación en la nube usadas para configurar y manejar una implementación de IoT sean la forma más fácil de obtener acceso a un sistema IoT y ponerlo en peligro. Proteja las credenciales cambiando la contraseña con frecuencia y no usándolas en equipos públicos.

Las funcionalidades de los distintos dispositivos IoT varían. Algunos dispositivos pueden ser equipos que ejecutan sistemas operativos de escritorio comunes, y otros pueden estar ejecutando sistemas operativos muy ligeros. Los procedimientos recomendados de seguridad descritos anteriormente pueden ser aplicables a estos dispositivos en diverso grado. En caso de proporcionarse, deben seguirse las prácticas recomendadas de seguridad e implementación facilitadas por el fabricante de estos dispositivos.

Puede que algunos dispositivos heredados y limitados no se hayan diseñado de forma específica para la implementación de IoT. Estos dispositivos pueden carecer de la funcionalidad para cifrar datos, conectarse a Internet o proporcionar auditoría avanzada. En estos casos, una puerta de enlace de campo moderna y segura puede agregar datos desde dispositivos heredados y proporcionar la seguridad necesaria para la conexión a Internet de estos dispositivos. Las puertas de enlace de campo proporcionan una autenticación segura, una negociación de sesiones cifradas, la recepción de comandos desde la nube y muchas otras características de seguridad.

DIVULGACIÓN

La divulgación del proyecto “Construcción de procedimientos para minimizar las vulnerabilidades a las que se ven expuestas las organizaciones (frente al IoT.)” busca la vinculación de actores institucionales con fin de promover su uso y acceso a nivel corporativo, así mismo se utilizaran los siguientes medios para su difusión.

- Mediante el uso de las redes sociales institucionales para promover el conocimiento de los contenidos educativos del proyecto, y los beneficios que aporta a las organizaciones.

- Comunicar a las autoridades institucionales sobre el proyecto, con el interés de que se asuma como un proyecto colaborativo o participativo, donde toda la comunidad académica se involucre en pro de adoptar buenas prácticas de seguridad.

- Emplear el sistema de repositorio en línea que cuenta la institución, con el fin de que el proyecto sirva de insumo y pueda ser adoptado como una herramienta de prevención frente al uso de dispositivos IoT.

CONCLUSIONES

La industria de consumo piensa primero en vender que, en seguridad, es así como vemos hoy en día gigantes avances en interconectividad y prestación de servicios, en los cuales se ha dejado de lado la seguridad, es por esto que los profesionales de la seguridad informática deben de estar abantes ante la premisa que marca el hecho de saber que un ataque en red por medio de IoT puede llegar a ser base para un ataque masivo a nivel mundial.

Las organizaciones hacen uso de los avances de interconectividad que han tenido las "cosas" convirtiéndose en completas herramientas tecnológicas que facilitan las tareas cotidianas, mejorando los procesos y haciéndolos más prácticos, es por esto que se deben centrar los esfuerzos en no permitir el mal uso de estas herramientas, pues a un gran beneficio viene ligada una gran responsabilidad.

En algunos sectores de la sociedad existe confusión sobre lo que es IoT, o por lo menos no tienen una idea real del alcance de la interconexión de las "cosas" que llegue al usuario de forma clara y concisa, puesto que se argumenta que hace referencia a las cosas interconectadas, dejando de lado la tecnología utilizada, sus beneficios, correcto uso y por supuesto las medidas que se deben de tener en cuenta a la hora de implementar IoT.

Aunque tanto a nivel nacional como internacional los países se han ido actualizando desde el punto de vista legal, hace falta difundir y dar a conocer de una forma clara y concisa las leyes de protección de datos creadas, facilitando el uso de herramientas legales al usuario para que haga valer sus derechos.

IoT necesita leyes que vayan dirigidas concretamente hacia esta tecnología, se deben de crear parámetros legales que orienten, tanto para la creación como para la adquisición de equipos, como ya se evidencio en el documento hay un vació legal frente a los equipos importados en forma masiva, ya que no hay un lineamiento frente a que parámetros de seguridad deben de tener estos antes de ser puestos al servicio de los usuarios finales.

La utilización de IoT permite automatizar los entornos en que desarrollamos nuestras vidas, las herramientas puestas en marcha dan soluciones prontas y valederas frente a retos que hace unos años era imposible realizar, lo que se veía en películas que creíamos del futuro se puede hacer realidad hoy de forma segura, si se acompaña de controles que permitan mitigar los problemas de seguridad.

La seguridad de los dispositivos conectados a internet es básica, por eso se hace necesario seleccionar metodologías diseñadas para controlar y mitigar los riesgos a los que se enfrenta la infraestructura de interconexión IoT, esto acompañado de

la posibilidad de contar con servidores propios para la recepción de la información generada permitirá generar espacios más seguros para la valiosa información recolectada.

Las tecnologías actuales tienen una premisa de adaptabilidad que además de ser amables con los usuarios los hacen vulnerables, todo esto se da gracias a que las herramientas Tecnológicas se hacen para que hasta un niño las pueda utilizar generando un estado de seguridad falso, es así como los usuarios desempacan cualquier equipo, o descargan cualquier aplicación sin ni siquiera pararse a revisar las medidas de seguridad que se deben de tener para no poner en riesgo los datos alojados en los mismos.

Es un error creer que nunca se va a ser blanco de un ciberataque y por eso se suman cada año a los registros de víctimas de los hackers esto sumado La falta de conocimientos en áreas de seguridad lo cual pueden permitir que un ciberataque sea exitoso poniendo en riesgo la organización o privacidad de un usuario, algo que puede costar más que invertir en profesionales capacitados para configurar los equipos.

RECOMENDACIONES

Las organizaciones antes de poner en marcha un plan de interconectividad, deben aplicar todos los modelos que sean necesarios para obtener producción inteligente, con el fin de alcanzar máximos resultados tanto en el área de producción, logística y mercadeo, como en la seguridad de sus datos e infraestructuras IoT.

Se debe de investigar en forma detallada y oportuna, antes de comprar cualquier equipo de interconectividad, para saber cuáles son sus protocolos de seguridad.

Revisar de forma detallada el catálogo de compra, analizando las instrucciones que el vendedor de un artículo de consumo IOT, pone para activar su seguridad, en caso de no tenerlo debe de configurarse siguiendo los pasos que en esta monografía se especifica en el sexto capítulo.

Es necesario actualizar de forma continua el firmware de los dispositivos, como los parches de seguridad, debido a que estos cambian de constantemente.

Una vez adquirido un equipo, se debe de cambiar la contraseña por defecto, debido a que la mayoría de ataques se hacen mediante la utilización de las contraseñas universales.

BIBLIOGRAFÍA

Vormetric data threat. (2017). Informe de seguridad y confianza en la red. San José: Universidad de california.

Gartner “Magic Quadrant for Endpoint Protection Platforms”, de Eric Ouellet, Ian McShane, Avivah Litan; 30 de enero de 2017

IoT 2020 Informe de negocio El futuro del Internet of Things: De los sensores al sentido de negocio schneider electric

James F. Kurose & Keith W. Ross (2011), “Redes de Computadoras: un enfoquedescendente”, 5ta Edición de Prentice Hall
Ribas Lequerica, Joan (2013), “Manual imprescindible de Arduino práctico”,Anaya Multimedia

Upton, Eben (2013), “Raspberry Pi.: guía del usuario”, Anaya Multimedia
Arias, Ángel (2014), “Aprende a programar Ajax y jQuery”, Amazon

Informe Things Matter (Iot) Revista Transformación Digital | jueves 02 - noviembre - 2017

Colombia. (1991). Constitución Política nacional (primera ed.). Bogotá, Cundinamarca, Colombia: Imprenta Nacional.

WEBGRAFÍA

MCI electronics. ¿qué es arduino?. [En línea]. [Consultado 17 de octubre de 2017]. Disponible en internet: http://arduino.cl/que-es-arduino/

Fundación Wikimedia, Inc. Big Data. [En línea]. 2017 [Consultado 22 de noviembre de 2017]. Disponible en internet:https://es.wikipedia.org/wiki/Big_data#Definici.C3.B3n

INTERPOL. Delincuencia informática. [En linea]. [Consultado el 17 de Octubre de 2017]. Disponible en internet: https://www.interpol.int/es/Crime-areas/Cybercrime/Cybercrime

TechTarget. Internet de las cosas (IoT). [En línea]. 2017. [Consultado el 17 de octubre de 2017]. Disponible en internet: http://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT

DEL VALLE HERNÁNDEZ, Luis. Arduino y los dispositivos del IoT. [En línea]. [Consultado el 02 de noviembre de 2017]. Disponible en internet: https://programarfacil.com/podcast/61-arduino-y-los-dispositivos-del-iot/

Venemedia. ¿Qué es domótica?. [En línea]. [Consultado el 18 de Octubre de 2017]. Disponible en internet: http://conceptodefinicion.de/domotica/

Fundación Wikimedia, Inc. Internet de las cosas. [En línea]. [Consultado el 02 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/Internet_de_las_cosas

Fundación Wikimedia, Inc. M2M. [En línea]. [Consultado el 03 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/M2M

Fundación Wikimedia, Inc. Near field communication. [En línea]. [Consultado el 03 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/Near_field_communication

TENENGA. Ciudad inteligente y objeto inteligente: ¿qué es el IoT y cuál es su importancia para los negocios?. [En línea]. [Consultado el 02 de noviembre de2017]. Disponible en internet: http://www.tenenga.it/es/ciudad-inteligente-y-objeto-inteligente-que-es-el-iot-y-cual-es-importancia-para-los-negocios/

Fundación Wikimedia, Inc. IPv6. [En línea]. [Consultado el 03 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/IPv6

CASTRO, Alberto. ¿Qué es Raspberry Pi, dónde comprarla y cómo usarla?. [En línea]. 2014. [Consultado el 18 de octubre de 2017]. Disponible en internet: http://computerhoy.com/noticias/hardware/que-es-raspberry-pi-donde-comprarla-como-usarla-8614

Fundación Wikimedia, Inc. RFDI. [En línea]. [Consultado el 03 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/RFID

Fundación Wikimedia, Inc. Seguridad de la información. [En línea]. [Consultado el 19 de octubre de 2017]. Disponible en internet. https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Fundación Wikimedia, Inc Sensor. [En línea]. 2017. [Consultado el 28 de noviembre de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/Sensor

Domodesk. A fondo: ¿qué es iot (el internet de las cosas)?.[En línea]. [Consultado el 18 de octubre de 2017]. Disponible en internet: http://www.domodesk.com/221-a-fondo-que-es-iot-el-internet-de-las-cosas.html

DOMODESK. A fondo: ¿qué es iot (el internet de las cosas)?.[En línea]. [Consultado el 05 de noviembre de 2017]. Disponible en internet: http://www.domodesk.com/221-a-fondo-que-es-iot-el-internet-de-las-cosas.html

HIDALGO MARTÍN, Elena. The Internet Of Things. [En línea]. 2016. [Consultado el 05 de noviembre]. Disponible en internet: https://himarele.wordpress.com/2016/09/14/the-internet-of-things/

LOVELOCK, Julián. hacia un internet de las cosas confiable (IOT). [En línea]. [Consultado el 05 de noviembre de 2017]. Disponible en internet: http://www.seguridadenamerica.com.mx/noticias/de-consulta/articulos-destacados-de-seguridad/27704-hacia-un-internet-de-las-cosas-confiable-iot

MARTÍNEZ, Isaura. Internet de las Cosas (IoT): Ventajas para las empresas. [En línea]. 2017. [Consultado el 07 de noviembre de 2017]. Disponible en internet: https://www.commercient.com/internet-de-las-cosas-iot-ventajas-para-las-empresas/

RANDELL, Brian. Conferencia de Ingeniería de Software de la OTAN. [En línea]. 1996. [Consultado el 07 de noviembre de 2017]. Disponible en internet: http://homepages.cs.ncl.ac.uk/brian.randell/NATO/NATOReports/

CEDOM. Qué es Domótica. [En línea]. [Consultado el 08 de noviembre de 2017]. Disponible en internet: http://www.cedom.es/sobre-domotica/que-es-domotica

Justindeveloper. Desarrollo de Aplicaciones Móviles, Servicios Web, Arquitectura SOA. [En línea]. 2008. [Consultado el 10 de noviembre de 2017]. Disponible en internet: https://justindeveloper.wordpress.com/2008/12/15/arquitectura-de-software-%E2%80%93-overview/

ÉCIJA, Álvaro. una aproximación a algunos elementos de internet de las cosas. [En línea]. 2015. [Consultado el 12 de noviembre de 2017]. Disponible en internet: https://www.ecixgroup.com/una-aproximacion-algunos-elementos-de-internet-de-las-cosas/

SORIA PASTOR, Javier. Seguridad en Internet de las Cosas. [En línea]. 2016. [Consultado el 13 de noviembre de 2017]. Disponible en internet: https://aunclicdelastic.blogthinkbig.com/la-seguridad-como-preocupacion-universal/

GARRIDO, Felipe. El 2020 habrá 4 mil millones de conexiones a internet. [En línea]. 2016. [Consultado el 18 de noviembre de 2017] Disponible en internet: https://www.fayerwayer.com/2016/06/el-2020-habra-4-mil-millones-de-conexiones-a-internet/

LÓPEZ TAZÓN, Javier. El lado oscuro del Internet de las Cosas. [En línea]. 2016. [Consultado el 13 de noviembre de 2017]. Disponible en internet: http://www.elmundo.es/tecnologia/2016/01/28/56aa295922601d3d548b4653.html

GÓMEZ ABAJO, Carlos. La Internet de las Cosas es una oportunidad asequible para el desarrollo. [En línea]. 2016. [Consultado el 12 de noviembre de 2017]. Disponible en internet: https://www.tendencias21.net/La-Internet-de-las-Cosas-es-una-oportunidad-asequible-para-el-desarrollo_a41840.html

RODRÍGUEZ, Karina. Usuarios aún no tienen confianza en la seguridad de los dispositivos IoT. [En línea]. 2017. [Consultado el 14 de noviembre de 2017]. Disponible en internet: http://computerworldmexico.com.mx/usuarios-aun-confianza-en-la-seguridad-los-dispositivos-iot/

RIVERA, Nicolás. Qué es el Internet of Things y cómo cambiará nuestra vida en el futuro. [En línea]. 2015. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://hipertextual.com/2015/06/internet-of-things.

Unión Internacional De Telecomunicaciones. Y.2060 : Visión general de la Internet de las cosas. [En línea]. 2012. [Consultada 18 de noviembre de 2017]. Disponible en internet: https://www.itu.int/rec/T-REC-Y.2060-201206-I/es

SANTUCCI, Gérald. Official opening of the conference – Plenary sesión. [En línea]. 2009. [Consultado el 14 de noviembre de 2017]. Disponible en internet:http://cordis.europa.eu/pub/fp7/ict/docs/enet/20090128-speech-iot-conference-lux_en.pdf

EVERS, Joris. Forrester CEO: Web services next IT storm. [En linea]. 2003. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.infoworld.com/article/2681101/operating-systems/forrester-ceo--web-services-next-it-storm.html

EVANS, Dave. CISCO Internet Bussiness Solutions Group – IBSG. Internet de las Cosas: Como la próxima evolución de Internet lo cambia todo [en línea]. 2011. [Consultado el 14 de noviembre de 2017]. Disponible en internet: http://www.cisco.com/web/LA/soluciones/executive/assets/pdf/internet-of-things-iot-ibsg.pdfdf

TSCHOFENIG, Hannes; ARKKO, Jari; THALER, Dave y MCPHERSON, Danny. Internet Architecture Board (IAB). [En linea]. 2015. [Consultado el 28 de marzo de 2018]. Disponible en internet: https://tools.ietf.org/html/rfc7452

Symantec. iot-security-reference-architecture. [En línea]. 2016. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

CSIRT-CV. Informe-Internet_de_las_Cosas. [En línea]. [Consultado el 14 de noviembre de 2017]. Disponible en internet: http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

Dassault Systèmes. El internet de las cosas. [En línea]. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.3ds.com/es/historias/como-influye-la-tecnologia-en-el-futuro/el-internet-de-las-cosas/

Microsoft. Seguridad de Internet de las cosas desde el principio. [En línea]. 2017. [Consultado el 15 de noviembre de 2017]. Disponible en internet: https://docs.microsoft.com/es-es/azure/iot-suite/securing-iot-ground-up

Allied Business Intelligence, Inc. ABIresearch. [En linea]. [Consultado el 15 de noviembre de 2017]. Disponible en internet: https://www.abiresearch.com/

LYDON, Bill. Industria 4.0: producción inteligente y flexible. [En línea]. [Consultado el 14 de noviembre de 2017]. Disponible en internet: https://www.isa.org/intech/20160601/

OWASP. OWASP Internet of Things Project. [En linea]. 2018. [Consultado el 28 de marzo de 2018]. Disponible en internet:https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities

TARQUINO MURGUEITO, Daniel Felipe y GARCÍA GARCÍA, Edwin Sebastián. Escuela Colombiana de Ingeniería Julio Garavito. Trabajo fin de grado: Seguridad en Internet de las cosas. [En línea]. 2017. [Consultado 27 de marzo de 2018]. Disponible en internet: https://repositorio.escuelaing.edu.co/handle/001/605

TORRE ARCE, José Luis. Universidad de Cantabria. Trabajo fin de grado: Arquitectura de seguridad ligera para el Internet de las Cosas basada en HIMMO. [En línea]. 2015. [Consultado el 18 de noviembre de 2017]. Disponible en internet: https://repositorio.unican.es/xmlui/handle/10902/7228

CASTRO SOLA, Miguel. Universidad de Jaén. Trabajo fin de grado: Internet de las cosas. Privacidad y Seguridad. [En línea]. 2016. [Consultado el 18 de noviembre de 2017]. Disponible en internet: http://sinbad2.ujaen.es/sites/default/files/publications/Memoria_0.pdf

ROMERO GARCÍA, María Teresa. La protección de datos ante el Internet de las cosas. [En línea]. 2017. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://oa.upm.es/47426/

PINZÓN NIÑO, David Leonardo. Panorama de aplicación de internet de las cosas (IoT). [En línea]. 2015. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://repository.usta.edu.co/handle/11634/201/browse?type=author&value=Pinz%C3%B3n+Ni%C3%B1o%2C+David+Leonardo

INCIBE, Red.es, Huawei. Creación de un mundo IoT fiable y gestionado. [En línea]. 2017. [Consulado el 19 de noviembre de 2017]. Disponible en internet: https://underc0de.org/foro/almacen-de-manuales/(pdf)-libro-blanco-de-ciberseguridad-iot-de-huawei/

ZANONY, Leandro. Futuro inteligente. [En línea]. 2014. [Consultado el 19 de noviembre de 2017]. Disponible en internet: http://appstercerclick.com/futurointeligente/FuturoInteligente.pdf

COLOMBIA CONGRESO DE LA REPUBLICA. Ley 527. Bogotá. (Agosto 18 de 1999). Diario Oficial 43.673 de agosto 21 de 1999. p. 19.

COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (diciembre 31 de 2008). Diario Oficial 47219 de diciembre 31 de 2008. p. 17.

COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (enero 5 de 2009). Diario Oficial 47223 de enero 5 de 2009. p. 5.

DEPARTAMENTO NACIONAL DE PLANEACIÓN. CONPES 3701. Bogotá. (julio 14 de 2011). p. 43

COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1480. Bogotá. (octubre 12 de 2011). Diario Oficial 48220 de octubre 12 de 2011. p. 33.

COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1581. Bogotá. (octubre 18 de 2012). Diario Oficial 48587 de octubre 18 de 2012. p. 15.

COLOMBIA CONGRESO DE LA REPUBLICA. Decreto 2758. Bogotá. (diciembre 28 de 2012). Diario Oficial 48658 de diciembre 29 de 2012. p. 2.

COLOMBIA MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Resolución 76434. Bogotá. (diciembre 4 de 2012). p. 13

MINISTERIO DE DEFENSA NACIONAL. Resolución 3933. Bogotá. (junio 4 de 2013). Diario Oficial 48813 de junio 7 de 2013. p. 3.

COLOMBIA CONGRESO DE LA REPUBLICA. Decreto 1377. Bogotá. (junio 27 de 2013). Diario Oficial 48834 de junio 27 de 2013. p. 11.

COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1712. Bogotá. (marzo 4 de 2014). Diario Oficial 49084 de marzo 4 de 2014. p. 14.

COLOMBIA CONGRESO DE LA REPUBLICA. Decreto 857. Bogotá. (mayo 2 de 2014). Diario Oficial 49143 de mayo 6 de 2014. p. 8.

DEPARTAMENTO NACIONAL DE PLANEACIÓN. CONPES 3854. Bogotá. (abril 11 de 2016). p. 91

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Resolución 2710. Bogotá. (octubre 3 de 2017). Diario Oficial 50376 de octubre 4 de 2017. p. 4

CONCEJO DE EUROPA. Tratado 185. Budapest. (noviembre 23 de 2001). p. 26.

ASAMBLEA GENERAL DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Resolución AG /RES 2004. EEUU. (junio 8 de 2004). p. 46

Venemedia. ¿Qué es internet?. [En línea]. 2014. [Consultado 19 de octubre de 2017]. Disponible en internet: http://conceptodefinicion.de/internet/.

CanalComstor. 6 tipos de sensores para aplicación en la internet de las cosas. [En línea]. 2017. [Consultado 01 de noviembre de 2017]. Disponible en internet: http://blogmexico.comstor.com/6-tipos-de-sensores-para-aplicacion-en-la-internet-de-las-cosas

Fundación Wikimedia. Sensor.[En línea]. 2017. [Consultado 28 de noviembre de 2017]. Disponible en internet: http://es.wikipedia.org/wiki/Sensor#Caracter.C3.ADsticas_de_un_sensor

Jecrespom. Que es arduino. [En línea]. [Consultado 21 de octubre de 2017]. Disponible en internet: https://aprendiendoarduino.wordpress.com/2016/09/25/que-es-arduino/

Yash. basic-iot-actuators. [En línea]. 2017. [Consultado el 07 de marzo de 2018]. Disponible en internet: https://iotbytes.wordpress.com/basic-iot-actuators/

Premier Farnell Limited. Puerta de enlace. [En línea]. 2018. [Consultado el 06 de Marzo de 2018]. Disponible en internet: http://es.farnell.com/internet-of-things-gateway

Gartner. Principales tendencias en el ciclo Gartner Hype para tecnologías emergentes. [En línea]. 2017. [Consultado 20 de agosto de 2017]. Disponible enhttps://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

ACIS. Internet de las Cosas: La importancia de la infraestructura convergente de redes. [En linea]. 2017. [Consultado 02 de noviembre de 2017]. Disponible en internet: http://acis.org.co/portal/content/internet-de-las-cosas-la-importancia-de-la-infraestructura-convergente-de-redes

Semtech. Que es LoRa. [En Línea]. 2018. [Consultado el 7 de Marzo de 2018]. Disponible en internet:]https://www.semtech.com/technology/lora/what-is-lora

Electrónica S.L.. 11 redes inalámbricas fundamentales para Internet de las Cosas. [En línea]. 2016. [Consultado 05 de noviembre de 2017]. Disponible en internet: https://www.redeweb.com/articulos/software/11-redes-inalambricas-fundamentales-para-internet-de-las-cosas/

IT Business Solutions. Innovación del IoT en la nube: [En línea]. SF. [Consultado 03 de noviembre de 2017]. Disponible en internet: http://www.itbusiness-solutions.com.mx/innovacion-del-iot-a-la-nube

Crece vulnerabilidad en sistemas de seguridad para IoT. [En línea]. 2015. [Consultado el 07 de Noviembre de 2017]. Disponible en internet: http://www.cioal.com/2015/05/22/hp-da-a-conocer-vulnerabilidad-en-sistemas-de-seguridad-para-iot/

OWASP. Top 10 2014-I1 Insecure Web Interface. [En línea]. 2015. [Consultado octubre 3 de 2017]. Disponible en internet: https://www.owasp.org/index.php/Top_10_2014-I1_Insecure_Web_Interface

OWASP. Top 10 2014-I2 Insufficient Authentication/Authorization. [En línea]. 2015. [Consultado octubre 3 de 2017]. Disponible en internet: https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization

HUERTA, Antonio. Introducción al análisis de riesgos – Metodologías (II). [En línea]. 2012. [Consultado el 31 de octubre de 2017]. Disponible en internet:https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

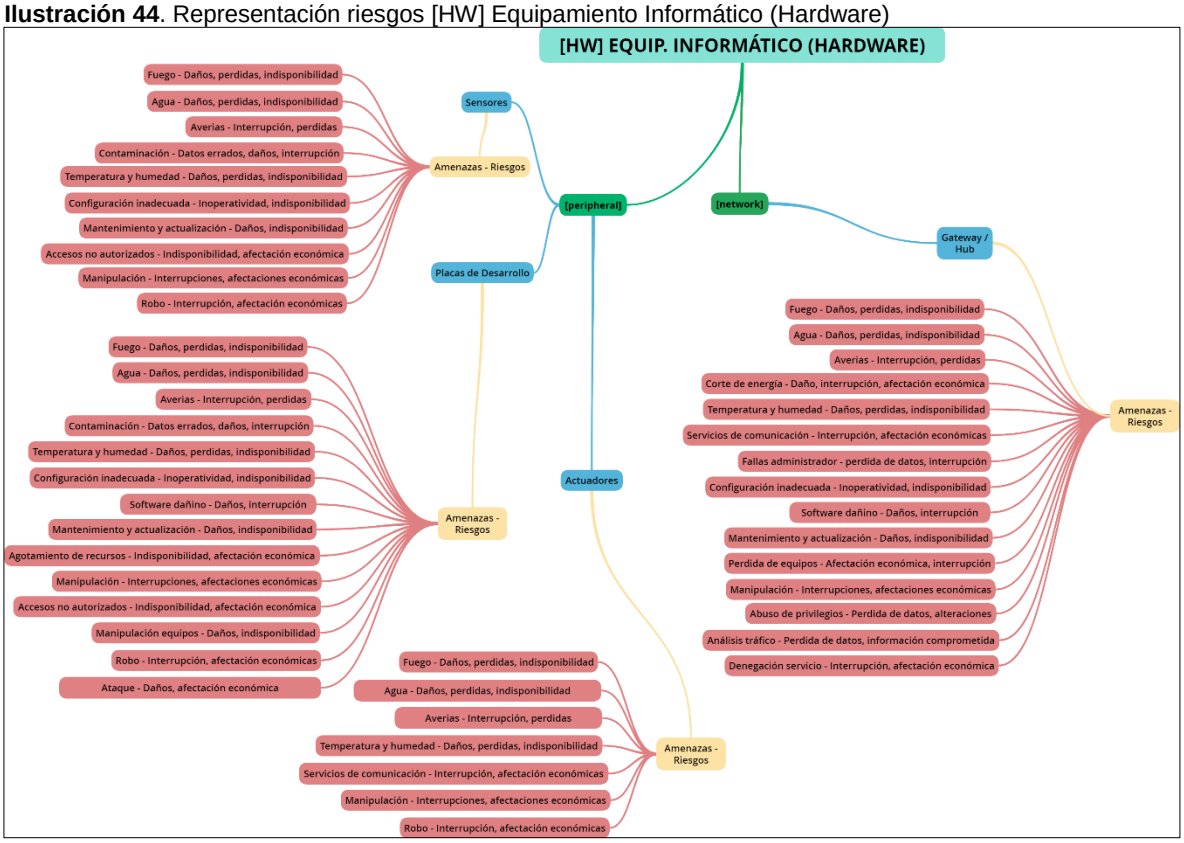
ALEMÁN, Helena; RODRÍGUEZ, Claudia. Metodologías Para el Análisis de Riesgos en los SGSi. [En línea]. 2015. [Consultado el 27 de marzo de 2018]. Disponible en internet: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Microsoft. Practicas recomendadas de seguridad en IoT. [En línea]. 2017. [Consultado el 15 de noviembre de 2017]. Disponible en internet: https://docs.microsoft.com/es-es/azure/iot-hub/iot-hub-security-best-practices

ANEXOS

Anexo 1. Mapa mental riesgos [HW] Equipamiento Informático (Hardware)

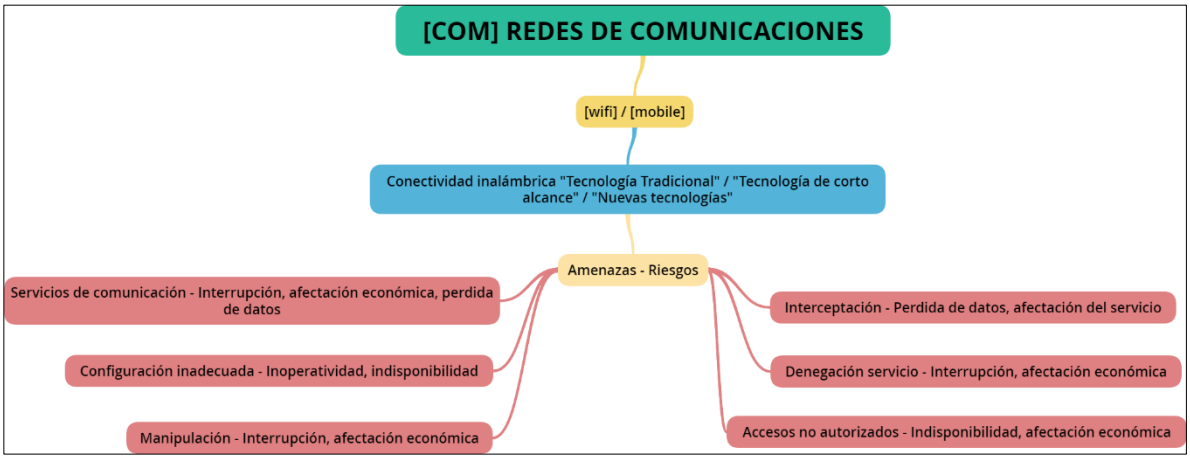
Ilustración 44. Representación riesgos [HW] Equipamiento Informático (Hardware)



Fuente: Los autores

Anexo 2. Mapa mental riesgos [COM] Redes de Comunicación

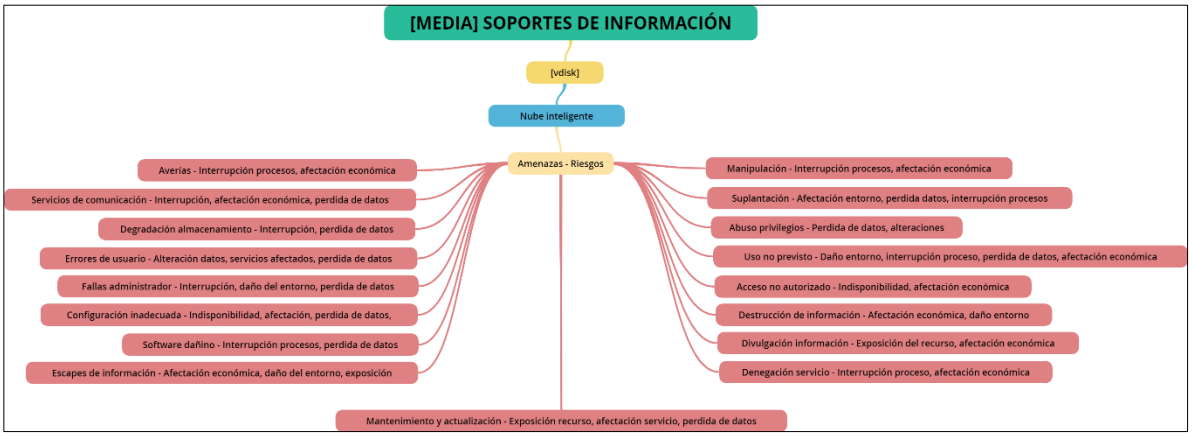
Ilustración 45. Representación riesgos [COM] Redes de Comunicación



Fuente: Los autores

Anexo 3. Mapa mental riesgos [MEDIA] Soportes de información

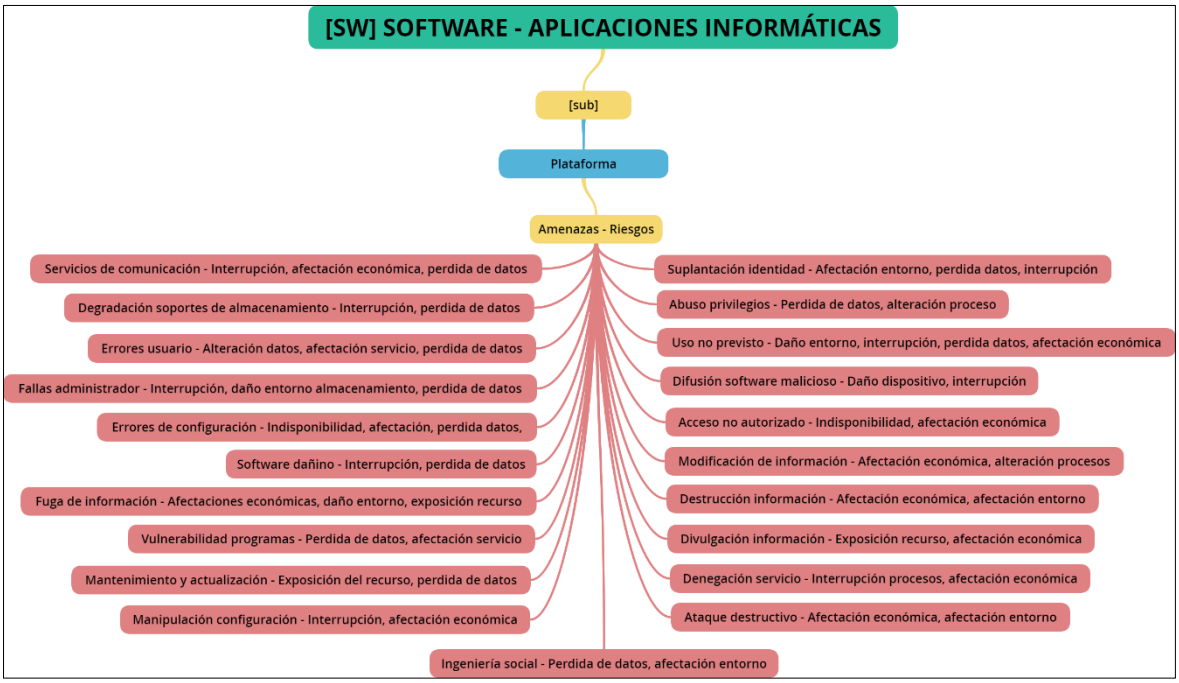
Ilustración 46. Representación riesgos [Media] Soportes de información



Fuente: Los autores

Anexo 4. Mapa mental riesgos [SW] Software – Aplicaciones informáticas

Ilustración 47. Representación riesgos [SW] Software – Aplicaciones informáticas



Fuente: Los autores