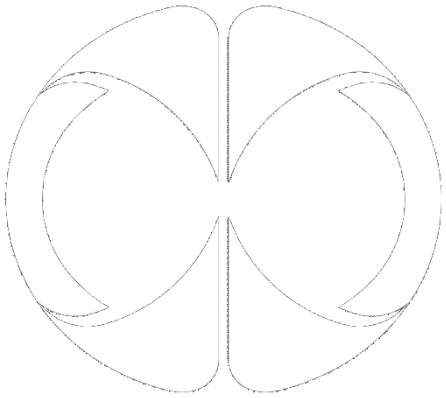

Fundación Universitaria
SAN MATEO

Fundación Universitaria
SAN MATEO

**FACULTAD DE INGENIERIAS**

**INGENIERÍA EN TELECOMUNICACIONES**

# ANÁLISIS GENERAL DEL ENFOQUE IOT EN REDES

**TRABAJO DE GRADO MODALIDAD DE OPCIÓN DE GRADO**

**BRAYAN ALEXANDER HERNANDEZ**

**DIANA PAOLA ORTIZ GALEANO**

**DIRECTOR (A)**

**HERNAN DARIO JIMÉNEZ JIMÉNEZ**

**BOGOTA D.C**

**2019**

**NOTA DE SALVEDAD DE RESPONSABILIDAD INSTITUCIONAL**

*"La Fundación Universitaria San Mateo NO se hace responsable de los conceptos emitidos en el presente documento, el departamento de investigaciones velará por el rigor metodológico de la investigación".*

# CONTENIDO

# ÍNDICE DE ILUSTRACIONES

# ÍNDICE DE TABLAS

# DEDICATORIA

El presente trabajo investigativo va dedicado principalmente a Dios por haberme dado la vida y permitirme llegar a este momento tan importante en mi formación profesional. A mi madre quien ha sido de apoyo incondicional a pesar de nuestras diferencias es el pilar más importante de mi vida. A mi padre quien me guía desde el cielo. A mi hermano por sus valiosos consejos. A Raúl quien me ha colaborado en mi crecimiento personal aprendiendo por sí misma. A los maestros que han compartido sus conocimientos y me han apoyado para lograr culminar esta etapa en mi vida de formación profesional.

Diana Paola Ortiz Galeano.

# AGRADECIMIENTOS

Brayan Hernández y Diana Ortiz expresan sus agradecimientos a:

Dios por darnos la fortaleza en momentos de dificultad y debilidad. A Familiares y amigos por el apoyo incondicional durante este proceso, consejos y palabras de aliento.

Finalmente a los Directores del proyecto Hernán Jiménez y Ricardo Ceballos quienes con su conocimiento, enseñanza, dirección y colaboración permitieron el desarrollo de este trabajo.

# ABREVIATURAS

IOT (Internet Of Things)

IDS (Sistema De Detección De Intrusos)

IPS (Sistema De Prevención De Intrusos)

ISP (Provide Service Internet)

SGSI (Sistema De Gestión De Seguridad De La Información)

UIT (Unión Internacional De Telecomunicaciones)

DDOS (Denegación De Servicio Distribuido)

RFID (Identificación Por Radiofrecuencia)

UPNP (Universal Plug And Play)

IANA (Internet Assigned Numbers Authority)

TMN (Telecomunicación Network Management)

PDU (Unidad Del Protocolo De Datos)

PBM (Policy Based Management)

WBEM (Web Based Enterprise Management)

LAN (Local Area Network)

M2M (Machine To Machine)

# RESUMEN

**PALABRAS CLAVE: IoT, Malware, Ataque Cibernético, Seguridad Informática, IPV4, IPV6, Integridad, Blockchain, Vulnerabilidad, Internet, Smart City, Smart Home, Intrusión, Bots, Bonet, RFID, M2M, WSN.**

En la investigación se conoce el origen de este término que aparece en el año 1999 por Kevin Asthon quien estaba realizando investigaciones en el campo RFID y dio a conocer esta idea en una conferencia. En 2005 la ITU comenzó a realizar un estudio sobre el tema y en 2009 este término se convertiría en el título de todo, por la conexión de las cosas y ejecución de redes dinámicas con conectividad desde cualquier momento y lugar, generando facilidades en todos los campos desde Salud, Smart home, Smart city, oficina, automóviles, logística, navegación, medio ambiente, farmacéutica, agricultura y ganadería entre otros, con uso de tecnologías basadas en radiofrecuencia como es el mismo RFID, redes inalámbricas de sensores como WSN, uso de redes de área personal, redes Wlan en conjunto con tecnologías como el uso de la nube, big data, desde luego la cantidad de dispositivos aumenta, así que de tal modo aparece el protocolo ipv6 con 128 bits a diferencia de ipv4 que carece de 32 bits, permitiendo así lograr más conectividad de dispositivos en las redes y hacia internet todo esto administrado por IANA, encargada de la coordinación mundial de los sistemas de direccionamiento del protocolo de internet.

Dado a conocer una generalización de lo que conforma IoT, nuestro enfoque de estudio es la seguridad de los datos en enfoque a la privacidad de esta tecnología, en búsqueda de garantizar que la información que viaja por estas redes en diferentes topologías y clasificación de estas se salvaguarde, de este modo se busca que los datos no sean alterados evitando la violación de la integridad en la información que son causadas por medio de técnicas de ataque aprovechando las vulnerabilidades en las redes , ataques directo al usuario mediante ingeniería social, entre otros aspectos, que pueden generar riesgos en el manejo del usuario.

Para ello se plantean soluciones técnicas y de mediación del uso de esta tecnología al ser consumible para el usuario, generando así una conciencia en el mismo usuario al instante de comprar u observar una cosa orientada a conexión teniendo en cuenta el tipo de información privada que manipularan estos dispositivos entre las redes ya sea de uso hogar o corporativo.

El documento x.800 de la ITU en conjunto con la CCITT, en búsqueda de soluciones de seguridad de modelos abiertos nombra aspectos a tener en cuenta como un control de acceso, la responsabilidad del administrador como el manipulador de la información generando así una aplicación del no repudio, clasificación de amenazas, modelos de autenticación, implementación de políticas. De tal modo que con estos ítems a tener en cuenta podemos brindar un

nivel mayor de seguridad de nuestras redes, ya que el ingreso de IoT en las redes genera recolección de la información, espacio de control del usuario y espacio de conocimiento del usuario.

Para solución de la privacidad de manera técnica dentro de la red se dan a partir de manejos como los IDS e IPS (Sistemas Detector De Intrusos, Sistema Preventivo De Intrusos) no brindando accesos a no autorizados, recopilación de registros de tráfico y consumo dentro de la red, al igual que la aplicación de firewall, métodos de cifrado robustos en el enrutamiento, identificación de dispositivos mediante patrones.

Un término a tratar en la actualidad y que servirá para un análisis de fondo y a futuro de posibles ataques es la seguridad predictiva encargada de análisis de vulnerabilidades constante en todos los aspectos para el presente y el futuro de la seguridad en enfoque a las tecnologías, donde se incluyen estudios estocásticos, psicológicos y de disuasión, en el ser humano frente a sus tomas de decisiones, puesto como lo nombrábamos la seguridad no solo es fiable de manera técnica sino además el usuario se comporta como ( backdoor ) dentro del modelado de seguridad en una red, siendo de los más efectivos puesto que la falta de capacitación y comportamientos del mismo usuario frente a la interacción con las políticas de seguridad establecidas se aplican métodos estocásticos para obtención de resultados.

Volviendo a la parte técnica para el aseguramiento de la integridad de la informática, se genera la aplicación del lenguaje de programación utilizado para administración sistematizada de monedas virtuales como el bitcoin, llamado "blockchain", el cual genera un nivel mayor de seguridad puesto a su manejo y administración del mismo de las transacciones, métodos de autenticación, comunicaciones descentralizadas, primordialmente caracterizado por su manejo de bloques y secuencias de cadena de manejo de las transacciones, de tal modo indicando que es una buena apuesta lo que ofrece blockchain a nivel de seguridad para el IoT.

Podríamos indicar que la cantidad de elementos cosas interconectados en las redes al ser aumentados van en paralelo con el incremento del tráfico a nivel global para ello se requiere de marcos legales que apunten a aspectos jurídicos o de retención de cuentas frente a un mal manejo, intrusión, alteración, entre otros que afecten o vulneren la integridad de la información, que son dirigidos como leyes, decretos y estándares globales tales como recomendaciones realizados por ITU, leyes nacionales de acuerdo a cada país, ley de habeas data, estándares ISO 27000,27001,entre otras.

# ABSTRACT

**KEY WORDS: IoT, Malware, Cyber-Attack, Computer Security, IPV4, IPV6, Integrity, Blockchain, Vulnerability, Internet, Smart City, Smart Home, Intrusion, Bots, Bonet, RFID, M2M, WSN.**

In the course of the document we will find a brief review of the birth of IoT, in the investigation we know the origin of this term that appears in the year 1999 by Kevin Asthon who was conducting research in the RFID field and presented this idea in a conference. In 2005 the ITU began to conduct a study on the subject and in 2009 this term would become the title of everything, by connecting things and executing dynamic networks with connectivity from any time and place, generating facilities in all fields from Health, Smart home, Smart city, office, automobiles, logistics, navigation, environment, pharmaceutical, agriculture and livestock, among others, with the use of radiofrequency-based technologies such as RFID, wireless sensor networks such as WSN, use of personal area networks, Wlan networks in conjunction with technologies such as the use of the cloud, big data, of course the number of devices increases, so that the protocol appears ipv6 with 128 bits unlike ipv4 that lacks 32 bits , thus allowing to achieve more connectivity of devices in the networks and to the internet all this managed by IANA, in charge of the global coordination of the management systems of the internet protocol.

Given a generalization of what constitutes IoT, our approach to study is the security of data under the application of this technology, in search of ensuring that the information that travels through these networks in different topologies and their classification is safeguarded, in this way it is sought that the data are not altered to avoid the violation of integrity in the information that are caused by means of attack techniques or vulnerabilities in the networks, in addition there is the means of direct attack through social engineering, among other aspects , which can generate risks in the user's management.

To do this, technical and mediation solutions are proposed for the use of this technology as it is consumable for the user, generating an awareness in the same user when buying or observing a connection-oriented thing, taking into account the type of private information that will be manipulated. these devices between the networks, whether for home or corporate use, where the ITU document x.800 in conjunction with the CCITT, in search of security solutions of open models, names aspects to be taken into account as an access control, the responsibility of administrator as the manipulator of the information thus generating an application of non-repudiation, classification of threats, authentication models, policy implementation. In such a way that with these items to be taken into account we can provide a higher level of security of our networks, since the entry of IoT in the networks generates information collection, user control space and user knowledge space.

For solution of the privacy of technical way within the network they are given from managements like the IDS and IPS (Intrusion Detector Systems, Preventive System of Intruders) providing non-authorized accesses, compilation of traffic and consumption records within the network, like the firewall application, robust encryption methods in routing, identification of devices through patterns; a term to be dealt with at present and that will serve for a thorough and future analysis of possible attacks is the predictive security in charge of vulnerability analysis in all aspects for the present and the future of security in approach to technologies, where stochastic, psychological and deterrent studies are included in the human being in front of his decision making, since as we named it, security is not only technically reliable but also the user behaves as (backdoor) within the safety modeling in a network, being of the most effective since the lack of training and behavior of the same user in front of the interaction with the security policies established by applying the stochastic method for obtaining results.

Returning to the technical part for the assurance of the integrity of the computer, the application of the programming language used for systematized management of virtual currencies such as bitcoin is generated, called "blockchain", which generates a higher level of security placed at its management and administration of transactions, authentication methods, decentralized communications, primarily characterized by its handling of blocks and chain sequences of transaction management, thereby indicating that it is a good bet what blockchain offers at the security level for the IOT.

We could indicate that the amount of things interconnected in the networks when increased increases in parallel with the increase in global traffic. For this, legal frameworks that point to legal aspects or retention of accounts in the face of mismanagement, intrusion are required. , alteration, among others that affect or violate the integrity of the information, which are addressed as laws and global standards such as recommendations made by ITU, national laws according to each country, habeas data law, ISO standards 27000,27001, among others.

# INTRODUCCIÓN

En la actualidad y en el futuro de cosas conectadas a internet se observara el incremento al igual que con los modos de acceso, a mediados del 2009 empieza a ser público el termino Internet de las cosas, siendo primero implementado ipv6, el cual nacía con el objetivo de permitir conectar más nodos, puesto que ipv4 genera conectividad de 4,294,967,296 direcciones compuestas de 32 bits e ipv6 compuesta de 128 bits generando alrededor de 4.3 billones de direcciones , permitiendo el acceso de más nodos, nuevos modos de redes a través de la utilización de medios inalámbricos conocidos desde su publicación por el IEEE como el 802.15, 802.11,802.3,802.15.4, etc .

Podríamos albergar e indicar que, de acuerdo con todos los medios de acceso para la interconexión de las cosas frente a internet, es una comodidad y revolución en la humanidad con la implementación de cosas en todos los campos posibles de producción, Smart City, Smart home, agricultura, medicina, etc.

Frente a las implementaciones de IoT y sus diferentes medios de red acceso, así mismo se produce el aumento de la ciberdelincuencia intervenida a partir de diferentes métodos que pueden alterar la seguridad de la información de los datos, donde en este enfoque se analiza en el sector de la integridad de los datos en búsqueda de soluciones en protección de los mismos, además se estudian métodos que satisfagan un nivel moderado de protección de la integridad de los datos de todos los nodos persona, cosas y su aplicación en los distintos campos donde el ejemplo más permisivo seria en el uso de la medicina, ciudades inteligentes y casas inteligentes. Las técnicas que se aplican van desde la seguridad en las redes hasta análisis de la interactividad del usuario con el dispositivo IoT Mediante el uso de sensores, Wifi, bluetooth, entre otros.

Para la satisfacción de una posible protección de la integridad de la información se efectúa la aplicación de solución en la confiablidad de los IDS, IPS en las infraestructuras de redes, la creación de entablación de políticas de uso, análisis de uso de las interacciones y cómo afecta una urbanización social referente a la privacidad del usuario, utilización de términos y análisis de posibles soluciones mediante la seguridad predictiva.

# CAPÍTULO I

# DESCRIPCIÓN DEL PROYECTO

El proyecto se elabora para estudiar las vulnerabilidades a nivel de privacidad que presenta Internet de las cosas (IoT) en la búsqueda de violación de los datos, en varios campos y cotidianidades. Con el objetivo de buscar soluciones de seguridad cibernética en IoT, puesto que es unos de los problemas más grandes que se presentan con las implementaciones del mismo en la actualidad.

## I. Presentación del problema de investigación

¿Cómo se puede garantizar la privacidad de seguridad de los datos mediante la búsqueda de técnicas informáticas enfocadas al IoT?

## II. Justificación

En la actualidad y a medida de la evolución de la tecnología la cantidad de cosas estarán interconectados hacia internet vista desde a la accesibilidad en un clic con el apoyo de dispositivos electrónicos en hospitales, Smart City, entre otros, donde de manera paralela y exponencial avanzan las redes para soportar estas cosas brindando eficiencia y accesibilidad frente a una calidad y servicio.

Por lo tanto el tráfico en estas redes es exponencial, desde sus surgimientos e implementaciones del IoT ha facilitado más las tareas al ser humano, donde nombramos que uno de los mayores problemas mundiales en el IOT es que estos tipos de sistemas han sido abruptamente hackeados, los atacantes informáticos e intrusos realizan la obtención de datos por fuga o vulnerabilidades del sistema IoT, cuyo papel es encontrar información del tráfico que circula desde el elemento IoT hasta el hotspot y el destino de este.

El resultado de datos obtenidos más allá de los mismos datos del IoT, es el muestreo de un diseño y dispositivos conectados en una red que puede ser de carácter corporativa u hogar, donde luego en lo posible el atacante propenderá al análisis de todas las máquinas de la red en busca de vulnerabilidades de cada una para un mal trato de la información e intrusión en la red, generando así una violación de privacidad, entre otros aspectos, ya sea porque el elemento IoT conectado

[1]IoT (Internet Of Things): Internet de las cosas es la conexión de los objetos o dispositivos a través de la red.

a la red tenía sus credenciales por defecto y por allí se ingresó u otros tipos de acceso mediante técnicas de intrusión famosos en el IoT, tal como; el DDos (Denegación De Servicio Distribuido), encargado de saturar el elemento con el propósito de obtención de algún dato, caída del servicio dentro de la red, para ingreso a la misma, entre otros como el uso de los bots y bonet en crecimiento.

Por lo tanto, lo que se busca con la investigación es mejorar y mitigar los tipos de acceso de intrusos informáticos en los elementos IoT, debido a que es una gran necesidad con gran demanda puesto que la información personal como de grandes o pequeñas compañías y demás ambientes se ve expuesta en internet por los tipos de conexiones comunicaciones de máquina- máquina máquina-persona.

## III. Objetivos

### *A. Objetivo General*

- Identificar maneras o soluciones para garantizar la integridad de la información en el IoT, para la proposición de soluciones y sistemas que sean seguros y poco vulnerables para los cracker informáticos.

### *B. Objetivos Específicos*

- Analizar las vulnerabilidades de la privacidad en conexiones del tipo IoT.
- Estudiar el comportamiento de una comunicación IoT.
- Definir búsquedas de técnicas informáticas u otras que permitan la integridad de los datos.

# CAPÍTULO II

# MARCO TEÓRICO

Internet de las cosas, considerado como una infraestructura global de la información por medio de la cual permite ofrecer servicios de interconexión a objetos sea físico o virtual, aprovechando la evolución de la tecnología para el procesamiento de información y la comunicación, para ser aplicado en cualquier entorno.

Los diferentes significados que tiene IoT desde que se conoció este término, fue referenciado con varias definiciones tanto para la Comisión de la Unión Europea, como para Unión Internacional de Telecomunicaciones (ITU), en este texto se puede encontrar que la IoT es una arquitectura que permite compartir la información entre objetos o acerca de las personas a través de una red.

## IV. Antecedentes de la investigación

### Historia de IoT

En 1926 Nikola Tesla preparo las bases de las comunicaciones, después en el año 1990 Berners-Lee creo HTTP estas son las bases donde posteriormente en el año 1999 Kevin Ashton fue la persona que utilizo por primera vez la expresión de IoT en una conferencia, desde entonces comenzó a ser normal referirse al sistema de conexión de cosas a internet. [1]

Kevin Asthon Trabajaba en Procter & Gamble (P&G) tenía 28 años en ese momento estaba en problemas porque los productos que manejaba no estaban disponibles en las tiendas, se dio cuenta de cuál era el problema de información, por lo tanto se le ocurrió una idea de colocar sensores a los productos para saber cuándo dejaran de estar en stock, el trato de convencer a P&G para poder implementar la idea que tenía. Asthon asegura que "entendió que la palabra "internet" podría atraer la atención de esta compañía porque en 1998 los gerentes pensaban que la red era lo más importante y buscaban nuevos proyectos. Después la palabra "cosas" se comenzó a usar por la idea de empotrar las computadoras en las mesas y cada vez los equipos llegaban más económicos y más pequeños, la idea era confusa pero era lo suficiente para que comenzara a investigar sobre IoT. [2]

En 2005 ITU (International Telecommunications Unión) realizo el primer estudio sobre el tema, ellos afirmaron lo siguiente "Una nueva dimensión se ha agregado al mundo de las tecnologías de información y la comunicación (TIC): a cualquier hora, en cualquier lugar, ahora vamos a tener conectividad para cualquier cosa. Las conexiones se multiplican y crearán una nueva red dinámica de redes con redes, Internet de las Cosas". En el año 2008 un grupo de empresas crearon una

alianza para promover el uso de protocolos de internet de objetos inteligentes comenzaron a trabajar en ello para que se hiciera realidad esta idea. La Alliance IPSO tiene empresas involucradas actualmente como Google, Bosch, Motorola, Toshiba, etc... Primero comenzaron con el proyecto de desarrollo del protocolo IPV6.En el año 2009 comenzó a ser más escuchada esa palabra IoT, en 2011 fue lanzado como tal el protocolo IPV6 y otros fabricantes anunciaron sus proyectos, después se inició la adopción de estándares para IoT a escala global. [3]

## Definición y conceptos de IoT

El paradigma IoT será considerado en su ámbito de desarrollo como la cuarta revolución industrial, ya que actuará en campos como la industria y automatización, transporte, salud, ciudades inteligentes, casas inteligentes y actividades de la comunidad. IoT es la interconexión en red de todos los objetos que se encuentran equipados con algún tipo de inteligencia, IoT es una verdadera evolución por su interconectividad dando manejo de la información y servicios inteligentes (Silvestre, 2016) afirma:

IoT ofrece grandes oportunidades en diferentes campos, mejorando continuamente la gestión y dando cambio radical en la vida cotidiana ofreciendo nuevas oportunidades en los datos y otros servicios, se puede explorar nuevos modelos de negocio por medio de los dispositivos interconectados. [4]

Con IoT se espera que las cosas sean capaces de interactuar y comunicarse entre ellas por la interconexión basada en estándares de protocolos de comunicación, IoT permitirá comunicarse desde cualquier lugar del mundo a través de diferentes tecnologías de información y comunicaciones con el objetivo de permitir el control y monitorización en tiempo real y de manera automática.

Según el autor (Luis Alberto Pèrez, 2014) En enero de 2013, Telefónica lanzo Smart M2M Solution que conecta, gestiona y controla las comunicaciones M2M usando tarjetas SIM y como servicio derivado de esta solución se lanzó Smart Parking con la que se puede conocer el estado en tiempo real de las plazas de aparcamiento en zonas reguladas a través de sensores con tarjetas SIM, permitiéndole al usuario entre otros servicios el pago del aparcamiento a través del móvil. [5]

El avance que ha tenido la IoT y el crecimiento exponencial de los dispositivos electrónicos con los cuales se puede vincular al Internet de las cosas, ha evolucionado cada vez más, generando un mayor consumo de estos productos logrando una demanda mayor para la implementación de aplicaciones que permitan realizar trabajos sin mayor esfuerzo. El IoT pese a generar una gran facilidad de manejo en objetos y a distancia, genera que cada uno de los dispositivos deba tener unos requerimientos tecnológicos e infraestructura, para implementar un diseño de redes más especializado y evaluar los costos de tal implementación.

A continuación, se nombran algunas soluciones implementadas del IoT:

- En el hogar permitirá darle órdenes a cada uno de los objetos configurados para realizar acciones predeterminadas.
- En cuanto al sector de la salud permitirá mejorar la calidad de vida, y mejora de los procedimientos médicos ya que permitirá monitorear con más precisión los síntomas y el estado de salud de cada uno de los pacientes.
- En la agricultura se puede reflejar el siguiente paso para el área rural ya que permitirá tener un control más detallado de las condiciones climatológicas y de los cultivos.
- En la parte de industria y comercio la implementación del IoT aumentara la capacidad de control en seguridad, calidad y producción.

La implementación de IoT genera un consumo más alto de energía causando que a futuro esto pueda ser un problema de alta demanda de energía teniendo así que implementar distintos medios de aumento de energía. [6]

## Características de IoT.

IoT ha aumentado en la capacidad de transmisión y procesamiento, anteriormente en la década del 2000 comenzó la propuesta de generar la tecnología necesaria para que IoT hoy en día sea una realidad avanzada, teniendo en cuenta el ahorro energético, también los costos que este con lleva para que sean asequibles para cualquier persona.

A continuación se observara las tecnologías que contribuyen al desarrollo de IoT en la Tabla1.

| ***Tecnologías que Contribuyen directamente al desarrollo de Internet de las Cosas*** | ***Tecnologías que pueden llegar a adicionar valor a Internet de las Cosas*** |
|---|---|
| Interfaces máquina-máquina (M2M) y protocolos de comunicación electrónica | Etiquetado Geográfico |
| Microcontroladores | Biometría |
| Comunicación inalámbrica | Máquinas de Visión |
| Tecnología RFID | Robótica |
| Tecnología de almacenamiento de energía | Realidad aumentada |
| Sensores | Escenarios paralelos |
| Actuadores | Tele presencia |
| Software | Interfaces tangibles |
| Tecnología de localización | Tecnologías limpias |

*Tabla 1.* Tecnologías de internet de las cosas.

IoT nació de ciertas tecnologías según afirma (Eduardo Sosa, 2014) "Radiofrecuencia (RFID) y de las redes inalámbricas de sensores (WSN). Las WSN han sido preferidas en estudios e interacción con el ambiente y situaciones de emergencias y desastres. RFID ha sido concebida como una herramienta ligada a las cadenas de abastecimiento de diferentes productos. Las primeras hacen uso de capacidades limitadas de procesamiento, almacenamiento, transmisión y agregación de Tecnologías que Contribuyen directamente al desarrollo de Internet de las Cosas." [7]

Los RFID son dispositivos pequeños los cuales pueden ser incorporados a cualquier cosa, existe mucha variedad de dispositivos con diferentes capacidades de comunicación y computo dependiendo el campo donde se requiera utilizar. Los avances de los sistemas Micro-eléctrico-Mecánicos (MEMS) y la computación en la nube, servicios Web, tecnología de sensores RFID (Radio Frecuency-ID) y UPnP (Universal Plug and Play) estas han surgido para la nueva era de IoT.

Se puede observar, analizar y comparar las diferentes arquitecturas que conforman la IoT. Se aclara que la estandarización es un proceso en desarrollo y los principales aportes que destacan la IEEE (Institute of Electrical and Electronics Engineers), 802.15 y el protocolo 802.15.4 se encarga de permitir la comunicación con bajas tasas de transmisión para trabajar con dispositivos de bajo costo y recursos limitados.

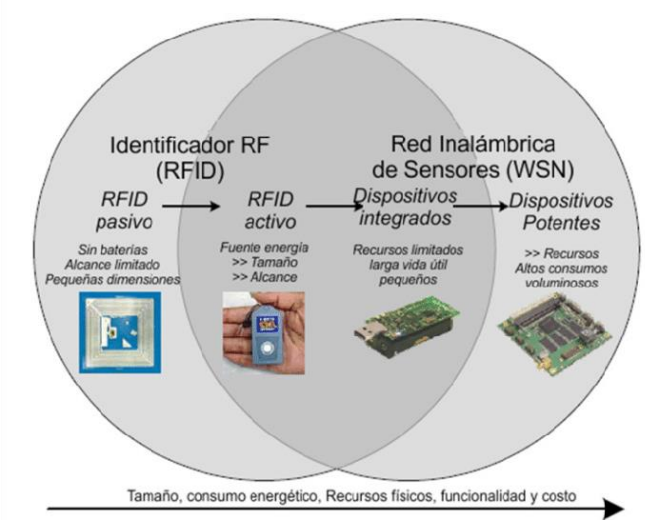


Figura1. Convergencia de tecnologías RFID y WSN.

Tomado de: [8]

## Protocolos y arquitectura.

IPV4 – IPV6

Los protocolos IP van de la mano con todo el proceso de interconectividad no solo a personas sino también a objetos esto significa que "Actualmente la IANA (Internet Assigned Numbers Authority) es responsable de la coordinación global de los sistemas de direccionamiento del Protocolo de Internet, así como los Números de Sistemas Autónomos utilizados

para enrutar el tráfico de Internet, hoy en día existen dos tipos de direcciones del Protocolo de Internet (IP) en uso activo: IP versión 4 (IPv4) e IP versión 6 (IPv6). IPv4 se desplegó inicialmente el 1 de enero de 1983 y sigue siendo la versión más utilizada. Las direcciones IPv4 son números de 32 bits, la implementación del protocolo IPv6 comenzó en 1999, las direcciones IPv6 son números de 128 bits lo que aumenta varias veces su capacidad de la red, las direcciones IPv4 e IPv6 se asignan generalmente de una manera jerárquica, a los usuarios se les asignan las direcciones IP de los proveedores de servicios de Internet (ISP). Los ISPs obtienen la asignación de direcciones IP a partir de un registro local de Internet (LIR) o Registro Nacional de Internet (RNI), o de su adecuado Registro Regional de Internet (RIR). Hoy en día las direcciones IPV4 son insuficientes para satisfacer la demanda puesto que está limitado a 4.3 mil millones de direcciones, la dirección IPV4 es un número formado por 4 octetos dando un valor de 32 bits, cada día los usuarios incrementan en el uso de internet, ahora que llega el sistema de interconexión de objetos, se requiere de mayor asignación de direcciones IP, para ello se implementa el protocolo de direccionamiento IPV6 formada por 128 bits, cuenta con mayor seguridad y espacio de direccionamiento y movilidad, además mejora la compatibilidad del servicio y su infraestructura, ya que genera un enrutamiento eficaz y autoconfiguración. [9]

IPV6 ahorra el procesamiento y ancho de banda, tienen una etiqueta llamada (Flow Label) esta permite enviar información respecto a la calidad del servicio, genera a los usuarios calidad de acuerdo a sus necesidades. Existe diferencias entre la versión 4 y 6 como: ampliación del tamaño de la dirección, privacidad y autenticación para generar integridad en los datos, estos dos protocolos deben realizar una integración utilizara dos técnicas, una es DUAL STACK y DTTS.

**DUAL STACK:** es una técnica de integración donde el nodo tiene conectividad para los dos protocolos IPV4 e IPV6, es recomendada para admitir ambos protocolos, cada nodo tendrá la configuración de dos stacks.

**DTTS (Dynamic Tunneling Technique):** es una técnica de túnel donde se puede implementar en la infraestructura de reenvió de IPV6 mientras IPV4 será la base.

Como tal los próximos desarrollos de aplicaciones y servicios serán implementados con el protocolo IPV6, por eso Internet de las cosas necesita de seguridad en la información por los grandes volúmenes de información que manejan, por ende el protocolo IPV6 proporciona una capa de seguridad en la red, este proceso se realiza por medio de IPsec el cual define dos servicios de protocolo de seguridad de encapsulado tales como: ESP ( encargado de proporcionar confidencialidad, protección, autenticaciones) y la cabecera de autenticación AH ( proporciona autenticación en el origen de los datos y protección de reproducción).

Bajo los estándares del IEEE 802.15 y 802.15.4 se puede encontrar diferentes propuestas y protocolos de la capa de aplicación que corre sobre UDP permitiendo conectar dispositivos con recursos limitados a través de la Web, el protocolo

RPL (IPv6 Routing Protocol for Lower and Lossy Networks), protocolo de capa de red que permite trabajar los dispositivos limitados o el 6LoWPAN (IPv6 over Low power Wireless Personal Área Networks), o protocolos de organizaciones que se destacan como SOAP (Simple Object Access Protocol) que define como los objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML etc…

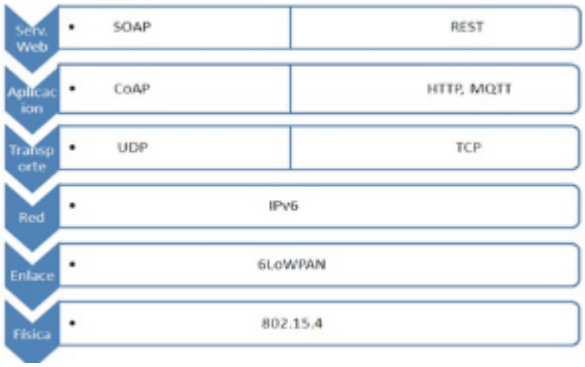


Figura 2. Stacks de protocolos de la arquitectura IOT

Tomado de: [10]

802.15.4 Estándar que permite trabajar con recursos limitados, consumo eficiente de energía y empleo de tasas de transmisión baja, donde dentro de este protocolo se destaca la comunicación ZigBee y tecnología de sensores RFID.

En el área de capa de enlace se encuentra el estándar 6LoWPAN, permite emplear 802.15.4 a IPV6, siendo este el único estándar que tiene una infraestructura de red existente permitiendo la asignación de Ip sin ninguna limitación.

También se puede conocer que funcionamiento tienen en la capa de aplicación los protocolos como CoAP, HTTP y MQTT y otros conocidos tales como FTP, SMTP y JMS. En conclusión se puede ver todos los factores que benefician la arquitectura, permite resolver el problema en sectores específicos y en las intercomunicaciones de objetos por medio de protocolos de internet estandarizados.

De Acuerdo a la afirmación del autor(a) Dana Rodríguez González del artículo, la implementación de gestión de IoT se divide en cuatro grupos como:

**SNMP (Simple Network Management Protocol)** para la gestión de este protocolo deben suplir las limitantes, en caso de no ser así no serán implementadas de forma eficaz para gestionar la IoT las limitantes de este protocolo se encuentran en RFC35126, por ello se deben realizar modificaciones, tales como: gestionar elementos instalando un agente por cada dispositivo, gestor local en cada Gateway y remoto en la infraestructura de red IP existente.

Las modificaciones para este protocolo serán:

1. Emplear el broadcast para transmisión del mensaje y configuración de los dispositivos ahorrando potencia en caso de que se gestionen dispositivos similares.
2. Incorporar un GETREquest PDU y StopGETRequest PDU de forma periódica, encargada de optimizar la energía.

3. Comprimir el mensaje SNMP para igualmente reducir el consumo de energía.

**TMN (Telecomunication Network Management).**

Permite combinar la robustez de CMIP; es un protocolo que define la información entre aplicaciones de gestión con la interoperabilidad de CORBA; conocido como un framework encargado de entrar en el grupo de sistema de gestión, estos sistemas aportan modularidad, abstracción y reutilización del software.

**WBEM (Web Based Enterprise Management)**

Es una iniciativa que provee un conjunto de estándares y tecnologías enfocados en la gestión de internet unificando los sistemas de gestión de redes, usuarios y aplicaciones. Tiene como componente fundamental (WBEM-Client) siendo intermediario entre el gestor y el dispositivo, la ventaja del manejo de este, es que obtiene la información a partir de una comunicación directa con el CIMOM (pieza clave del WBEM-Server) empleando mensajes. Por otro lado el WBEM-server permite ocultar los detalles de comunicación del gestor, los proveedores, adicionalmente enruta la información de los objetos y eventos.

**PBM (Policy Based Management)**

Este tipo de gestión modifica el rol del operador, no controla el sistema directamente, solo pasa a realizar funciones de la descripción de políticas, solventa problemas de gestión en los dispositivos complejos, como tal la gestión autonóma, se encarga de configuraciones de auto-configuración, auto-reparación, auto-optimización y auto-protección, permitiendo automatizar el trabajo. [11]

## Redes alámbricas e inalámbricas.

Las redes cableadas serán muy utilizadas por las aplicaciones SCADA las redes basadas en IP, M2M, son muy utilizadas por la cantidad de protocolos que manejan tales como SS7 (conmutación de paquetes que mantiene unido la conmutación de circuitos) y DOCSIS (estándar que permite la transferencia de datos a alta velocidad a un sistema de televisión) estas redes son opciones para plan de convergencia, actualmente DOCSIS proporciona internet por medio de HFC (hybridfiber-coaxial).

Las redes inalámbricas se clasifican de corto y largo alcance. En el grupo de corto alcance se encuentra NFC, PAN, LAN, MAN, RFID, WIFI, WiMAX etc. Dentro del grupo de largo alcance se encuentra WAN, GSM, CDMA, WCDMA o comunicación vía satélite. Se espera que aparezcan nuevos estándares en las redes inalámbricas para alcanzar lo propuesto en IoT.

Un ejemplo de cómo funciona un PLCs es que la cadena de control es el bus que une los PLCs de los componentes de los dispositivos IoT que realmente hacen el trabajo, tales como sensores, actuadores, motores eléctricos, la consola, luces, interruptores, válvulas, y contactores. El protocolo industrial común (CIP) es la base para una familia de tecnologías afines

y tiene numerosos beneficios tanto para los fabricantes de dispositivos y los usuarios de los sistemas de automatización industrial. La primera de las tecnologías basadas en CIP, fue DeviceNet, surgió en 1994 y es una implementación del CIP sobre CAN (Controller Area Network), que proporciona la capa de enlace de datos para DeviceNet." [12]

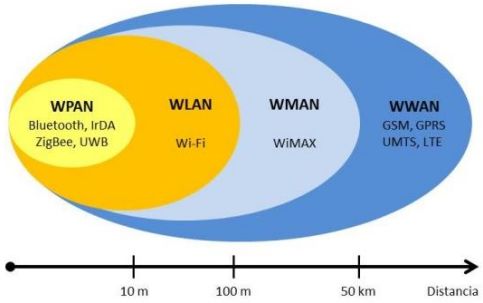


Figura 3. Clasificación Redes inalámbricas de corto y largo alcance.

Tomado de: [13]

## Tipos de conexiones y modelos de comunicación de IoT.

**M2M:** La conexión máquina a máquina permite que los dispositivos conectados en red intercambien información y realicen acciones sin necesidad de intervención manual, de este modo facilita el desarrollo de actividades en diferentes sectores.

**M2P:** En las conexiones máquina a persona, los sistemas técnicos interactúan con las personas y las organizaciones para proporcionar o recibir información, es intercambio transaccional por el flujo de datos que transmite en ambas direcciones.

**P2P:** Las conexiones persona a persona emplea recursos del ecosistema IoT es una conexión bidireccional de datos, son soluciones cooperativas que aprovechan la infraestructura, los dispositivos y las aplicaciones de red existentes para permitir la comunicación y la colaboración sin inconvenientes entre las personas. [14]

**Comunicación de dispositivo a puerta de enlace:** En este tipo de comunicación los dispositivos se conectan a un dispositivo intermediario para acceder a la nube, esto implica software o aplicaciones que operen en un dispositivo de puerta enlace local actuando como intermediario entre el dispositivo y el servicio en la nube. La puerta de enlace puede proporcionar seguridad, traducción de protocolos o datos.

**Comunicación de dispositivo a la nube:** En este tipo de comunicación el dispositivo se conecta directamente a un servicio en la nube de internet, la conectividad a la nube permite obtener acceso remoto a un dispositivo y tiene compatibilidad para las actualizaciones del software para el dispositivo, utiliza conexiones Wi-Fi, Ethernet o tecnología celular como la red 4.5G.

**Comunicación de dispositivo a dispositivo:** Este tipo de conexión se puede realizar de dos a más dispositivos conectándose directamente y comunicándose entre sí por medio de diferentes redes como; Ip o internet, bluetooth, Z-

Wave y ZigBee. Es utilizado en sistema de automatización para transferir pequeños paquetes de datos entre dispositivos a una velocidad de datos baja.

**Back End Data Sharing:** Es una comunicación de dispositivo a la nube especialmente para que solo las personas autorizadas puedan acceder a los dispositivos o datos del sensor, por este modelo se puede analizar y exportar datos de objetos inteligentes desde el servicio en la nube. [15]

## Evolución de las redes dentro de IoT.

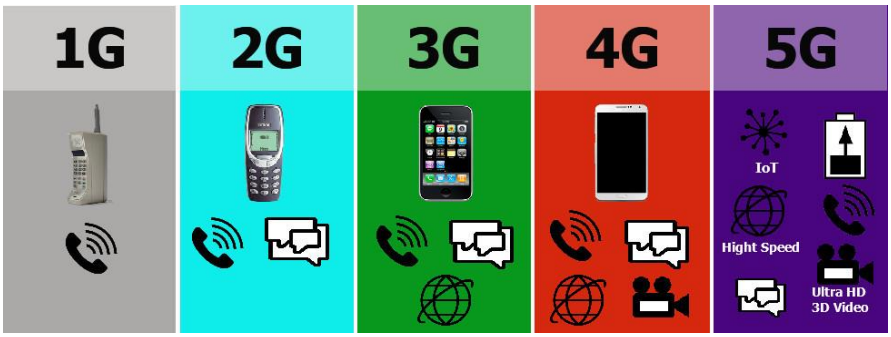


Figura 4. Evolución de 1G a 5G.

Tomado de: [16]

**Red 1G:** fue la primera red de comunicación móvil analógica lanzada en 1979, solo manejaba servicio de voz, la cobertura era intermitente, el estándar que utilizaba era AMPS (Advanced Mobile Phone System), la multiplexacion FDMA y la frecuencia de 800 a 900 MHz, en ese momento era mala la comunicación y no existían seguridad en las llamadas de voz.

**Red 2G:** llega los procesos digitales facilita voz y datos, roaming internacional, llamada en espera, retención de llamada, transferencia de llamada, bloqueo de llamadas, SMS etc... La velocidad era de 14kbps a 64 Kbps, manejaba tecnología TDMA y CDMA, la Banda de frecuencia - 850 - 1900 MHz (GSM) y 825 - 849 MHz (CDMA).

**Red 3G:** esta generación integra el aumento de la tasa de datos, mayor capacidad en voz y datos, alta transmisión a bajo costo, llega a facilitar la transferencia de archivos multimedia, trabaja con el estándar UMTS (WCDMA) basado en GSM y CDMA. Aplicaba para servicio de acceso a internet de alta velocidad, video, chat, conferencia, televisión móvil, multimedia, mapas de navegación etc.

**Red 4G:** como característica principal proporciona alta velocidad, calidad, capacidad y seguridad, esta generación se basó en IP. Inicio en 2008 a 2010 bajo el estándar LTE-TDD y LTE-FDD (Long-Term Evolution Time-Division Duplex) y WiMAX 802.16m, tiene ancho de banda más amplio y la tecnología de multiplexación es OFDM, MC-CDMA, CDMA, aplica para servicios de acceso móvil web, telefonía IP, video conferencia, televisión, DVB Digital Video Broadcasting.

**Red 5G:** inicio en el año 2015 el objetivo de esta generación es mejorar el ecosistema IoT, maneja estándares IP, LAN, WAN, PAN, alta velocidad, rendimiento en tiempo real, velocidad de 1 a 10Gbps, especialmente aplica para soportar internet de las cosas y M2M ofreciendo más cobertura, eficiencia, ahora las personas y los dispositivos pueden estar conectados desde cualquier lugar, porque permite la interconexión de equipos inteligentes bajo el esquema de velocidad, latencia, costo. [17]

## Tecnologías de comunicación para IoT.

| TECNOLOGÍA | CONSUMO | ALCANCE | MADUREZ | DISPONIBILIDAD | SEGURIDAD | USABILIDAD | TASA DE DATOS |
|---|---|---|---|---|---|---|---|
| GSM/GPRS | Muy alto | Alto | Muy Alto | Muy alto | Alta | Alta | Alta |
| SigFox | Bajo | Medio | Alto | Medio | Media | Alta | Muy baja |
| LoRa | Bajo | Medio | Bajo | Muy bajo (ad hoc) | N A | Baja | Muy baja |
| NB IoT | | | | | | | |
| WiFi | Alto | Bajo | Muy alto | Alto | Baja | Alta | Muy alta |
| BLE | Muy bajo | Muy bajo | Alto | Bajo | Baja | Media | Baja |
| ZigBee | Medio | Bajo | Medio | Muy bajo | Alta | Baja | Baja |

Figura 5. Redes de comunicación utilizadas en IoT.

Tomada de: [18]

**M2M GSM/GPRS:** Actualmente es la más comercializada y ofrecida por los operadores de telefonía, la conexión máquina-máquina tiene ciertas desventajas como: alto costo para volumen de datos pequeños, el volumen de datos debe superar 1MB y consume mucha batería.

**SIGFOX (La red alternativa para IoT):** es una red de comunicaciones LPWA **(**Low Power Wide Área) Network no requiere de una licencia para ofrecerla en el mercado por eso se ha transformado en operador de su propia tecnología, está construida sobre una modulación UNB (ultra narrow band), es una tecnología de bajo costo y los dispositivos IoT se han adaptado a esta tecnología.

**LoRa (alianza de IoT):** es una red que tiene características similares con SIGFOX ya que pertenece a la red LPWAN, es diferente en cuanto al espectro ya que es más amplio, es compatible con IPV6, además incluye portales que se conecten al servidor de red central y está mejor preparada para la comunicación bidireccional en tiempo real. También incorpora encriptación para la seguridad en el dispositivo y en la red.

**NB IoT (NarrowBand IoT):** es otra tecnología LPWAN, en el espectro está dentro del rango de LTE o 4G, ha decidido lanzar los servicios para consumo masivo y de pocos datos sobre su propia red, tienen estándares para que los dispositivos que se conecten a la red lo realicen sin restricciones. [19]

**BLE (Bluetooth de baja energía):** Bluetooth ULP Ultra Low-Energy es una tecnología inalámbrica, está enfocado en el campo de aplicaciones de IoT a pequeña escala que envían pequeñas cantidades de datos, reducen el consumo de energía sin afectar el rango de comunicación, sirve para localización de activos o implementación en electrodomésticos. [20]

**ZigBee (Radiodifusión digital de bajo consumo):** es una tecnología inalámbrica, utilizada en aplicaciones domóticas e industriales, de bajo consumo tiene alta escalabilidad y capacidad para soportar gran número de nodos, es robusto y tiene más seguridad que los anteriores, la cobertura que puede brindar es de 100 metros.

## Vulnerabilidades y soluciones en la integridad de seguridad de la información en el IoT.

La IoT se ha implementado de acuerdo con el éxito que logra día a día, además por la cantidad de dispositivos que ya han sido conectados a internet, se pueden encontrar vulnerabilidades, ya que es un objetivo clave del ciberdelito. Por esta razón si hay un mal diseño en la interconexión al dispositivo, el usuario puede verse afectado por desprotegimiento de la información. En la actualidad las personas se han vuelto dependientes del funcionamiento de IoT por los servicios que ofrece, pero no han llegado a analizar que las redes son inseguras y de los cuidados del usuario frente al manejo de esta tecnología.

IoT presenta ciertos problemas puesto que sus capacidades tienden a ser limitadas, generando inseguridad en las conexiones y difusión de información, permitiendo así tipos de ataques de Denegación de servicio.

Puesto al inconveniente con el ataque nombrado anteriormente se encuentran algunas posibles soluciones:

- Revisar los recursos de la red para la inversión en la seguridad por la vulnerabilidad de la información.
- Detección o monitoreo de anomalías, análisis de los datos transmitidos para la prevención de los ataques y evitar la propagación de este.
- Controlar tráfico generado por los dispositivos IoT por medio del Proxy.

IoT busca lograr dar mayor seguridad, mediante el uso de métodos en todos los contextos aplicados bajo su objetivo, generando así una mayor resistencia, algunas de estas se pueden ver en un buen sistema de autenticación, sistema de control, monitoreo del envió de la información, puesto que hoy en día se han generado cambios en los tipos de comunicación peer to machine, m2m, mejorando los procesos y ofreciendo diferentes servicios. [21]

Existe 3 elementos fundamentales a tener en cuenta frente a la seguridad de la información: confidencialidad, integridad y disponibilidad, donde en nuestro documento nos enfocaremos a la privacidad en la cual se ven aspectos de violaciones de datos hechas por cracking, negligencia del empleado, datos en tránsito, robo de información privilegiada, exposición accidental etc. Esto pasa por la falta de políticas o procedimientos, la mala gestión del control de accesos o

mala administración de la información sin tener un plan de continuidad que ayude a prevenir las situaciones de contingencia.

Se pueden encontrar diferentes estadísticas de vulnerabilidades de la información en diferentes países, los riesgos asociados que afecta la evolución de IoT y los inconvenientes en la integridad en la información.

Actualmente las empresas sienten preocupación por la fuga de información y la falta de disponibilidad, los riesgos más comunes son:

- Robo de información.
- Ubicación mediante dispositivos GPS.
- Mal uso de los elementos IoT.

Para analizar las vulnerabilidades de ataque al IoT se debe tomar en cuenta los vectores de ataque, los dispositivos IoT que acceden por otros medios a una interfaz de administración, pues estos no tienen una entrada o salida de datos directa. Los usuarios no tienen los suficientes conocimientos de seguridad en los dispositivos, según el análisis que realizo Henry Castillo, que indica que el 86% de estos equipos tienen una configuración insegura. [22]

Retomaremos de manera abreviada y general el comportamiento de las capas de arquitectura técnica compuesta del IoT:

- Capa de percepción.
- Capa de red.
- Capa de aplicación.

La capa de percepción es la que identifica los tipos de objetos y recolección los datos, mediante dispositivos como sensores, teléfonos inteligentes, etiquetas de identificadores por radiofrecuencia (RFID) entre otros, donde luego son transferidos a la capa de red equivalente a un medio inalámbrico o alámbrico para que ocurra una propagación y transmisión de datos, mientras que la capa de aplicación es la de la interactividad con el usuario mediante interfaces y diferentes utilidades haciendo uso de protocolos como http, https, entre otros.

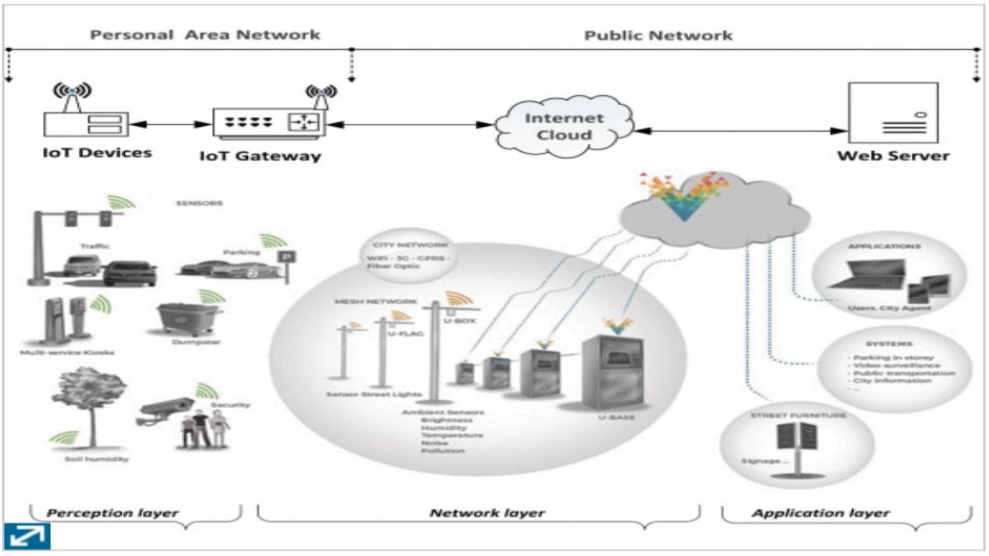


Figura 6. Arquitectura genérica de capas del IoT y su aplicación.

Tomado de: [23]

## Problemas de privacidad del IoT.

La privacidad se define como el derecho de selección de la información personal de cada individuo de manera específica es pública o no frente a las demás personas, donde de cierto modo esta se ve vulnerada bajo la división de tres espacios: la recolección de los datos, espacio de control del usuario y el espacio de conocimiento del usuario. [24]

Identificación y seguimiento individual, perfil de usuario, interacción y presentación, transiciones del ciclo de vida, ataques de inventario y vinculación, donde el perfil del usuario es considerado la mayor amenaza.

Las U-city bajo conectividades ubicuas como se observa en la figura 6, presenta inconvenientes en relación con la privacidad acerca de la información personal e información de la vida diaria, tales como privacidad humana, privacidad de la ubicación y la privacidad del objeto. [25]

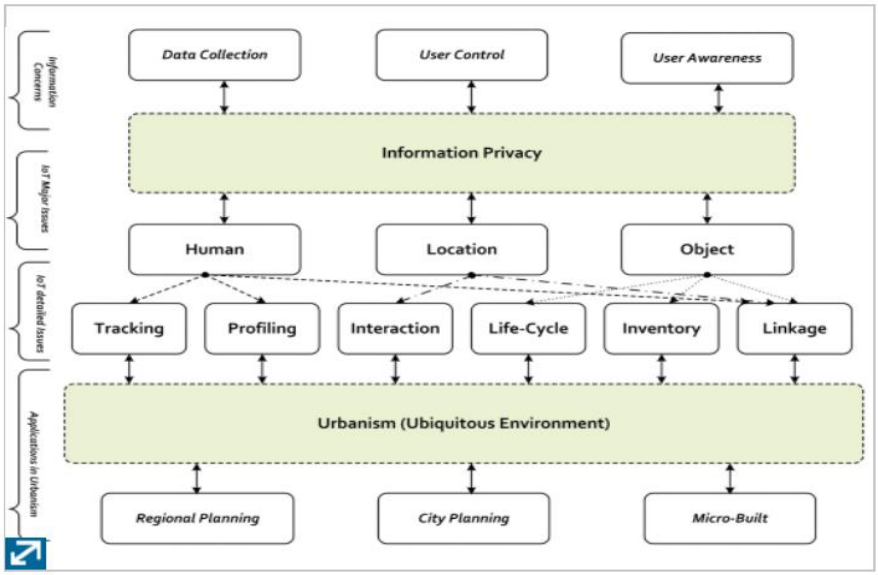


Figura 7. Entorno ubicuo y vinculación con el urbanismo desde varias perspectivas, y amenazas expuestas de la privacidad en los entornos.

Tomado de: [26]

Para garantizar la protección de los flujos de datos dentro de un ámbito IoT se recomienda poner atención a las puertas de enlace, entre otros requisitos como la mejora en la autenticación de datos, privacidad del cliente para evitar interferencias sobre una persona en específica. [27]

Se indica que el 25% de los ataques cibernéticos en el año del 2013 fueron alrededor de 750000 mensajes de correo electrónico tipo spam, provinieron principalmente de las cosas inteligentes, entre estos los electrodomésticos. El problema se establece desde la recopilación de datos por cada uno de los dispositivos por hogar y luego las ciudades inteligentes. [28]

En busca de soluciones de privacidad de IoT a nivel urbano se da la opción de mejoras e implementaciones en la legislación de cada nación respecto a su manejo, al igual se espera también leyes e iniciativa de la asociación internacional de privacidad, sugeridas por la naciones unidas en búsqueda de dictámenes de protocolos de seguridad del IoT, de este modo mejorar la capacidad de implantar sanciones iguales en todos los países y los fallos puedan ser los mismos tanto en el extranjero como en la nación, cuyos regímenes a actuar son las participaciones organizativas, gubernamentales y un entorno legislativo donde los temas a tratar son la privacidad, anonimato de datos, administraciones de identidad y cómo estos se almacenan, recopilan, la igual que también sus movimientos y manipulación de datos. Ya que los datos IoT se encontraran rondando a un nivel global. [29]

Al igual que en un ámbito empresarial multinacional IoT tendría dificultades frente al ancho de banda acceso y bloqueo de la nube de aplicación, para ello obtener una mejor calidad y control de flujo se vincula el big data.

Hoy en día ha avanzado el uso de internet para el funcionamiento de los servicios y aplicaciones, principalmente comenzó con la computación, pero ha mejorado a que sea en la nube, una evolución impactante que ha tenido.
Actualmente ha sido muy fácil la implementación de la computación en la nube por bajos costos y porque la información se encuentra disponible desde cualquier lugar u hora, el internet de hoy ofrece video, datos y voz, ahora con la implementación de internet de las cosas se puede comunicar cualquier objeto y hace referencia a que los objetos se convierten en nodos de comunicación a través de internet, la comunicación entre el hombre y las cosas ya es un hecho.
La integración de computación en la nube e internet de las cosas busca optimizar ciertas funciones como; implementación de Ipv6, soporte de protocolos, eficiencia energética, seguridad y privacidad de los datos, calidad de servicio y almacenamiento de los datos. [30]
Crece la ciberdelincuencia en las redes con diseños de malware actuales e innovadores de manera progresiva utilizando ataques de tipo mutación. Por lo tanto se busca soluciones técnicas en defensa para este o demás ataques y se propone el uso de IDS e IPS.
(Alsunbul et al) muestra un sistema de defensa de red para detección de intentos de acceso no autorizado, mediante la presentación de un nuevo protocolo estándar, cuya finalidad es realizar una confusión en los intentos de sniffing; respecto al enrutamiento, puesto que las rutas cambian periódicamente, para evitar accesos no autorizados y seguimiento de tráfico.
Zitta, Neruda y votech en el dispositivo frambuesa pi 3,aplicada para la alta frecuencia (UHF) e identificación por radio frecuencia(RFID),de lectores que utilicen protocolos (LLRP);fails2ban y suricata son los protocolos seleccionados por su alta escalabilidad, considerado el más adecuado para trabajo con sensores, nube y servidores.
Suricata presenta mayor rendimiento frente a otro tipo de IDS e IPS como snort cuyas resultados fueron observados al lanzar un DDOS donde suricata respondió mejor a este, en un solo núcleo al igual que en varios núcleos.
Chan y ramachandran proponen una seguridad multicapa para cloud computing, teniendo en cuenta que la criptografía es usada para proporcionar confidencialidad e integridad de los datos, de tal forma que en la primera capa de seguridad se plantea es la imposición de un firewall y controles de acceso. En la segunda capa se aplican los IPS en administración de identidad, enfoque de eliminación de archivos maliciosos. En la tercera capa se observa un cifrado convergente que genera una política de seguridad descendente, para el cual se realizaron pruebas de penetración cuyos resultados pronosticaron que el tiempo en que tarda en recuperarse de un acceso no autorizado está en un mínimo

de 125 horas; otra de las soluciones de seguridad por Makkaoui, indica un modelo de seguridad y privacidad en la nube (CSPM) de varias capas, las cuales son:

(PESL) Capa de seguridad de infraestructura en la nube.

(NSL)Capa de seguridad de red.

(DL) capa de datos.

(ACPML) control de acceso y capa de gestión de privilegios. [31]

Podemos observar que otra técnica mediante la mejora de autenticación de las VPN y uso de sistemas de posicionamiento global (GPS), proporciona protección de geo privacidad para móviles.

Los honeypot y honeynet no pueden faltar, en este caso Olagunju y Samu implementaron un honeypot automatizado aplicando el uso de la técnica de gestión de sistema de registro centralizado (títere, máquinas virtuales),logrando recopilar información de dirección origen, hora, país de donde proviene el ataque, para ello lo primero a realizar es servir la trampa hacia el atacante, un protocolo de transferencia de archivos es el indicado mediante estos los atacantes dejan ver sus rastros nombrados anteriormente. [32]

### Soluciones técnicas de clasificación por estructura de red.

En los métodos de clasificación de estructura de red, Filipe y hudec proponen un modelo de seguridad para redes MANET, cuyas redes orientadas en protocolos que permitan eficiencia en ancho de banda respecto a las propiedades flexibilidad y movilidad. Los protocolos a utilizar son basados en RSA el cual es un protocolo seguro de enrutamiento incluyendo PKI ,firewall e IPS cuyos paquetes de enrutamiento están firmados y las claves son de carácter simétricas para cifrar el tráfico, mientras el IPS monitorea el tráfico alertando de nodos sospechosos, la consecuencia de llevar este planteamiento son encontrados con límites de tráfico debido a los dispositivos firewall, latencia de alta respuesta por el envío de paquetes por cada nodo, comparación con base a búsquedas en bases de datos, cifrado y control.

Un IDS especializado para sensores de redes inalámbricas, con la utilización técnica de comparación de patrones, donde estos si coinciden, son administrados mediante el conjunto de políticas, reglas implantadas en el IDS, este después prosigue con un análisis de datos de recopilación, para luego ser comparados con políticas puestas en IDS, de obtener resultados frustrados este notifica una alerta. [33]

### Clasificación por aplicación.

Los sistemas de riesgo electrónico de salud, se plantean en tres medidas preventivas aplicadas a la detección, prevención y corrección, empezando por el sistema de prevención, que mediante el uso de contraseñas y paráfrasis y varias maneras de autenticación, todo esto obtenido bajo IDS/IPS para detecciones de un ataque, al igual que el manejo

del control (administración, respaldos del sistema), que en caso de algún tipo de ataque, sea posible restaurar la configuración y administración.

Otra solución es el desarrollo de un sistema inmune, es la selección clonal conformada de un IDPS basado en host de manera híbrida obteniendo cantidad de datos para analizar. [34]

### Seguridad predictiva.

Relativamente este tema o refrán ha salido hace poco, enfocado a la prevención en la seguridad cibernética, mediante la detección, reparación, garantizando ataques existentes y a futuro dentro de las redes.

Noureddine. Basado en la teoría general de la disuasión que está impulsada por la toma de decisiones del ser humano, realizaron estudios del comportamiento humano en la seguridad cibernética teniendo en cuenta campos como psicología, ciencias sociales, para lograr así la construcción de modelos predictivos de seguridad para indagar la efectividad de la seguridad de las contraseñas y auditorías. En frecuentes búsquedas de vulnerabilidades, teniendo en cuenta las herramientas que manejan el usuario en especial la autenticación, se utilizó un estudio de caso para observar el comportamiento de los representantes de servicio al cliente y redes de actividad estocástica para la modelación de interacción entre los empleados y las políticas de seguridad de la organización, cuyo modelado de estudio está dividido en varias fases, nombramos el primero desde la perspectiva del atacante, perspectiva de los empleados, y administradores, mediante técnicas de granularidad distinta por fase, cuya palabra se puede describir como la relación de cómputo a comunicación en un programa paralelo.[35]

En cuestiones de protección de infraestructura Abraham y Nahir propusieron la implementación de un nuevo modelo estocástico evaluando la seguridad enfocado a resultados de ataques frente a la infraestructura, luego se define un modelo markov (modelado estocástico para cambios de sistemas aleatorios) dependiente a variables en el tiempo teniendo en cuenta gráficas de ataques y aspectos como la longevidad del ataque y tasa de descubrimiento de vulnerabilidad, para así mismo dar posibles resultados de ataques futuros de estados de seguridad de la red en actividad de detección de ataques día cero. Mediante el marco de puntuación de vulnerabilidad CVSS. [36]

Para la recolección de rasgos de explotabilidades complejas, como tipos de acceso, autenticación y vector de acceso, se llevaron otros estudios mediante los análisis de impacto, generación de gráficos para hacer uso del CVSS, dando resultados en cuanto a la explotabilidad, impacto y el alineamiento de inclusión de vulnerabilidades mediante el uso de un árbol de ataque.

En las antiguas secciones se puede observar distintas soluciones de seguridad de enfoque en el IoT, sin embargo más allá de los estudios estocásticos, aplicación de software IDS, IPS, IDPS. Se ve que no se abarca toda la seguridad de los datos donde para ello al igual se propone la implementación del blockchain en conjunto de seguridad para el IoT,

considerándolo una de varias ideas de seguridad de los datos puesto que el tráfico IoT va a ser expansivo y divulgado en varias redes de manera descentralizada, mediante el uso de blockchain y redes inteligentes que se hace de aplicación de la integridad de los datos.

La tendencia desde el nacimiento de blockchain, es originalmente para tipos de transferencias financieras de bitcoin, criptomonedas, donde cuyas transacciones son difíciles de rastrear y detectar fácilmente por un intruso.

## Blockchain

Es buena idea el uso de blockchain para la seguridad IoT porque este tipo de lenguaje ha sido usado para registros, transacciones financieras, entre las cuales están las criptomonedas, el bitcoin, dando resultados con transparencia y rastreo de detección de modificaciones, con base en esto se muestran dos formas de uso del blockchain a IoT.

Primer tipo:

En esta se crea el bloque cuando se ejecuta la transacción, este se propaga en todos los nodos de la red donde uno de estos nodos valida el bloque siendo este proceso llamado el minado en bitcoin, este luego lo esparce por la red, donde cada uno de los nodos agregan los respectivos bloques de acuerdo a su secuencia de su cadena de bloques.

Por otro lado el método dos consta de un intercambio de datos garantizando la integridad de los mismos haciendo uso de la métrica de integridad de referencia, de tal modo que este enfoque circula de la siguiente manera dentro de una red; se encuentra un punto centralizado cuyo propósito es mantener las referencias de repositorios miembros y de cierta manera se almacenan y se distribuyen los conjuntos de datos, cuyos datos como la información de dirección, membresía, propietario y uso compartido prevalece dentro de la cadena de bloques, independiente de la cadena de bloques del RIM (métrica de integridad de referencia). [37]

Se difiere del anterior método que cuando los conjuntos de datos son publicados disponibles, se encuentra la falencia cautelosa de un no manejo administrativo de tipo automatizado de anonimato en la publicidad de los conjuntos de datos antes de ser publicados, al igual otro tipo de reto a tener en cuenta frente a las implementaciones del blockchain con IoT el ciclo de vida del conjunto de datos respecto a su compartimiento con los demás nodos, puesto que los propietarios de un conjunto de datos no querrán la visibilidad constante de estos, después de realizar el registro de cadena de bloques, estos no pueden ser eliminados o modificados, de ser así se pierde la trazabilidad en la cadena, ya que allí se puede encontrar el RIM y los conjuntos de datos no se encontraran con la disponibilidad para su divulgación.

Podemos indicar algunas características del blockchain que de cierto modo puede garantizar las transacciones frente al IoT puesto que a su versatilidad y cadena de bloques en manejo descentralizado, mediante el respeto de la misma cadena de bloques, es decir posee un orden en cada uno de estos bloques identificados por una cabecera que es única y es conocida por su bloque siguiente de acuerdo a la secuencia(bloque 1, bloque 2 ) en cadena manejando una

llave pública que es transmitida a todos los nodos de la red y luego se utiliza criptografía asimétrica, con cada uno de los mismos para las llaves privadas, otra característica que nos brinda blockchain en la integridad mediante la cadena de bloques, es que las transacciones tienen que ser coherentes y basadas en una anterior transacción registradas en el sistema descentralizado de mineros y secuencia consecutiva sin saltos en los bloques por cada transacción, referente a las colisiones respecto a blockchain, debido a su uso descentralizado los mineros o nodos de este sistema trabajan de manera homogénea mediante la comunicación en la red de peer to peer, para la búsqueda de la solución que se notifica a los demás nodos que ya fue encontrada, podríamos indicar que el blockchain sería ese libro de bases de datos de todos las transacciones realizadas por P2P o M2M las cuales son registradas y divulgadas a todo los nodos de la red, de tal modo que nuestras transacciones son registradas en una red de máquinas a diferencia de los sistemas centralizados y no se genera un registro tan exacto de cada transacción o petición. [38]

Detección de riesgos expuestos en el Firmware del IoT y de la proposición del blockchain como herramienta auto curable: Podríamos enfrentar este tipo de inconvenientes cuando se presenta un ataque hacia un dispositivo expuesto IoT mediante la técnica de denegación de servicio distribuido, el cual es uno de los que más afecta este tipo de dispositivos, donde se indica que una de las posibles causas de que este dispositivo fuese expuesto, es por falta de parches de actualizaciones en el firmware, o por violación de técnica de ataque por fuerza bruta, donde estos elemento después de ser atacado, el personal de tecnología o infraestructura es el encargado de la solución al inconveniente de manera manual, ejecutan el parche de actualizaciones pero no garantiza la integridad, puesto que la solución está después de haber sucedido el hecho.

Blockchain como base de datos distribuida encargada del seguimiento de cada una de las transacciones solicitadas y después registradas en cada uno de los dispositivos activos dentro de la red los cuales conservan todos estos la misma información con transparencia, al menos que un ataque logre comprometer la principal parte de los nodos de la red, la integridad desde este aspecto no se ve comprometida, en el IoT con blockchain los firmware serán de autoconfiguración y se auto actualizarán cambiando ciertos aspectos en firmwares normalmente usados que se guardan en un lugar seguro como el sistema raíz con un acceso de solo lectura.

La auto curación de los firmware de estos dispositivos por parte del blockchain es mediante la redundancia para sanar el software dañado, a través del reemplazo de código, o cuando se encuentra un firmware comprometido también es reemplazado por otro para obtener mejoras, actualizaciones, de todos estos procedimientos nombrados anteriormente, podemos obtener un acceso de registro de historia del firmware mediante la cadena de bloques.

Los dispositivos IoT deben contar con una interfaz de depuración, por ejemplo JTAG, ya que estos están siempre en red, para hacer posible de actualizaciones remotas, donde la autenticación es vital para no permitir modificaciones, donde

luego de ser autenticado, una lógica de recuperación adapta el firmware nuevo, a través de la interfaz de depuración o red, que actualiza la memoria flash y calcula el RIM metadata. [39]

Ahora en la contextualización de los niveles del IoT los cuales son campos residenciales, urbano, o red de superposición y almacenamiento en la nube, donde los aspectos fundamentales son la seguridad, la descentralización, administración de energía y anonimato, se observa un enfoque de optimización de blockchain enfocado a una casa residencial.

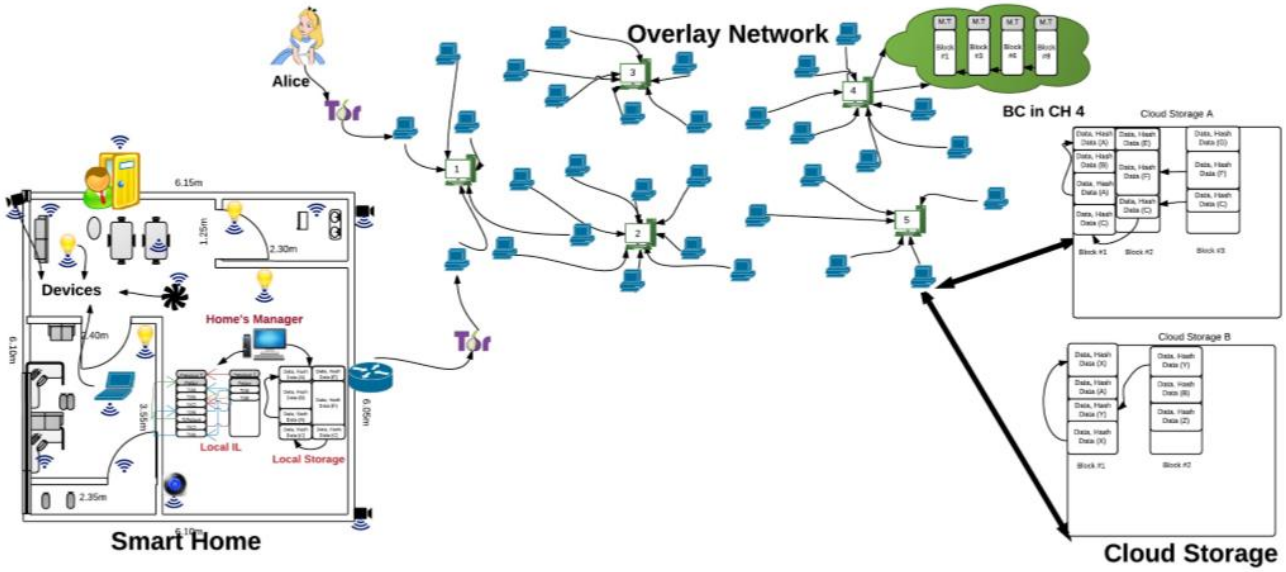


Figura6. Composición de una Smart home mediante blockchain

Tomado de: [40]

La Smart home dispone de un, IL local y un almacenamiento local como se observa en la anterior figura, donde los IL privado local asemejado a una administración blockchain pero de manera centralizada siendo dirigida por un SHM (administrador de casa inteligente),el cual procesa las transacciones entrantes y salientes mediante el uso de una clave compartida para la divulgación local, adicionalmente se administra un manejo de políticas prolongadas por el usuario para permitir o denegar difusiones en una red P2P. Los nodos como el SHM, teléfono inteligente o pc ayudarán en mejoras de latencia y sobrecarga en la red.

Para hablar acerca de una superposición en este ámbito, se refleja en formación de grupos, de tal manera que en cada uno de los grupos conformados seleccionan un líder de grupo (CH) bajo métodos. Estos tienen un PK único, distinguido por otros CHs en la Superposición, la cual es aplicada para originar nuevos bloques para que otros CH den permiso de generar bloques y cada nodo es libre de cambiar su clúster en caso de retrasos exagerados.

Los CH se componen para su funcionamiento de un directorio de PK de solicitantes y de UN PK con autorización de acceso a los datos de los SHM conectados a un clúster.

- **PK de solicitantes:** Considerada la lista de PK que tienen permiso para acceder a datos, para los SHMs conectados a este clúster. Un ejemplo de lo que podría ser un SP que proporciona ciertos servicios para los dispositivos domésticos inteligentes.
- **PK de requisitos:** La lista de PK de SHM conectados a este clúster, que están permitidos para dar acceso.

Los CH superpuestos dentro del papel de blockchain público, que clasifica un contenido mayor sobre cada uno de los nodos que se hospedan en la red superposición, donde además posee el historial de transacciones realizadas por el usuario, en condiciones de solicitud y compartimiento de datos mediante la multisig, lo que indica es que cada transferencia es obligada a ser firmada por dos entidades donde se validan cada una de las transacciones del solicitante. Para validación del usuario y en búsqueda de infiltrados mediante el historial de transacciones indica si el usuario puede o no tener acceso a realizar la transacción con base en el certificado específico con comparación del hash del PK de entrada con el de salida, después los CH verifican los bloques generados de acuerdo a una secuencia y validación de bloque por los demás CH.

Al momento de la generación de un nuevo bloque también se produce una transacción multisig empleada para la generación de confianza, luego es divulgada la misma transacción multisig, junto con los bloques a los demás CH vecinos, los cuales verifican las transacciones. [41]

Hablemos ahora acerca de las transacciones de monitoreo las cuales son hechas en la red de superposición por los nodos hospedados allí recolectando datos en tiempo real, tales datos del dispositivo y supervisión al procesamiento de transacciones.

## V. Bases legales de la investigación

La aplicación de las bases legales en IoT no es muy amplia en Colombia a pesar de que actualmente está siendo muy utilizada este tipo de tecnología en el área de la salud, ambientes inteligentes, sensores, transporte, consumo personal, redes sociales, industrias manufactureras por lo tanto la legislación establece deberes y obligaciones para asegurar el crecimiento continuo por medio de la calidad de los servicios y generando confianza en el consumidor.

Se podrá encontrar las políticas que debe tener en el área de las telecomunicaciones para que se pueda gestionar y licenciar en el espectro, asegurando la disponibilidad de una amplia gama de aplicaciones de IoT en bandas con o sin

Licencia. En el área de la privacidad se establece la obligación de la protección de los datos personales del consumidor brindando seguridad, transparencia, dando claridad y certeza del funcionamiento de los servicios de IoT contando con una infraestructura robusta, de alta disponibilidad y confiablidad.

De acuerdo al análisis de vulnerabilidades de seguridad de la información del IoT en busca de proteger la privacidad, se tendrá en cuenta las bases legales que esta necesita para cumplirse, respetar los derechos al usuario, compromisos del proveedor y protección de datos.

## ITU (UNIÓN INTERNACIONAL DE TELECOMUNICACIONES)[2]

Unión Internacional de Telecomunicaciones – ITU es encargado de regular las telecomunicaciones se enfoca en 3 sectores como: radiocomunicaciones, normalización y desarrollo, son importantes para el funcionamiento de las redes, acceso a internet, protocolos etc. realizan conferencias y se encargan de dar las recomendaciones en distintas empresas. Impacto de la privatización y regulación de las telecomunicaciones en estructuración de la industria

La ITU (Unión Internacional De Telecomunicaciones), bajo la CCITT (Comité Consultivo Internacional De Telégrafos Y Teléfonos) en recomendación renombrada x.800 (arquitecturas de seguridad y aplicaciones en sistemas abiertos de interconexión).

Algunas definiciones nombradas a continuación son de gran notoriedad al relatar de seguridad orientada a la privacidad y seguridad en las de redes de datos:

1. Control de acceso: Difiere de una selección al medio o servicio de manera seleccionada por finalidad, previniendo el ingreso no autorizado.
2. Listas de control de acceso: numeración o listado de personal, entidades que poseen acceso autorizado a un recurso.
3. Responsabilidad: Garantizar el rastreo de acciones de una entidad, disponibles para la misma.
4. Amenaza activa: Amenaza que genera un cambio preconcebido en el sistema.
5. Autenticación: autenticidad de entidad par, origen de datos.
6. Integridad de los datos: promueve que los datos no se han alterados o destruidos mediante una amenaza.
7. Política: Imponencia de reglas o parámetro que se deben tener en cuenta al momento del uso de recursos y hacia quien va dirigido en búsquedas de generar seguridad frente a las amenazas.

Dentro del documento, la integridad de los datos es la propiedad de que estos mismos no sean alterados o arruinados de una manera no autorizada.

La firma digital, considerada aquella que podemos revisar para validar origen y privacidad de los datos.

[2] Norma ITU Unión Internacional de Telecomunicaciones 1865 estas recomendaciones son fundamentales para las redes TIC.

Algunas de las aplicaciones de integridad de los datos mediante el uso de servicios de autenticación que promueven la reducción de amenazas tal como se indica en el siguiente proceso:

En cierta conexión se genera el uso de un servicio de autenticidad de la entidad par, el preámbulo de la conexión en modo servicio es aplicado como índole de la integridad nos permitirá obtener un historial de detección, duplicidad en los datos mediante usos de secuencias numéricas en el transcurso de vida de una conexión.

La integridad de los datos con recuperación indica que el servicio se subdivide para la integridad de todos los datos del usuario (x) en una conexión (x), detectando modificaciones, inserciones, eliminación de datos dentro de una secuencia del SDU (Servicio De Unidad De Datos), con el intento de una restauración. [42]

### LEY 1273 de 2009[3]

A través de esta ley se enfoca a la protección de la información y de los datos, cada artículo especifica desde el acceso abusivo a un sistema informático, interceptación de datos informáticos, daños o uso de software malicioso etc. como tal esta ley se encarga de asegurar la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y aplica en el análisis de vulnerabilidades del sistema. [43]

### LEY 1341 DEL 30 DE JULIO DE 2009[4]

Esta ley define los principios y conceptos sobre la sociedad de la información u organización de las tecnologías de la información y las comunicaciones, se encarga de ordenar, controlar que los recursos sean eficientes, dirigidos por el sector de las tecnologías, como tal busca dar uso eficiente de la infraestructura dar prioridades al uso de las tecnologías de la información y proteger los derechos del usuario. [44]

### CONPES 3701[5]

Lineamientos de política para ciberseguridad y ciberdefensa para las amenazas informáticas desarrollando la prevención y control en la seguridad de la información como tal es un compromiso del gobierno nacional, por la evolución que está presentando las nuevas tecnologías, este lineamiento incluye las anteriores leyes expuestas para ejercer la estrategia de ciberseguridad. [45]

[3]Ley 1273 de 2009 De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos 5 de enero de 2009 p-1.

[4] Ley 1341 de 2009 marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones 30 de julio 2009 p-34.

### LEY 1581 DE 2012 PROTECCIÓN DE DATOS PERSONALES.[6]

Esta ley aplica la seguridad, confidencialidad y transparencia de la privacidad del usuario, regula el derecho al Habeas Data y derecho a la información, es definida por el alcance, principios, derechos de acceder a los datos personales y aplica para el respaldo de la información que guarde el usuario cuando implemente el manejo de los dispositivos IoT. [46]

### Norma ISO 27001.[7]

ISO 27001 gestión de la seguridad de la información considera que la información debe estar protegida, se enfoca a preservar la integridad, confidencialidad y disponibilidad de la información, define el alcance, analiza los riesgos y los gestiona, se implementa control de riesgos medidas preventivas y correctivas para identificar las vulnerabilidades, amenazas y por ultimo tratar el riesgo.[47]

### Norma ISO 27002.[8]

Dominio de política de seguridad es un estándar que complementa ISO 27001 se enfoca a todo tipo de empresas aplicando buenas prácticas para la gestión de la información y controles establecidos en la norma 27002, esta norma incluye la política de seguridad de la información, organización, seguridad física y del medio ambiente, control de acceso, adquisición de desarrollo y mantenimiento de sistemas, gestión de incidentes de seguridad de la información y gestión de continuidad para asegurar que las operaciones sean recuperadas para evitar la violación informática.

[5]Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación Bogotá D.C., 14 de julio de 2011p.1- 43.

[6] Norma ISO 27001 año 2013, sistema de gestión de la seguridad de la información para evaluar el riesgo y aplicar controles para tratarlos o eliminarlos.

[7] Norma ISO 27002:2013 mejora las prácticas en la seguridad de la información establece principios para mejorar la gestión de la seguridad de la información.

# CAPÍTULO III

# DISEÑO METODOLÓGICO

## VI. Tipo de investigación.

El tipo de investigación utilizada en este trabajo es documental, debido a que permite examinar las fuentes consultadas por medio de la recopilación de información, clasificando los datos, analizando las propiedades y características del tema estudiado, de este modo se desarrollara el enfoque general de IoT en redes y se determina los diferentes niveles de seguridad que se pueden aplicar, para determinar los beneficios de los procesos de IoT.

## VII. Métodos de investigación.

Los métodos aplicados en la investigación de este trabajo son:

- Exploratoria.
- Experimental.

## VIII. Técnicas e instrumentos de recolección de datos.

Se utilizó las siguientes técnicas e instrumentos de recolección de datos:

- Investigación en internet.
- Investigación Bibliográfica.
- Análisis documental.
- Observación experimental.

# CAPÍTULO III

# RESULTADOS DE LA INVESTIGACIÓN

## IX. Resultados del objetivo específico no. 1

Como todo tipo de sistemas siempre tiene backdoors u otras vulnerabilidades que pueden generar daño, en este caso la expuesta es la privacidad alterando la integridad de la información del usuario de tal modo que pueden ocurrir casos como:

- La información que el usuario comparte es extraviada o perdida por la falta de conocimiento del manejo de dispositivos IoT.
- La amenaza del ciberataque a los dispositivos conectados a internet, por lo tanto se retienen los datos o son mal utilizados.
- Mala implementación del cifrado, no deja que las acciones funcionen de forma correcta, o manejos de doble autenticación.
- denegación del servicio.
- Estructuras deficientes para la programación de contraseñas débiles.
- El intruso de tener acceso a la red puede manipular, análisis de tráfico para espionaje y subordinación por falta de controles de accesos y cifrado de autenticidad.
- Desactualización de firmware y software.

## X. Resultados del objetivo específico no. 2

Se estudia diferentes redes de comunicación más utilizadas en IoT y los principios que deben cumplir, existen diferentes tecnologías que cumplen con largo alcance de comunicación, disponibilidad, seguridad, baja frecuencia de transmisión, bajo consumo de energía, bajas velocidades de datos.

Algunas son: GSM/GPRS, SigFox, LoRa, Wifi,BLE, ZigBee, bluetooth.

## XI. Resultados del objetivo específico no. 3

De acuerdo a las fuentes consultadas podemos encontrar formas de prevención para garantizar seguridad en la información orientado a la privacidad, se ha evaluado que debe especificarse esta implementación en:

- Interfaces de acceso: es necesario la implementación de una interfaz web donde se pueda configurar los parámetros del dispositivo con credenciales de acceso por defecto con autentificación, dando complejidad posible para protección de información del usuario.
- Actualización de equipo: mantener equipo actualizado última versión de software y firmware, tener cuidado cuando se realice un soporte al dispositivo, ofrecer conexión segura.
- Configuración de red de datos segura: control de acceso a los puertos, habilitar los que sean necesarios para reducir el riesgo de seguridad en conjunto de manejos de IDS e IPS.
- Control de servicios Cloud: evitar que los datos terminen en internet por el acceso a servicios en la nube.
- Blockchain e internet de las cosas da posibilidad de almacenamiento de la información y detección de cambios y de problemas de seguridad donde los elementos de la red estén comprometidos, permitiendo automatizar criptográficamente el consumo en procesos.

# CAPÍTULO V.

# CONCLUSIONES Y RECOMENDACIONES

- En este trabajo se identificó medidas de riesgo y control para las redes que son compatibles con la tecnología de IoT, al momento de ser implementada la misma IOT en cualquier campo para eludir ataques generales como por fuerza bruta o denegación de servicio distribuido afectando la seguridad del usuario, se tenga un control o medidas de seguridad para manejo de accesos, control de flujo de tráfico, monitoreo de IOT mediante el uso de protocolos, actualización de software y firmware, seguridad en la infraestructura a través de ids,ips, o blockchain.
- Las empresas encargadas de ofrecer servicios de IoT muchas veces no generan una planeación de posibles vulnerabilidades en los dispositivos desde su creación, al igual que no generan enseñanza al usuario para garantizar la seguridad de la privacidad de la información, donde el usuario debe tener una conciencia clara para que y como lo va a utilizar y que datos privados circularan en el entablamiento de nodos, teniendo en cuenta siempre el control de sus datos, por ende por aspectos como estos no tenidos en cuenta el usuario puede dar acceso a terceros al ingreso o manejo de la información.
- Se garantiza la privacidad de manera descentralizada y con detalles de acceso, no repudio a través de la aplicación de blockchain para IOT debido a su robustez de administración, de tal modo que una de sus consecuencias frente a su uso es el aumento de energía por ser administraciones descentralizadas.
- Los protocolos y arquitectura que tiene IoT están en mejora continua, para controlar de manera adecuada los datos que circulan por la red, además la implementación de 5G se enfoca para la conexión de dispositivos inteligentes, desde cualquier lugar dando más capacidad y velocidad que 4G.

# BIBLIOGRAFÍA

**Referencias**


[1] Alcalá, U. D. (24 de Septiembre de 2018). *ORIGEN E HISTORIA DEL INTERNET OF THINGS*. Obtenido de https://www.master-internet-of-things.com/historia-iot/

[2] C, M. A. (5 de Octubre de 2017). La historia detrás de la internet de las cosas. *El Espectador*, 1. Obtenido de https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678

[3] paniagua, S. (15 de abril de 2012). *Un poco de historia sobre Internet de las Cosas*. Obtenido de http://www.sorayapaniagua.com/2012/04/15/un-poco-de-historia-sobre-internet-de-las-cosas/#comments

[4] SILVESTRE, J. S. (2016). *Internet De Las Cosas.* Obtenido de https://upcommons.upc.edu/bitstream/handle/2117/100921/LM08_R_ES.pdf

[5] Luis Alberto Pèrez, W. A. (2014). *Estado del Arte de las Arquitecturas de Internet de las Cosas (IoT)*.

[6] Alcaraz, M. (2014). *Internet De Las Cosas*. Obtenido de http://jeuazarru.com/wp-content/uploads/2014/10/Internet-of-Things.pdf

[7] Eduardo Sosa, D. G. (1 de Junio de 2014). *Internet del Futuro. Desafíos y Perspectivas* . Obtenido de https://www.researchgate.net/publication/317536830_Internet_del_futuro_Desafios_y_perspectivas

[8] Godoy, D. (s.f.). *Convergencia de tecnologías RFID y WSN.* . Obtenido de https://www.researchgate.net/figure/Figura-2-Convergencia-de-tecnologias-RFID-y-WSN_fig2_317536830

[9] Luis Carlos, L. G. (2014). Estudio del impacto técnico y económico de la transición de internet al internet de las cosas (IoT) para el caso colombiano. *Universidad Nacional de Colombia*, 45-49.

[10] Dujovne, D. (5 de Septiembre de 2014). *IoT, 6TiSCH y ROLL: Tres conceptos en construcción en la IETF*. Obtenido de https://docplayer.es/53867999-Iot-6tisch-y-roll-tres-conceptos-en-construccion-en-la-ietf.html

[11] González, D. R. (2013). Arquitectura y Gestión de la IoT. *Revista Telem@tica.*, p49-60.

[12] JOSÉ DANIEL, A. S. (2017). *Diseño, implementación e integración de un sistema de medición de variables de entorno en un sistema iot con software y hardware libre*. Obtenido de https://riunet.upv.es/bitstream/handle/10251/89420/48645867Q_TFG_1504721962405488303143047818600l.pdf?sequence=2

[13] inalámbricas, C. d. (s.f.). *Tecnologías inalámbricas*. Obtenido de http://techpedia.fel.cvut.cz/html/frame.php?oid=9&pid=1003&finf=

[14] Mendez, F. O. (27 de Septiembre de 2017). *Internet de las cosas*. Obtenido de http://www.unsij.edu.mx/radio/2017/%20270917.pdf

[15] Castillo, O. (15 de Noviembre de 2017). MANERAS EN QUE FUNCIONA EL IOT, ¿CÓMO SE DA LA COMUNICACIÓN? Obtenido de https://telcelempresas.com/maneras-en-que-funciona-el-iot-como-se-da-la-comunicacion/

[16] Mutabazi, P. (6 de Marzo de 2019). *The Mobile Wireless Communication Technology Journey - 0G, 1G, 2G, 3G, 4G, 5G*. Obtenido de https://www.linkedin.com/pulse/mobile-wireless-communication-technology-journey-0g-mutabazi

[17] Tecnologia, C. y. (21 de marzo de 2018). *Evolución de la red de comunicación móvil, del 1G al 5G*. Obtenido de https://www.universidadviu.com/evolucion-la-red-comunicacion-movil-del-1g-al-5g/

[18] IoT, E. t. (s.f.). TECNOLOGÍAS DE COMUNICACION PARA IOT. Obtenido de https://www.efor.es/sites/default/files/tecnologias-de-comunicacioon-para-iot.pdf

[19] Triquet, J. (2016). GPRS, SigFox, LoRa, NB-IoT ¿Qué tecnología adoptar? Obtenido de http://director-it.com/index.php/es/ssoluciones/comunicacion-entre-maquinas/221-conexion-adopcion.html

[20] Wedd, M. (17 de Octubre de 2018). *Aplicaciones de Bluetooth IoT: de BLE a malla*. Obtenido de https://www.iotforall.com/bluetooth-iot-applications/

[21] Brayan Sánchez Torres, J. A. (24 de Diciembre de 2017). *Campus inteligente: Tendencias en ciberseguridad y desarrollo futuro*. Obtenido de http://www.scielo.org.co/pdf/rfing/v27n47/0121-1129-rfing-27-47-104.pdf

[22] Alexander, C. M. (2016). *Análisis de la gestión de seguridad y fallos en internet de las cosas, usando el estándar 6lowpan*. Ecuador: Universidad de las Américas.

[23] Issue, I. E. (8 de Mayo de 2015). *Connected Boulevard aprovecha la solución de IoT*. Obtenido de https://iebmedia.com/wireless.php?id=10940&parentid=74&themeid=275&hft=88&showdetail=true&bb=1

[24] Xavier caron, S. B. (Diciembre de 2015 ). *El Internet de las cosas (IoT) y su impacto en la privacidad individual: una perspectiva australiana*. Obtenido de https://www.researchgate.net/publication/288918372_The_Internet_of_Things_IoT_and_its_impact_on_individual_privacy_An_Australian_perspective

[25] Abbas M. Hassan, A. I. (3 de Mayo de 2018). *Urban Transition in the Era of the Internet*. Obtenido de https://ieeexplore.ieee.org/document/8360930/references#references

[26] Malhotra, N. K., Kim, S. S., & Agarwal, J. (4 de Diciembre de 2014). *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale And a Causal Model*. Obtenido de https://pdfs.semanticscholar.org/7307/1a056403ed5f9fd5b16b9dd70a93e9a4e375.pdf

[27] Weber, R. H. (2015). *Internet of things: Privacy issues revisited*. Obtenido de https://www.dhi.ac.uk/san/waysofbeing/data/governance-crone-weber-2015c.pdf

[28] Kim Thuat Nguyenuna, M. L. (Septiembre de 2015). *Survey on secure communication protocols for the Internet of Things*. Obtenido de https://kundoc.com/pdf-survey-on-secure-communication-protocols-for-the-internet-of-things-.html

[29] Jan Henrik Ziegeldorf, O. G. (10 de Junio de 2014). *Privacy in the Internet of Things*. Obtenido de https://onlinelibrary.wiley.com/doi/full/10.1002/sec.795

[30] Arturo González García, Y. G. (22 de Agosto de 2016). *Impacto medioambiental de la integración de la computación en la nube y la internet de las cosas*. Obtenido de http://repository.lasallista.edu.co:8080/ojs/index.php/pl/article/view/1236/1027

[31] Comunicaciones Digitales y Redes (Volumen 4, Número 3 , agosto de 2018 , páginas 149-160)

[32] Pérez, P. A. (Junio de 2018). Seguridad En Internet De Las Cosas Honeypot to capture IoT-attack methods. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/82136/6/parriagaTFM0618memoria.pdf

[33] Romero, A. (Junio de 2009). Seguridad en Redes. Obtenido de https://www.academia.edu/11190534/Protocolos_Seguros_de_Internet_Parte_I_Seguridad_en_Redes

[34] García, M. I. (2008). *Utilización de Sistemas de Detección de Intrusos como elemento de Seguridad Perimetral* . Obtenido de http://www.adminso.es/images/1/1d/PFC_marisa.pdf

[35] MA Noureddine, A. M. (2017). *Redes de actividades estocásticas: definiciones formales y conceptos*.

[36] Subil Abraham, S. N. (12 de Diciembre de 2014). *Análisis de seguridad cibernética: un modelo estocástico para la cuantificación de la seguridad utilizando cadenas de Markov absorbentes.* Obtenido de http://www.jocm.us/uploadfile/2014/1231/20141231022619157.pdf

[37] Michael Crosby, N. P. (2 de Junio de 2016). *BlockChain Technology: Beyond Bitcoin.* Obtenido de https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

[38] Caballero Gimeno, J. Á. (Junio de 2018). *Estudio de tecnologías Bitcoin y Blockchain.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81268/6/javicgTFM0618memoria.pdf

[39] Choo, M. B.-K. (Agosto de 2018). *Un futuro blockchain para la seguridad de internet de las cosas: un documento de posición.* Obtenido de https://www.sciencedirect.com/science/article/pii/S2352864817302900

[40] CSIRO. (20 de Abril de 2017). *Blockchain para seguridad y privacidad de IoT*. Obtenido de https://research.csiro.au/dss/blockchain-iot-security-privacy/

[41] Ali Dorri, S. S. (21 de Abril de 2017). *Hacia un BlockChain optimizado para IoT*. Obtenido de https://dl.acm.org/citation.cfm?id=3055003

[42] TELEFÓNICO, C. C. (1991). *REDES DE COMUNICACIÓN DE DATOS: INTERCONEXIÓN DE SISTEMAS ABIERTOS (ISA); SEGURIDAD, ESTRUCTURA Y APLICACIONES*. Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.800-199103-I!!PDF-S&type=items

[43] REPÚBLICA, C. D. (2009). *Ley 1273 de 2009* . Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[44] *LEY 1341*. (30 de Julio de 2009). Obtenido de https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

[45] *LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA*. (14 de Julio de 2011). Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[46] *LEY ESTATUTARIA 1581 DE 2012*. (18 de Octubre de 2012). Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[47] 27001-27002. (s.f.). *Sistemas de Gestión de Riesgos y Seguridad*. Obtenido de https://www.normas-iso.com/iso-27001/