
**FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS**

# ANÁLISIS DE LA GESTIÓN DE SEGURIDAD Y FALLOS EN INTERNET DE LAS COSAS, USANDO EL ESTÁNDAR 6LOWPAN.

**Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de:**
**TECNÓLOGO EN REDES Y TELECOMUNICACIONES.**

**PROFESOR GUÍA:**

**ING. JOSÉ LUIS RODRÍGUEZ AÑAZCO**

**AUTOR:**

**HENRY ALEXANDER CASTILLO MERCHÁN**

**AÑO:**

**2016**

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

José Luis Rodríguez Añazco
Ing. Telecomunicaciones C.C.
171690945-0

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Sr. Henry Alexander Castillo Merchán
C.C.170710799-9

## DEDICATORIA

De manera muy especial, dedico esta humilde obra de trabajo de grado, primeramente a Dios, ya que me ha dado la fuerza y la fe para lograr con esfuerzo y perseverancia, ser un profesional.

También el apoyo incondicional de mi mamá, hermanos y especialmente de mi esposa e hijo, que han estado a mi lado dándome el impulso para lograr este y otros objetivos propuestos.

De todo corazón, agradezco a los docentes de la Universidad de las Américas, por compartir su profesionalismo, inculcándome día a día sus experiencias motivadoras, que me han inspirado para lograr impulsarme y ahondar en un futuro prometedor.

Por supuesto, agradezco de todo corazón, a mi tutor guía, que pacientemente con su profesionalismo ético y disponibilidad, me orientó en la realización de la tesis.

**HENRY CASTILLO MERCHÁN**

# RESUMEN

En el presente trabajo de titulación se propusieron las pautas a seguir para la implementación de un adecuado sistema de gestión de seguridad y fallos en aplicaciones relacionadas con el Internet de las Cosas basados en el estándar 6LoWPAN. El trabajo consta de Resumen en español e inglés, Introducción, Desarrollo, Conclusiones y Bibliografía. El desarrollo del trabajo consta de tres capítulos, en el Capítulo I se definieron los principales conceptos relacionados con el Internet de las Cosas, surgimiento y evolución de estas nuevas funcionalidades de la red, las principales aplicaciones que se están implementando, el nivel de penetración que tienen estas tecnologías en la sociedad actual, así como cuál será la tendencia para los próximos años. Se presentan las características del estándar 6LoWPAN y se hizo una comparación entre los estándares desarrollados para aplicaciones inalámbricas de redes de área personal de baja potencia. En el Capítulo II se presentaron los principales fallos que suelen ocurrir en sistemas informáticos y se valoró el impacto que pueden tener sobre aplicaciones relacionadas al Internet de las Cosas. Se determinaron las principales vulnerabilidades que conlleva la interconexión con la red así como las formas de atenuarlas. El Capítulo III es el más importante de la investigación, en él se expusieron los criterios que deben seguirse a la hora de implementar sistemas de gestión de seguridad y fallos en aplicaciones del Internet de las Cosas para que los mismos sean efectivos y se explicaron las consecuencias de la no existencia de estos sistemas de seguridad y fallos.

**Palabras claves o descriptores:** IoT**,** Internet de las cosas, seguridad de comunicación, vulnerabilidad, protocolos de seguridad, 6LoWPAN.

# ABSTRACT

In the present work, the guidelines were proposed for the implementation of an adequate system of management of security and failures in applications related to the Internet of the Things based on the standard 6LoWPAN. The work is composed of Abstract in Spanish and English, Introduction, Development, Conclusions and Bibliography. The development of the work is formed by three chapters. In Chapter I, the main concepts related to the Internet of Things were defined, the emergence and evolution of these new functionalities of the network, the main applications being implemented, the level of penetration of these technologies in today's society, and as will be the trend for the next years. The features of the 6LoWPAN standard are presented and a comparison was made between the standards developed for wireless applications of low power personal area networks. Chapter II presented the main faults that usually occur in computer systems and assessed the impact they may have on applications related to the Internet of Things. The main vulnerabilities associated with the interconnection with the network were identified as well as ways of mitigating them. Chapter III is the most important of the research, in which he explained the criteria that should be followed when implementing security management systems and faults in Internet applications of the Things so that they are effective and explained the consequences of the non-existence of these security systems and failures.

**Keywords or descriptors:** IoT**,** Internet of things, communication security, vulnerabilities, security protocols, 6LoWPAN.

**ÍNDICE DE CONTENIDOS**

# ÍNDICE DE FIGURAS

# GLOSARIO DE TÉRMINOS

**Dirección IP** Dirección numérica que corresponde a tu equipo dentro de una red.

**Ethernet** Red de área local con topología de bus, que sigue la norma IEEE 802.3. Su velocidad de transmisión es de 10Mbps

**FTP** File Transfer Protocol. Protocolo de Transferencia de Archivos

**IDE** Integrated Development Environment IEEE Institute of Electrical and Electronics Engineers

**IETF** Internet Engineering Task Force JTAG Joint Test Action Group. Estándar IEEE para el acceso de puertos en circuitos integrados kbps Kilo Bits per Second

**LAN** Red de área local (Local Area Network)

**MAC** Control de Acceso al Medio (Medium Access Control)

**MTU** Unidad Máxima de Transmisión (Maximun Transmission Unit)

**PAN** Red de Área Personal (Personal Area Network)

**WAN** Red de área amplia, es una red que cubre un área más extensa.

**WPAN** Redes inalámbricas de área personal (wireless personal area network)

**SMTP** Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol)

**TCP** Protocolo de Control de Transmisión (Transmision Control Protocol)

**UDP** Protocolo de Datagrama de Usuario (User Datagram Protocol)

**6LowPan** (IPv6 over Low power Wireless Personal Area Networks) es un estándar que posibilita el uso de IPv6 sobre redes basadas en el estándar IEEE 802.15.4

**ZIGBEE** Conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal

# INTRODUCCIÓN

Internet es un conjunto de redes conectadas que utilizan la familia de protocolos TCP (Transmission Control Protocol) y el IP (Internet Protocol) “Protocolo de control de transmisión/Protocolo de Internet” TCP/IP, lo cual garantiza que funcionen como una red lógica única de alcance mundial. La versatilidad de Internet ha superado cualquier previsión y constituye una verdadera revolución en la sociedad.

Un próximo paso en el desarrollo de este fenómeno es la conectividad entre todos los objetos que nos rodean. Esta nueva vertiente la llamó CISCO: Internet de las Cosas (IoT, por sus siglas en inglés: Internet of Things). Es un conjunto de diferentes sensores y equipos de todo tipo que pueden tener un mejor entendimiento con su entorno y una mayor autonomía en su funcionamiento.

Ejemplo de lo anterior es IBM Watson, un proyecto a gran escala en el que trabaja IBM. Watson es un mega servidor que se alimenta de fuentes tales como bibliotecas, hospitales e incluso Internet. Esta herramienta permite responder de manera lógica a cualquier pregunta por más complicada que sea e incluso proyectar información analítica provista por una empresa.

Si los objetos tuvieran incorporadas etiquetas de radio podrían comunicarse con otros equipos de la misma manera que si fueran controlados por el hombre. Las etiquetas de radio operan con bajos niveles de potencia, por lo que su alcance es muy limitado y forman parte de las PAN (Personal Area Networks) “Redes de área personal”. (Shelby & Bormann, 2009, pág. 3)

En el mundo de IoT cada objeto tiene una identidad propia y potencialidad para interactuar con otros entes y debe ser diferenciado a través de un código único. El protocolo estandarizado para la interconexión de dispositivos en red es el IP, el cual en su versión 6 puede proveer un número para cada objeto del mundo. IP es un protocolo de la capa de red del modelo OSI (Open System Interconnection) “Interconexiones de Sistemas Abiertos”. Para las capas física y de enlace en aplicaciones de baja potencia el IEEE, (Institute of Electrical and Electronics

Engineers) dictó el estándar 802.15.4. Estándares como ZigBee y 6LoWPAN se crean para hacer más eficiente la comunicación entre las capas de enlace y red.

Se considera utilizar este último por ser considerado más apropiado para sistemas IP, pues posibilita comunicar sistemas que se basan en 802.15.4 y sistemas que no. Para la integración de objetos a IoT, la cualidad de comunicarse con sistemas IP es crucial para escoger un estándar (Culler, 2008, pág. 65).

El crecimiento de IoT es sumamente acelerado y se ha convertido en una tendencia actual pues se abren muchas posibilidades en la concepción de aplicaciones y servicios; sin embargo su privacidad, seguridad y confiabilidad son puntos críticos que siguen sin estar del todo resueltos, de ahí que sea necesaria la generación de soluciones que ayuden a resolver esta dificultad.

Los análisis que se han realizado sobre el tema abordan el asunto desde una posición parcial o incompleta, con criterios no conclusivos sobre las posibles implicaciones sociales, tecnológicas e incluso morales y legales que pueden tener los fallos y la inseguridad en IoT. Este es un campo aún en pleno florecimiento donde hay mucho que decir y opinar al respecto.

Considerando todo lo anterior, se plantea como Problema de investigación el siguiente:

*¿Es posible implementar un sistema efectivo de gestión de seguridad y fallos vinculado al Internet de las Cosas, basados en el estándar 6LoWPAN?*

Para dar respuesta al problema se definen los objetivos de investigación:

**Objetivo General:**

Proponer las pautas a seguir para la implementación de un adecuado sistema de gestión de seguridad y fallos en aplicaciones relacionadas con el Internet de las Cosas basados en el estándar 6LoWPAN.

**Objetivos específicos:**

- Definir los conceptos de Internet de las Cosas y gestión de seguridad y fallos.
- Detallar las particularidades del estándar 6LoWPAN.
- Comparar el estándar 6LoWPAN con estándares similares.
- Analizar las principales vulnerabilidades de la seguridad del Internet de las Cosas.
- Valorar el impacto de los fallos asociados al Internet de las Cosas.
- Explicar las posibles consecuencias de la no existencia de sistemas efectivos de gestión de seguridad y fallos en el Internet de las Cosas.
- Elaborar una propuesta de lineamientos a seguir para la implementación de un sistema efectivo de gestión de seguridad y fallos para aplicaciones de Internet de las Cosas basados en el estándar 6LoWPAN.

En la investigación se aplicaron varios métodos: el método descriptivo utilizado para referir lo que se ha escrito sobre el tema y contrastar los diferentes puntos de vista y el método inductivo–deductivo que sirvió para poder alcanzar los objetivos propuestos y así seguir una línea de investigación coherente, además de realizar generalizaciones de las situaciones que se estudiaron y arribar a conclusiones en concordancia con los objetivos propuestos.

# CAPÍTULO I

# MARCO TEÓRICO

## 1.1. INTERNET

A Internet se le conoce como la “Red de redes” y definida de una forma muy sencilla, es un conjunto descentralizado de redes de comunicación interconectadas entre sí. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California (Estados Unidos) (Ávila 2012, p.2).

En la presente investigación se toma el concepto que define Internet como un “sistema de información mundial que permite que redes, ordenadores y dispositivos de diferentes tipos se intercomuniquen. Su esencia estriba en los protocolos y los procedimientos que permiten que eso ocurra” (UIT, 2010, pág. 17).

El funcionamiento de internet se basa en tres aspectos fundamentales: protocolos de comunicación, dirección IP y servidores. La familia de protocolos de Internet es un conjunto consensuado de normas que especifican como debe ser la comunicación entre equipos conectados a la red, lo cual garantiza que las redes físicas que la componen formen una red lógica única de alcance mundial. La dirección IP asigna un número o dirección única a cada equipo en la red. Los servidores son los ordenadores que ofrecen servicios y se encargan de organizar la comunicación (Ávila 2012, pp.3-5).

El uso del Internet tiene muchas implicaciones en lo social, por el uso diario de esta tecnología. Cada día más personas usan este medio por todos los servicios que ofrece, entre ellos destacan:

- Páginas web
- Envío de correo electrónico
- Transmisión de archivos
- Conversaciones en línea
- Videoconferencias
- Mensajería instantánea
- Telefonía
- Boletines electrónicos
- Acceso remoto a otros dispositivos
- Juegos en línea
- Redes sociales

Durante los últimos años los avances han sido extraordinarios. Lo que ha posibilitado la existencia de una interacción constante, no sólo con las personas cercanas, sino también con aquellas que se encuentren muy distantes; pero además obteniendo información adecuada y oportuna que ha permitido crecer en distintos ámbitos de la sociedad.

Todos estos avances han creado nuevos cambios en la vida cotidiana de las personas, en la forma de relacionarse, de efectuar sus labores diarias, de entregar productos y servicios, entre otras. La base de esta transformación ha sido posible gracias a Internet, estando hoy en día como la principal plataforma de comunicación disponible.

Entre las características que más sobresalen de Internet se pueden citar las siguientes:

- Universal por su alcance global
- Libre porque cualquier persona puede colocar información y acceder a ella.
- Fácil de usar porque no es necesario tener conocimientos avanzados de informática para su uso.

- Útil y variada pues dispone información y servicios de todo tipo muy accesibles.

A pesar de las bondades que ofrece Internet hay que tomar en consideración que la accesibilidad y su carácter libre hacen que sea poco fiable el contenido que puede encontrar y debido a su carácter universal la información viaja de un lugar a otro siendo fácil interceptarla. Por lo tanto la seguridad en Internet es un tema de gran consideración en la actualidad.

## 1.2 GESTIÓN DE LA SEGURIDAD EN INTERNET

Como se expuso en el acápite anterior, entre las principales razones del éxito y rápido posicionamiento de Internet está el hecho de ser una red abierta y accesible a todo público. Cualquier red puede conectarse, no hay ningún propietario de internet y esto es realmente riesgoso ya que existen cientos de millones de usuarios. Esta extraordinaria facilidad de acceso es el principal atractivo para todo tipo de indeseables.

¿Cómo se está protegiendo a los usuarios?, ¿qué consejos o tareas los internautas deben observar al momento de ingresar al Internet?, son interrogantes que no tienen una respuesta única. En definitiva, son muchas las recomendaciones adecuadas para el uso correcto de la red. Debido a que cada día se incrementa el número de usuarios, también aumentan los peligros y el robo de información; por ello es necesario disponer de mecanismos apropiados que protejan todos los datos disponibles en el Internet y que no sean empleados para perjudicar a los internautas.

### 1.2.1 Modelo del Sistema de Gestión de la Seguridad de la Información (SGSI) ISO 27001

Según la ISO 2700, la seguridad de la información contiene varios elementos que deben ser considerados con el propósito de brindar una verdadera seguridad en los datos:

- Confidencialidad: busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.
- Integridad: busca asegurar que no se realicen modificaciones por personas no autorizadas a los datos o procesos, que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos y que los datos sean consistentes tanto interna como externamente.
- Disponibilidad: busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

Existiendo por ello varias condiciones que son aceptadas en las empresas y definiendo los controles necesarios en el empleo del Internet como plataforma en sus operaciones, uno de los modelos más actuales en la gestión de la seguridad es el que indica la ISO 27001, siendo el siguiente:


- ***Plan (planificar):*** establecer el SGSI.
- ***Do (hacer):*** implementar y utilizar el SGSI.
- ***Check (verificar):*** monitorizar y revisar el SGSI.
- ***Act (actuar):*** mantener y mejorar el SGSI.

**Figura 1.** Modelo SGSI de la Norma ISO 27001

**Tomado de:** (ISO 27001, 2005)

Observando en la figura, para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

## 1.3. INTERNET DE LAS COSAS

Hoy en día disponemos de varios equipos que se conectan a internet, entre ellos Smartphones, dispositivos multimedia, etc. Internet evoluciona constantemente y actualmente el Internet de las cosas (IoT por sus siglas en inglés “Internet of Things”) se refiere a la conexión de objetos cotidianos con internet.

El concepto de internet de las cosas lo propuso Kevin Ashton en el Auto-ID Center del MIT en 1999, donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores (Evans, 2011).

Por ejemplo, si los objetos comunes como libros, termostatos, refrigeradores, lámparas, botiquines, partes automotrices, etc. estuvieran conectados a Internet y equipados con dispositivos de identificación, no existirían, en teoría, artículos fuera de stock o medicinas caducadas; se sabría ubicación exacta, su consumo; el extravío sería cosa del pasado y se sabría qué está encendido o apagado en cualquier momento.

La evolución del Internet al parecer no tiene límites, ya que de forma constante cada año aparecen nuevas tecnologías que cambia completamente el perfil de cómo se están ejecutando las tareas diarias. Intentando hacerlas en el menor tiempo posible y con un mínimo de esfuerzo, provocando al mismo tiempo un mayor uso del Internet, con el objetivo de disponer más tiempo para otras labores.

Llegando de esta forma a considerar una conexión total, es decir, no sólo entre las personas, sino que se puedan conectarse con sus cosas y estos puedan brindar información oportuna para satisfacer las necesidades de los usuarios.

## 1.4. PROTOCOLO DE SEGURIDAD

Para llevar a cabo una conexión, es necesario que se establezcan varios aspectos esenciales, teniendo en cuenta no solo los componentes físicos, sino también el software que se utilizará. Además, se debe identificar el propósito por el cual se construirá o efectuará la conexión o conexiones, sin dudarlo, lo que se busca es determinar de forma clara el tipo de red.

A más de lo señalado en la construcción de una red se debe considerar cuáles serán sus protocolos de seguridad, denominados como la base para la existencia de una conexión. Dependiendo del tipo de red, esta se podrá conectar con múltiples dispositivos dentro del entorno y fuera del él, lo más relevante, serán sus protocolos de seguridad que empleen al momento de la transmisión de información y el tipo de datos.

### 1.4.1. Papel de los Protocolos de Internet

Los protocolos son elementos base para llevar a cabo una conexión, teniendo su función principal el enlace entre servidores, computadores o cualquier otro dispositivo, en el Internet que es la red de redes, se consideran los más importantes para poder acceder a la información de un lugar a otro.

### 1.4.2. Tipos de protocolos

Con el objetivo de identificar cuáles son los tipos de protocolos mayormente empleados en el Internet, y el propósito de salvaguardar toda la información que circula por esta red, se escogió la clasificación de Cabello, opinando que se disponen de dos principales, siendo estas:

**Los orientados a la conexión**: controlan la transmisión de datos. Para esto, se van acusando recibos durante la comunicación de los datos que se van recibiendo. Un ejemplo de estos protocolos es el TCP.

**Los no orientados a la conexión**: no controlan la transmisión de datos durante la comunicación; un emisor envía datos a un receptor, y éste los recibe sin

confirmar los mismos. Un ejemplo de estos protocolos es el UDP. (Cabello, 2015)

A partir de estos protocolos presentados, se mencionan que los mayormente utilizados en el Internet, son los orientados a las conexiones, y en sus inicios existieron dos alternativas para llevar a cabo esta unión. El conjunto de protocolos que usa Internet es el TCP/IP, en referencia a los dos protocolos más importantes que la componen, fueron de los primeros en definirse en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en ARPANET y son los dos más utilizados de la familia:

- TCP Protocolo de Control de Transmisión.
- IP Protocolo de Internet.

Existen tantos protocolos en este conjunto que llegan a ser más de cien diferentes, entre ellos se encuentran: ARP (Address Resolution Protocol), Protocolo de Resolución de Direcciones, para la resolución de direcciones, FTP (File Transfer Protocol), Protocolo de Transferencia de Archivos, para transferencia de archivos o ficheros, HTTP (HyperText Transfer Protocol), Protocolo de Transferencia de HiperTexto, que es popular porque se utiliza para acceder a las páginas web, POP (Post Office Protocol), Protocolo de Oficina Postal, para correo electrónico, SMTP (Simple Mail Transfer Protocol), Protocolo de Transferencia Simple de Correo, para correo electrónico, Telnet (Teletype Network), para acceder a equipos remotos (Sánchez, 2014, P.6).

En la siguiente figura se ilustra los aspectos relevantes del protocolo TCP/IP:


**Figura 2:** Protocolo TCP/IP

**Tomado de:** (Cabello, 2015)

Observando en la figura 2, las características principales del protocolo TCP/IP como estándar para las conexiones en Internet.

### 1.4.3. Modelo TCP/IP

Siendo el estándar para las conexiones, el modelo TCP/IP es un modelo de descripción de protocolos de red. El protocolo TCP/IP es una familia de protocolos que sirven para crear conexiones en la red a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TCP da soporte a muchas de las aplicaciones más populares de Internet (navegadores, intercambio de ficheros, clientes FTP, etc.) y protocolos de aplicación HTTP, SMTP, SSH y FTP.

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar

una dirección IP a cada equipo de la red para poder enrutar paquetes de datos, como son transmitidos y como serán recibidos.

El modelo estándar para diseñar una arquitectura de red es el modelo OSI (Open Systems Interconnection), prototipo que consiste de siete capas: Capa física, Enlace de datos, Red, Transporte, Sesión, Presentación y Aplicación. El modelo TCP/IP es un prototipo híbrido derivado del OSI. El TCP/IP combina las tres capas superiores (Aplicación, Presentación y Sesión) del OSI en una capa (Aplicación), así mismo mantiene la capa cuatro (Transporte), combina las capas tres y dos (Red y Enlace de Datos) en una sola a la que llama Internet y mantiene la capa Física.

En la siguiente figura se podrá observar el proceso de comunicación según el modelo TCP/IP:

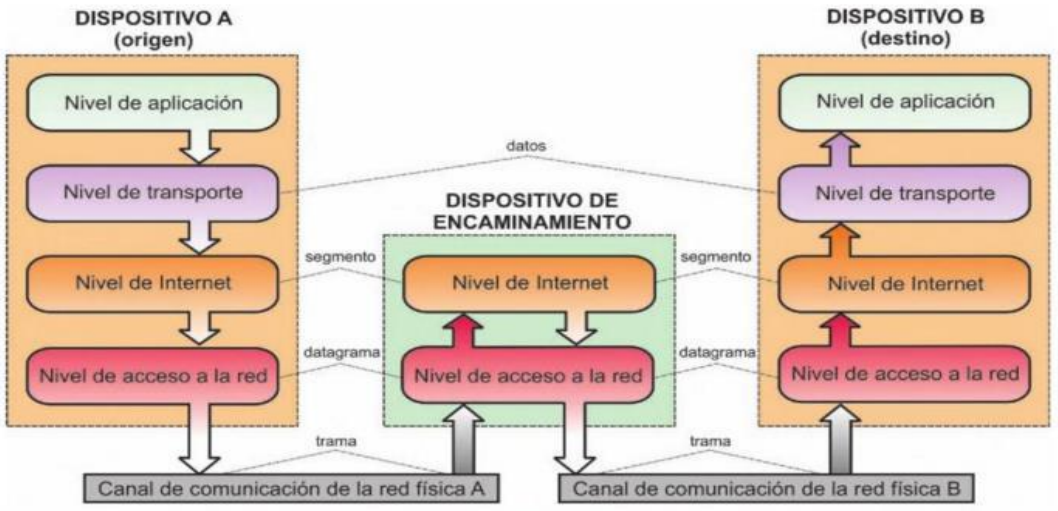


**Figura 3.** Proceso de comunicación modelo TCP/IP.

**Tomado de:** (Miranda, 2005)

La figura 3 muestra cómo se produce la comunicación en el modelo TCP/IP, identificándose cuatro niveles, tanto en el origen, como en el destino. También se encuentra el canal de comunicación de las redes físicas y en ellos los niveles de acceso a la red y de Internet.

### 1.4.4. Otros Protocolos en Internet

Como se ha mencionado, la base para la conexión hacia Internet, es el modelo TCP/IP, una familia de protocolos integrada por más de cien, estos hacen posible acceder a los diferentes formatos de la información en la red y servicios de correo, de compras y otros, a continuación se mencionan los principales:

- ARP (Address Resolution Protocol)
- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- POP (Post Office Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SSL (Secure Sockets Layer)
- Telnet (Teletype Network)

## 1.5. EL ESTÁNDAR IPV4

El IP tiene dos funciones principales: entrega de datagramas a través de la red y fragmentación y re ensamblado de datagramas. Este proceso se logra identificando cada paquete enviado con una dirección numérica llamada dirección IP. El esquema de direccionamiento IP es integral al proceso de enrutamiento de datagramas IP a través de la red. Cada dirección IP tiene componentes específicos y un formato básico definido.

Existen dos estándares de direccionamiento IP: la versión 4 (IPv4) y la versión 6 (IPv6). Él más difundido en la actualidad es el IPv4, con el cual se permite establecer conexiones entre múltiples ordenadores.

Siendo un protocolo que se ha mantenido desde los primeros inicios del Internet, sus números de direcciones están limitadas y por eso se desarrolló el IPv6 que puede ofrecer más direcciones de las existentes.

Siendo los principales factores que se establecieron en este protocolo, otros datos adicionales sería que aparece en el año de 1981, el formato determinado

fue el de 32 bits divididos en cuatro octetos y como ejemplo de su notación decimal tenemos 192.168.1.1, y la cantidad de direcciones que podría conectar en total era de $2^{32}$=4294967296, adicionales a esta, están:

- El tamaño de paquetes debe admitir un tamaño de 576 bytes.
- Debe configurarse manualmente, o a través de DHCP.
- Se utiliza el protocolo de administración de grupos de Internet (IGMP).
- Se utiliza el descubrimiento de enrutadores ICMP, y es opcional.
- Utiliza registros de recursos (A) de direcciones de host en el sistema de nombres de dominios (DNS), para correlacionar nombres de host.com direcciones IPv4.

### 1.5.1. ESTÁNDAR IPv6

Con el crecimiento del uso para el Internet, se presentaron algunas dificultades al mantener este ritmo acelerado, siendo una de las principales situaciones, poder mantener un sin límites de direcciones IP. Por este motivo fue necesario la creación de una alternativa, que permita seguir con el aumento de estas direcciones, sin que se provoque cambios en las conexiones a Internet.

Es así, que aparece el nuevo estándar, denominado como Internet Protocolo versión 6 (IPv6), el cual busca optimizar los recursos en las direcciones y sub mascaras que se emplean para la identificación de usuarios, origen y destino, también para evitar esa limitación de IP que presentaba su sucesor, la versión 4 de estos protocolos.

Como se podrá visualizar, en los ejemplos la aplicación de esta nueva dinámica para la determinación de las direcciones IP, posibilita el incremento y manejo de todos los dispositivos que se vayan incorporando a la red, evitan así la limitación de las direcciones IP, de forma ilustrada se representaría de la siguiente manera:

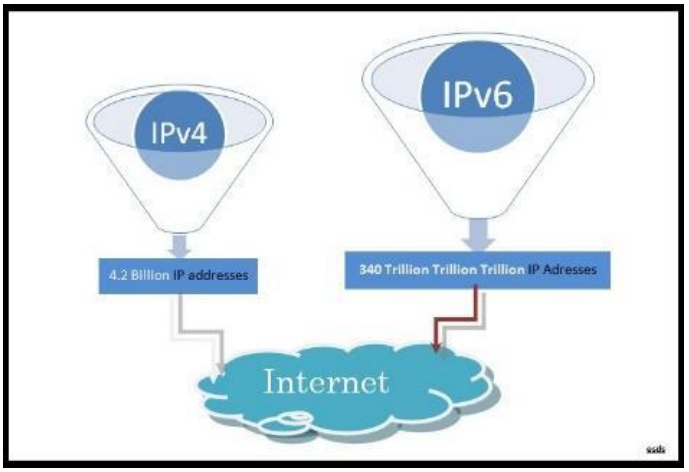


**Figura 4.** IPv4 vs IPv6

**Tomado de:** (kb.esds.co.in, s.f.)

## 1.6. ESTÁNDAR 6LoWPAN

Gracias al Internet de las cosas, existirá un mayor número de dispositivos conectados directamente a la red, o mejor sería decir que existirá una mayor cantidad de objetos físicos conectados a Internet. Los mentados objetos se valen de hardware especializado que le permite no solo la conectividad a Internet, sino que además programa eventos específicos en función de las tareas que le sean dictadas remotamente.

Se emplea para la conexión un único dispositivo, el conector, pero de forma inalámbrica para todos los equipos que se conecten a la red. Para ello se usa el protocolo nombrado como 6LoWPAN, ayudará con las conexiones a Internet según su nuevo estándar IPv6, el cual ha cambiado la nueva forma de ingresar a la red.

Con estas características este nuevo protocolo permitirá una mejor funcionalidad de los equipos que se conecten a Internet según su nuevo protocolo, el IPv6; es decir existirá una conexión directa entre el dispositivo e Internet. En la siguiente figura se observa un ejemplo de este tipo de conexión:


**Figura 5.** Ejemplo de conexión directa

**Tomado de:** (hipertextual, s.f.)

También se puede señalar como: “Es un grupo de trabajo en el área de Internet del IEFT, el nombre viene del acrónimo inglés Ipv6 Over Low Power Wireless Personal Area Networks que viene siendo Ipv6 para redes de área personal inalámbricas de bajo consumo” (García, 2015, pág. 7).

En la siguiente figura se podrá observar las capas de enlaces:

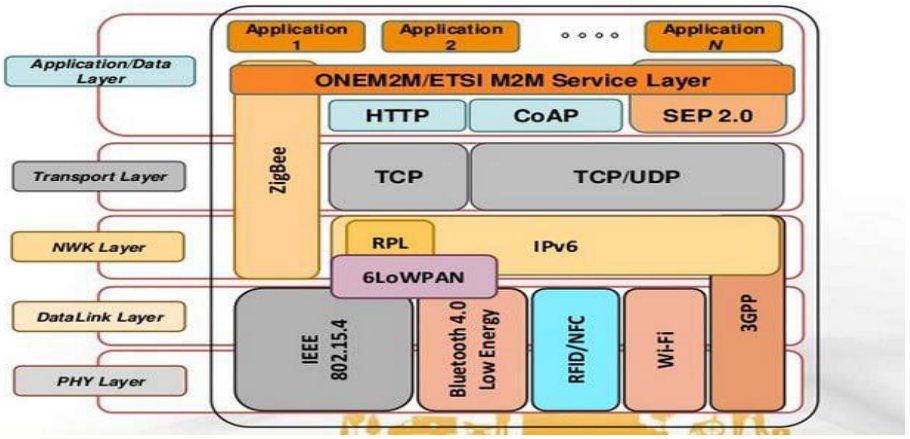


**Figura 6.** 6LoWPAN capas de enlaces.

**Tomado de:** (García, 2015, pág. 7)

**Data Link Layer**: se emplea en la familia de estándares IEEE 802, que compone el nivel básico de red, añadiéndose sobre la capa física, permite el control de acceso al medio de comunicación, de ahí su nombre. Entre sus funcionalidades se pueden encontrar:

- Corrección de errores de transmisión.

- Gestionar la transmisión entre dispositivos que se encuentran en un mismo canal de comunicación, regulando el acceso al canal físico.
- Agrega flag de control a las tramas para delimitar el inicio y fin de las mismas.
- La identificación de los dispositivos viene definida por la dirección MAC. (García, 2015, pág. 8).

**IEEE 802.15:** se especializa en redes WPAN, presenta una forma de interconexión de dispositivos de corto alcance, se dice que el espacio que cubren estas redes, es similar al que puede abarcar la voz de una persona.

**Dirección EUI-64 MAC:** está compuesto por 64 bits que permite identificar de manera unívoca un dispositivo en la red 802.15.4 (a diferencia de otras redes), esto genera la libertad de no necesitar implícitamente de dirección en la capa de red en comunicaciones básicas.

**CSMA/CA:** el control de flujo lo lleva la capa de enlace a través de un algoritmo, que a grandes rasgos lo que realiza por nodo, es la comprobación de la saturación del medio, mediante la escucha previa del canal de comunicación y el envío posterior (García, 2015, pág. 10).

**Cabecera 802.15.4**

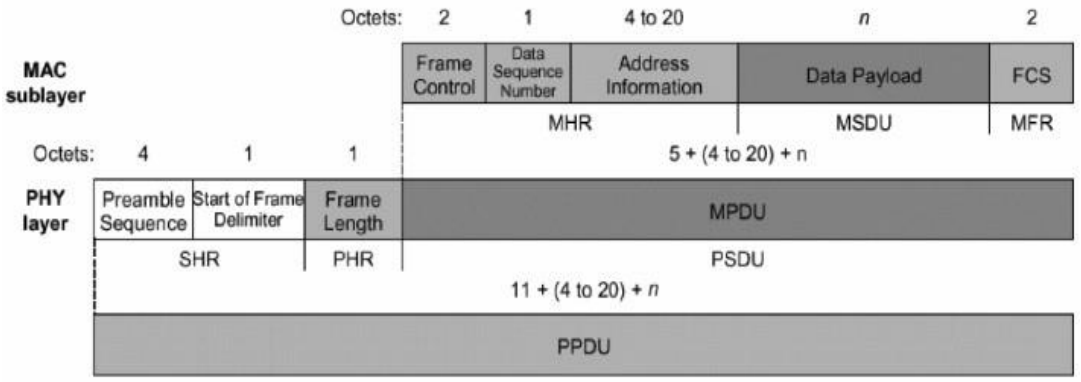


**Figura 7.** Cabecera 802.15.4

**Tomado de:** (García, 2015, pág. 10)

**Seguridad:** Ipsec permite cifrar las comunicaciones, además de permitir la autentificación de cada paquete IP que viaja por la red. Puede llegar a usarse entre un par de nodos, un par de gateways o entre gateways y nodos. Permite dar a la conexión entre los dos nodos, la capacidad de autentificar, evitando un ataque de falsificación de identidad (Reply Attack).

**Pila de protocolos IP y 6LoWPAN**

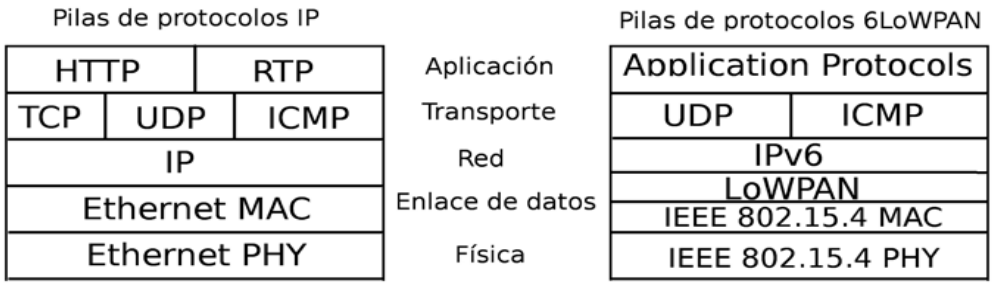


**Figura 8.** Protocolos IP y 6LoWPAN.

**Tomado de:** (CUC, 2012, pág. 167)

## 1.7. ESTÁNDAR ZigBee

ZigBee está basado en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (Wireless personal área Newark, WPAN) es un sistema para redes domóticas, diseñado para reemplazar la proliferación de sensores por nodos con transmisores inalámbricos que disponen de una antena integrada, control de frecuencia y una pequeña batería. ZigBee ofrece una solución tan económica porque la radio se puede fabricar con muchos menos circuitos analógicos de los que se necesitan habitualmente (Glen, 2012).

Básicamente sirven para el envío de datos en una baja tasa de las aplicaciones que requieren comunicaciones seguras, así se alarga la vida útil de las baterías.

La Alianza ZigBee define las capas superiores que corresponden a las de red y de aplicación y contienen perfiles de uso, ajustes de seguridad y mensajería.

A partir del Payload del nivel de aplicación, la entidad de datos crea y gestiona las unidades de datos del nivel de red y realiza un ruteo basado en la topología de la red en la que se encuentra el aparato. Así mismo el control puede

localizar la presencia de receptores, lo que posibilita la comunicación directa y la sincronización a nivel MAC (Glen, 2012).

En la siguiente figura se presenta un Mapa mental del ZigBee para su mayor comprensión:

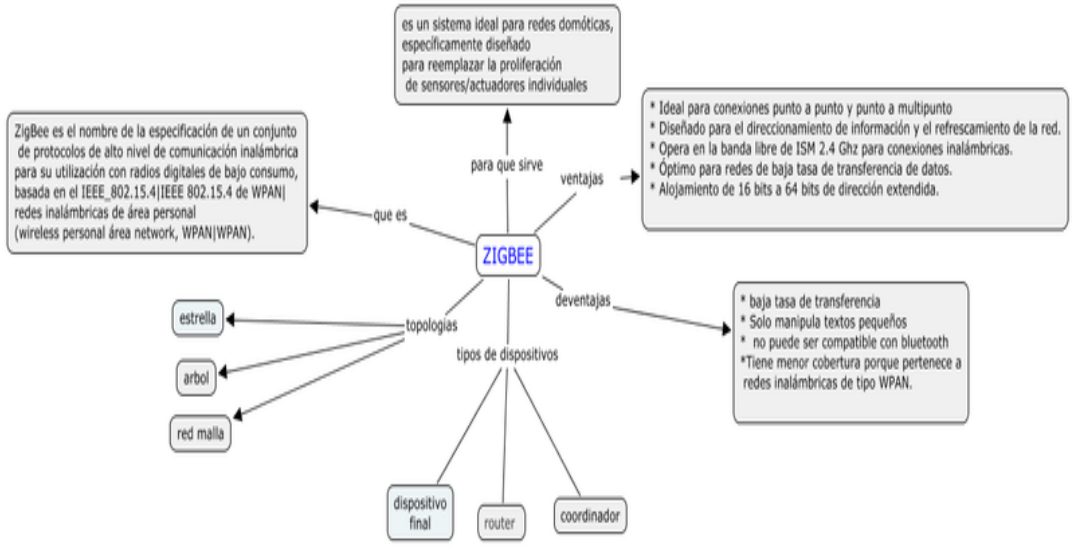


**Figura 9.** ZIGBEE mapa mental.

**Tomado de:** (Glen M, 2012)

## 1.8. ESTÁNDAR Z-Wave

El estándar Z-Wave está orientado a la automatización residencial y tiene por objetivo brindar un método fiable para controlar de forma inalámbrica una vivienda, es decir, Zwave es un protocolo Wireless destinado a la automatización de la vivienda. Fue desarrollado por el grupo danés Zen-Sys, que fue adquirido por Sigma Designs en 2008 (Tenealive, s.f).

### 1.8.1 Radio

A diferencia de ZigBee, la velocidad de su transmisión de datos puede llegar a los 9.6kbit/s, con una frecuencia menos potencial de 900 MHz, haciéndola adecuada para las aplicaciones de smarthomes en Europa, África y buena parte

de Asia, y un rango de alcance mayor, de 30 metros. Esta tecnología está especialmente indicada para el control de luces, calefacción, seguridad y asistencia en el hogar. Además, de la misma forma que ZigBee, su uso comporta un importante ahorro energético, pues es la responsable, entre otras funciones, de encender y apagar dispositivos remotamente. Es notable por su idoneidad para las funciones de automatización del hogar, pero entre las aplicaciones de Zwave destacan también la referente a la seguridad, especialmente para el pequeño comercio. Apoyada por la Zwave Alliance, su protocolo es más simple, con lo que su desarrollo puede ser más sencillo y fácil, con lo que es otro de los protocolos más demandados hoy en día (Tenealive, s.f).

### 1.8.2 Configuración de la red, topología y enrutamiento

Z-Wave utiliza una fuente de enrutado de red de malla. Los dispositivos pueden comunicarse entre sí mediante el uso de nodos intermedios, para activamente rodear y eludir los obstáculos domésticos o los puntos de radio muertos que podrían ocurrir en el ambiente de una casa. Por lo tanto, una red Z-Wave puede abarcar mucho más allá del rango de radio de una sola casa (Zwave, s.f).

La red más simple es un solo dispositivo controlable y un controlador primario. Se pueden añadir dispositivos adicionales en cualquier momento como controladores secundarios, por ejemplo controladores manuales, controladores de interruptor de pared, entre otros. Una red Z-Wave puede contener hasta 232 dispositivos.

Un dispositivo debe ser "incluido" en la red Z-Wave antes de poder ser controlado a través de Z-Wave. Este proceso, también conocido como "emparejamiento" y "adición", se logra usualmente pulsando una secuencia de botones en el controlador y en el dispositivo que se agrega a la red. Esta secuencia sólo necesita realizarse una vez, después de lo cual el dispositivo siempre es reconocido por el controlador. Los dispositivos se pueden quitar de la red Z-Wave por un proceso similar. El controlador aprende la intensidad de la señal entre los dispositivos durante el proceso de inclusión, por lo que la

arquitectura espera que los dispositivos estén en su ubicación final prevista antes de que se agreguen al sistema. Normalmente, el controlador tiene una pequeña batería interna de respaldo, lo que permite desconectarse temporalmente y llevarse a la ubicación de un nuevo dispositivo para emparejamiento. A continuación, el controlador vuelve a su posición normal y se vuelve a conectar (Z-Wave, s.f).

Cada red Z-Wave es identificada por un ID de red, y cada dispositivo es identificado además por un ID de nodo. El ID de red (también llamado Home ID) es la identificación común de todos los nodos pertenecientes a una red lógica Z-Wave. El ID de red tiene una longitud de 4 bytes (32 bits) y se asigna a cada dispositivo, por el controlador principal, cuando el dispositivo se "incluye" en la red. Los nodos con ID de red diferentes no pueden comunicarse entre sí. El Nodo ID es la dirección de un solo nodo en la red. El Nodo ID tiene una longitud de 1 byte (8 bits) y debe ser único en su red.

### 1.8.3 Seguridad

A pesar de que Z-Wave es un protocolo cerrado las investigaciones de seguridad todavía están en su fase inicial. Para analizar las capas de la pila del protocolo, se requieren el diseño de un dispositivo de captura de paquetes de radio y un software especializado para interceptar las comunicaciones Z-Wave (Philippe, 2015).

Se detectó de forma temprana una vulnerabilidad en cerraduras Z-Wave con cifrado AES (Advanced Encryption Standard) que podían ser desbloqueadas de forma remota sin el conocimiento de las claves de cifrado , pero esta vulnerabilidad no se debió a una falla en la especificación del protocolo Z-Wave, sino a un error de implementación del fabricante de las cerraduras (Philippe, 2015).

## 1.9. ESTÁNDAR Bluetooth

Es un estándar para redes de área personal inalámbrica, funciona en las frecuencias entre 2.402 y 2.480 MHz o 2400 y 2483,5 MHz incluyendo las bandas

de guarda de 2 MHz de ancho en el extremo inferior y 3,5 MHz de ancho en la parte superior. Esto es en el nivel global sin licencia (pero no reglamentada) Industrial, Científica y médica (ISM) banda de frecuencia de radio de corto alcance a 2,4 GHz. baja energía Bluetooth utiliza espaciado 2 MHz, que tiene capacidad para 40 canales (Udlap, 2013).

Bluetooth es un protocolo basado en paquetes con una estructura maestro-esclavo. Dos ciclos de reloj conforman una ranura de 625 mu s, y dos ranuras forman un par ranura de 1250 mu s. Los paquetes pueden ser de 1, 3 o 5 ranuras de tiempo, pero en todos los casos de transmisión del maestro comienza en las ranuras pares y el esclavo de las ranuras impares (Udlap, 2013).

Un dispositivo de Bluetooth maestro puede comunicarse con un máximo de siete dispositivos en una piconet (red ad-hoc ordenador mediante la tecnología Bluetooth), aunque no todos los dispositivos llegan a este máximo.

Los dispositivos pueden cambiar entre sí las funciones en un momento cumple el papel de maestro (principal) y luego pasa a ser esclavo (secundario) de otra unidad. El Bluetooth proporciona conexiones de dos o más piconets para formar una red dispersa donde algunos aparatos cumplen dos de estos roles simultáneamente. En estas conexiones se pueden transferir datos entre el maestro y el otro dispositivo (excepto para el modo de difusión de poco uso) (Udlap, 2013).

## 1.10. ESTÁNDAR SP100.11a

El objetivo principal del ISA100 es proporcionar una familia de estándares para redes inalámbricas industriales, que se ocupará de las necesidades de toda la planta, tales como el control de procesos, el personal, el seguimiento de activos y aplicaciones de larga distancia.

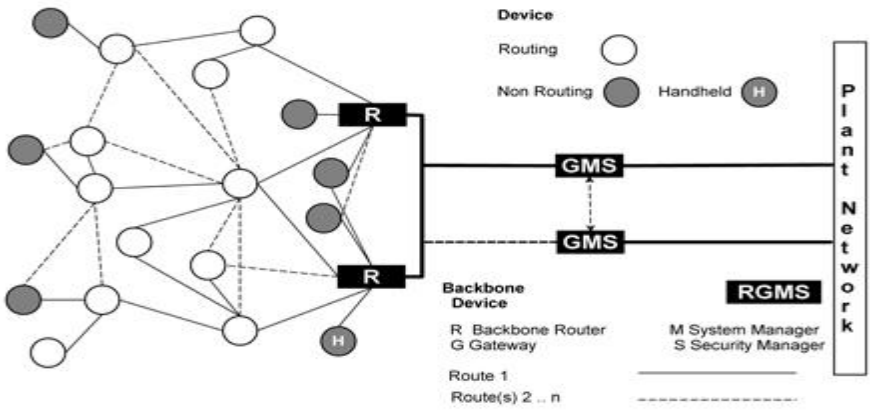


**Figura 10.** ESTÁNDAR SP100.11a.

**Tomado de:** (Amaral, 2011)

En la figura anterior se presenta dispositivos de enrutamiento y de no-enrutamiento, enrutadores de red troncal, un administrador de sistemas, un administrador de seguridad y una puerta de enlace.

En cuanto a los dispositivos de campo, los no enrutables son los dispositivos de I / O “Input/Output” (sensor y actuadores), mientras que los dispositivos de enrutamiento, también pueden actuar como dispositivos de I/O. Cabe mencionar que los dispositivos de enrutamiento desempeñan un papel importante en las redes de malla. En esta topología, los datos se transmiten desde la fuente hasta el destino a través de varios saltos, y los enrutadores son responsables de que los datos lleguen al destino correcto. Incluso pueden usar caminos alternativos para mejorar la confiabilidad. El enrutador de la columna vertebral es responsable de enrutar los paquetes de datos desde una subred a través de la red troncal hasta su destino, que puede ser otra subred o la puerta de enlace. La pasarela actúa como una interfaz entre la red de campo y la red de la planta (y las aplicaciones de host de control). El administrador del sistema es el administrador de la red y es responsable de la configuración de la comunicación (por ejemplo, asignación de recursos y programación) para la administración del dispositivo y el control de tiempo de ejecución de la red. El gestor de seguridad está a cargo de la gestión de la política de seguridad de la norma (Amaral, 2011).

# CAPITULO 2

# SISTEMA DE GESTIÓN DE SEGURIDAD Y FALLOS EN EL INTERNET DE LAS COSAS

En el presente capítulo se estudiarán los principales fallos que suelen ocurrir en sistemas informáticos y se valorará el impacto que pueden tener sobre aplicaciones relacionadas al Internet de las Cosas.

## 2.1. FALLOS DE SEGURIDAD EN LA INFORMACIÓN

En la actualidad la mayoría de vulnerabilidades de seguridad son fallas básicas de desarrollo e implementación. Según datos de Digiware estos ataques son muy comunes y representan más del 10%.

Como la seguridad consta de tres elementos fundamentales, estos forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son la confidencialidad, la integridad y la disponibilidad de los recursos. Bajo esta perspectiva, el atacante intentará explotar las vulnerabilidades de un sistema o de una red para encontrar una o más debilidades en alguno de los tres elementos de seguridad (Mieres, 2009). A continuación se muestran tres ejemplos:

**Confidencialidad.** Un atacante podría robar información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, atentando contra la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos.

**Integridad**. Mientras la información se transmite a través del protocolo de comunicación, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma. Este tipo de ataques se denomina Bit-Flipping y son considerados ataques contra la integridad de la información. El ataque no se lleva a cabo de

manera directa contra el sistema de cifrado pero sí en contra de un mensaje o de una serie de mensajes cifrados. En el extremo, esto puede convertirse en un ataque de denegación de servicio contra todos los mensajes en un canal que utiliza cifrado.

**Disponibilidad**. En este caso, un atacante podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema. Esto se conoce como Denial of Service (DoS) y atenta directamente contra la integridad de la información.

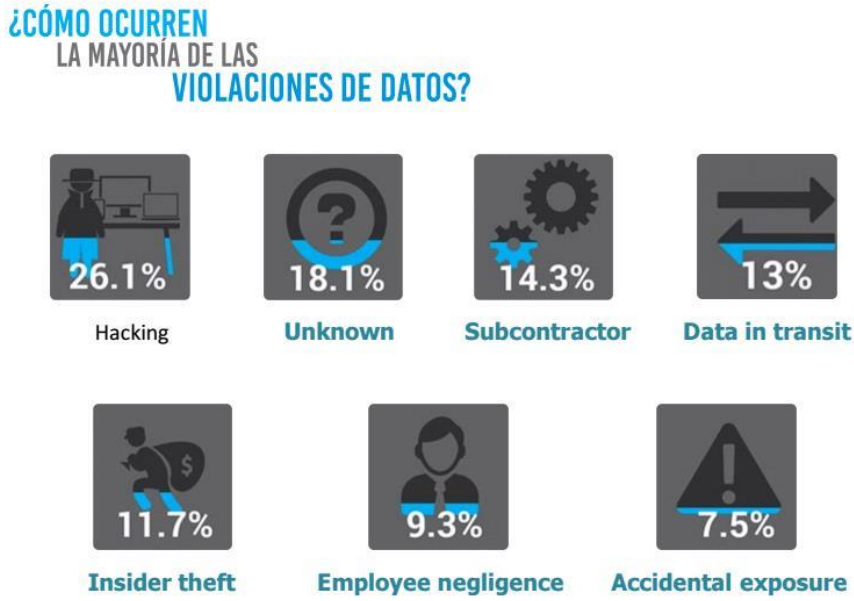


**Figura 11**. Violaciones de Datos

**Tomado de:** (Freire, 2015)

En los siguientes epígrafes se detallan las fallas más comunes que tienen lugar.

### 2.1.1. Falta de políticas, normas y procedimientos

Uno de los principales problemas encontrados en las organizaciones es que no sepan en que se están usando sus recursos tecnológicos, un ejemplo común de esto es el uso indebido de información de la empresa por medio de correos electrónicos.

### 2.1.2. Mala gestión del control de accesos

En algunas empresas que no tienen una gestión adecuada de perfiles y accesos de control se utiliza credenciales grupales para ciertos perfiles, debido a esto es técnicamente imposible identificar qué o cuáles personas realizaron determinada acción.

### 2.1.3. Ausencia total o parcial de un Administrador de la información

Una de las falencias más comunes en empresas de todo tipo, es la que se refiere a la ausencia total o parcial de un administrador de la información, este puede ser del área del negocio o técnica. Esta persona es la encargada de autorizar el acceso a cierto grupo de personas o una en específico a determinada información.

### 2.1.4. Planes de continuidad del negocio

Un plan de continuidad del negocio nos ayuda a prever situaciones de contingencia, un ejemplo de esto es la redundancia de servidores y servicios. Para que un plan de continuidad sea efectivo de ser constantemente actualizado y revisado.

### 2.1.5. Registros de aplicaciones

Se recomienda disponer de un registro de accesos a los servicios y aplicaciones. Esto con el fin de reconocer problemas de vulnerabilidad y determinar responsabilidades de los usuarios.

### 2.1.6. Copias de Seguridad

Uno de los bienes más importantes de una empresa es su información es por este motivo que se debe mantener a salvo las transacciones históricas de la empresa. Los procedimientos de respaldo deben mantenerse actualizados y constantemente probados para que estos sean restaurados de ser necesario en el menor tiempo posible.

### 2.1.7. Ausencia total o parcial de un Administrador de seguridad

La seguridad de la información es responsabilidad de toda la empresa. Sin embargo debe existir un administrador o responsable del proceso de seguridad. Es recomendable que exista una persona en específica para esta labor.

### 2.1.8. Usuarios

En cualquier organización un factor determinante para el éxito o fracaso son las personas. Por este motivo se debe capacitar constantemente al personal para la protección de la información de su información y así evitar amenazas de seguridad externas.

Según la página de Kaspersky Latinoamérica, La distribución de malware es principalmente dada por problemas de seguridad de los usuarios.

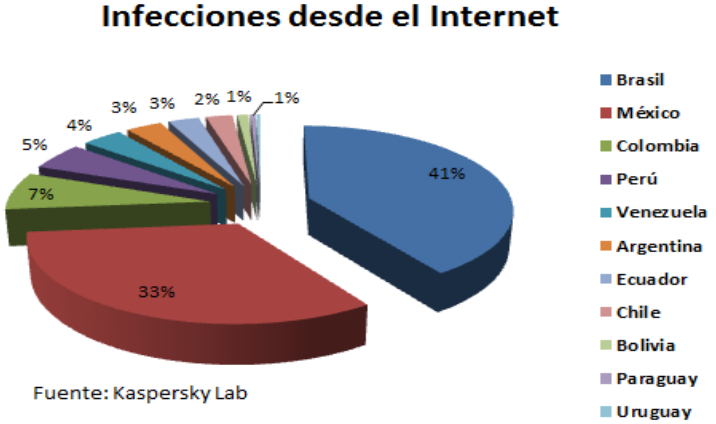


**Figura 12.** Infecciones desde el Internet

**Tomado de:** (Bestuzhev, 2012)

Las estadísticas mostradas incluyen ataques también ataques por descargas de la web, navegación no segura, email y FTP (Bestuzhev, 2012).

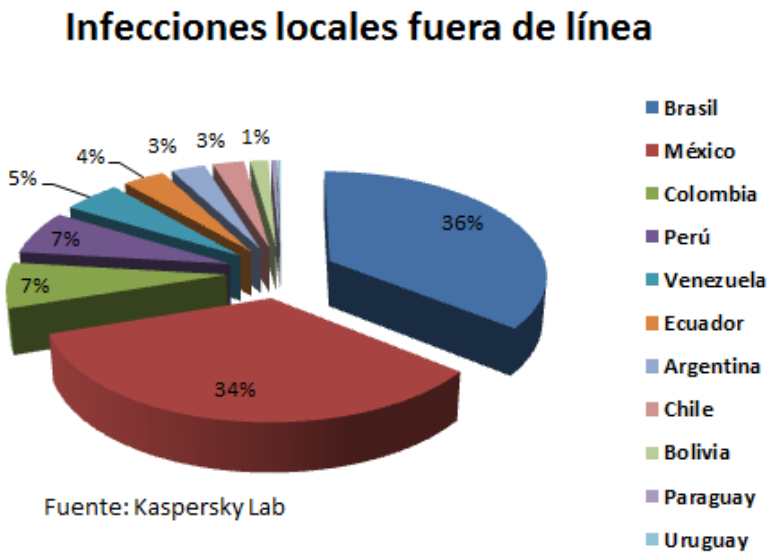


**Figura 13.** Infecciones locales fuera de línea.

**Tomado de:** (Bestuzhev, 2012)

En la gráfica estadística se muestra ataques fuera de línea tales como a través de dispositivos USB y otros medios donde se almacenada información.

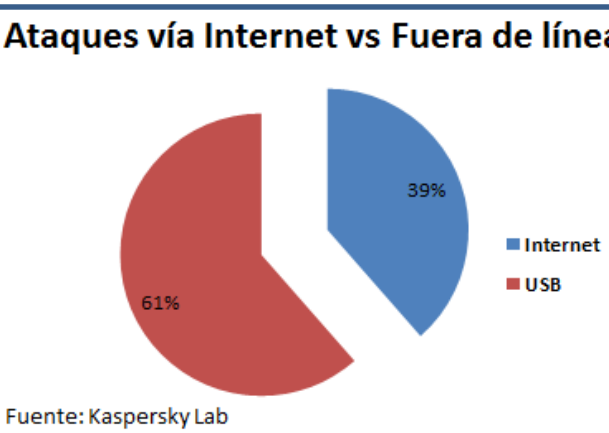


**Figura 14.** Ataques

**Tomado de:** (Bestuzhev, 2012)

Si se analizan las gráficas anteriores, muestran que en América Latina existen mayores ataques de malware por amenazas fueras de línea. Es decir que existe mayor riesgo por la mala utilización de dispositivos de almacenamiento de usuarios que por accesos no permitidos por la WEB.

## 2.2. RIESGOS ASOCIADOS A IoT

Los riegos varían dependiendo del dispositivo, aquí se analizará los riesgos más comunes y las principales áreas de afectación que conlleva la evolución de IoT. Actualmente se dice que existen más dispositivos electrónicos que personas conectadas, a continuación se muestra un crecimiento aproximado de los dispositivos electrónicos.

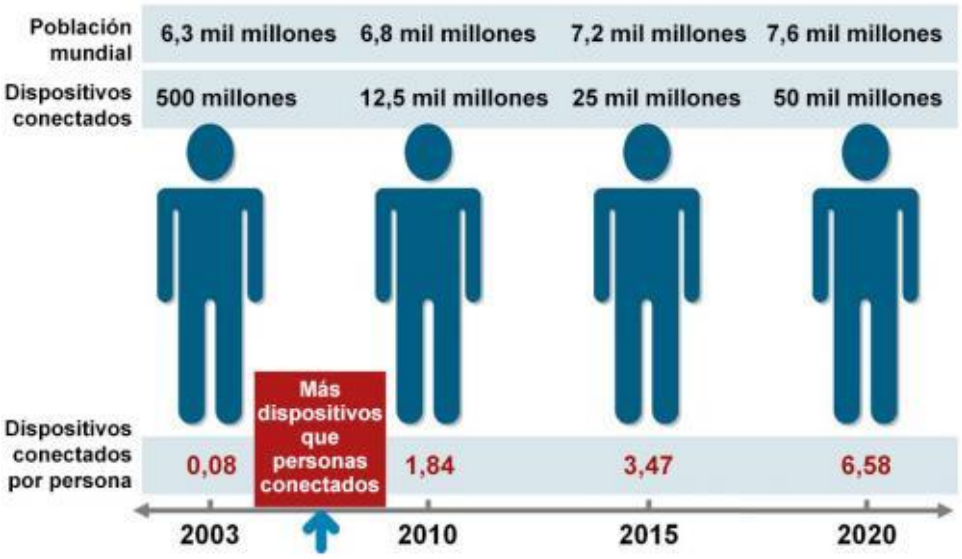


**Figura 15.** Dispositivos por usuarios.

**Tomado de:** (Evans, 2011)

Al materializarse una amenaza se pueden dar los siguientes inconvenientes:

- Accesibilidad
- Integridad

- Identidad
- Disponibilidad
- Confidencialidad

Cuando se da una amenaza puede afectar la accesibilidad de los dispositivos, por ende la integridad de la información y la identidad del usuario, ya que en la mayoría de las veces se suplanta la identidad para obtener información o beneficios económicos. Al afectar la identidad por materializarse una amenaza implica que no exista disponibilidad la mayoría de veces este aspecto es el de mayor influencia. En el caso de una empresa esto puede generar paradas de servicios que afecten el normal funcionamiento de esta. Otro factor a tomar en cuenta es la confidencialidad de la información.

Todos los factores antes mencionados son considerados como riesgos a IoT pero sin dudas la comunicación inalámbrica sea quizá uno de los riesgos a los que más expuestos se encuentre, puesto que en redes domésticas lo más generalizado es disponer de una red Wifi y, si esta red es insegura se convierte en una puerta de acceso a la red y por tanto a todos los dispositivos conectados a ésta (como pueden ser el horno, la lavadora, la calefacción,…) (csirtcv, s.f).

Según ESET en el año 2012, la infección por código malicioso a empresas alcanzó un 46.69%, estos datos se muestran en la Figura 16 y fueron tomados a nivel de Latinoamérica. Datos significativos considerando que IoT también engloba dispositivos utilizados en el entorno empresarial, se podría perder el control de una máquina de aire acondicionado de un centro de proceso de datos de una empresa, o de la nevera de un restaurante, o de las puertas de acceso a un comercio. Cualquiera de estos ejemplos podría provocar graves pérdidas a la organización afectada (ESET Security Report, 2014).


**Figura 16.** Violaciones de Datos

**Tomado de:** (ESET Security Report, 2014)

Adicional a estos las empresas se sienten preocupados por la fuga de información y falta de disponibilidad.

Como muestra la Figura 17, Ecuador se encuentra en el segundo puesto a nivel de Latinoamérica por infecciones de malware y ataques con código malicioso.

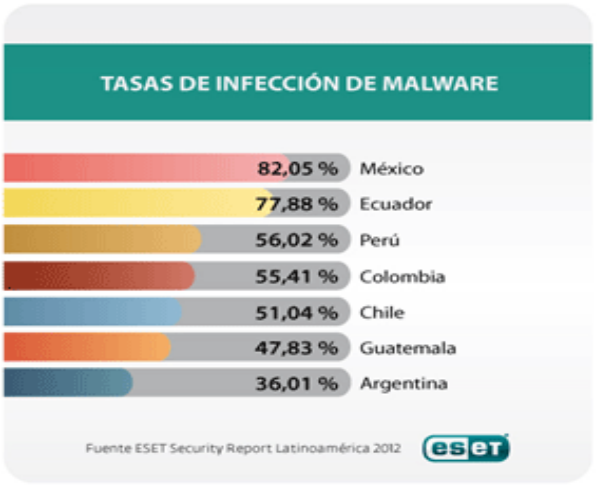


**Figura 17.** Violaciones de Datos

**Tomado de:** (ESET Security Report, 2014)

### 2.2.1. Casos de riesgos asociados al IoT

Los riesgos varían en función de la criticidad del dispositivo ya sea por la función que realiza o por la dependencia que se tenga del mismo. En cualquier caso, a continuación se exponen algunos de los riesgos más comunes y las áreas que pueden verse afectadas ante la materialización de una amenaza.

**Dispositivo GPS**: un ejemplo práctico son los dispositivos de geo posicionamiento, estos van conectados a Internet por lo que pueden ser fácilmente geo posicionados en todo momento (algunos incluso incluyen módulos GPS dedicados a ello). Esto hace que la localización del usuario quede registrada en algún sitio web y, en función de la configuración de privacidad pueda estar al alcance de cualquiera.

**Robo de información**: el caso del robo de información, puede no producirse por una vulnerabilidad en el acceso, como los dispositivos de geo posicionamiento son cada vez más pequeños, es más fácil perderlos también es un riesgo que cualquier persona tenga acceso a nuestra información.

El uso en la actualidad de múltiples dispositivos conectados a Internet puede hacer visible nuestra información, como las aplicaciones que interactúan con nuestro GPS revelando nuestra ubicación, rutas comunes y recorridos.

**Mal uso de los dispositivos**: actualmente uno de los más grandes riesgos al que nos enfrentamos diariamente son ataques que dejen vulnerables a nuestros equipos y perdamos el control total o parcial de ellos. El uso no legítimo de alguno de estos dispositivos puede afectar a la seguridad e integridad física de sus usuarios.

Los riesgos mencionados en este capítulo, no son tan alejados de la realidad Ecuatoriana a diario vemos que más dispositivos móviles aparecen, de la misma manera más vulnerabilidades y ataques se dan. En el 2012 se reportaron 839.705 usuarios de teléfonos inteligentes (Smartphone), un 60% más que lo del 2011, cuando llegó a 522.640 usuarios, según datos de la encuesta de Tecnologías de

la Información y la Comunicación (TIC) del Instituto Nacional de Estadística y Censos (INEC) (INEC, s.f).

Aunque quizá se crea que son bajas las amenazas de este tipo, hay que tomar en cuenta que ha llegado a la IoT, a los entornos profesionales e industriales. Los sistemas SCADA, como parte de IoT, integran sensores como son el caso de sistemas complejos de control de tráfico, distribución de recursos entre otros. Es obvio que existe riego inminente a sufrir atentados al utilizar sensores inalámbricos y estos aumentan su vulnerabilidad al ser conectados a Internet (Evans, 2011).

## 2.3. VECTORES DE ATAQUE AL IoT

Para analizar las principales vulnerabilidades se deben tomar en cuenta los principales vectores de incidencias de IoT.

Los dispositivos IoT pueden acceder a su interface de administración mediante otros medios puesto que no disponen de una entrada o salida de datos.

En el momento de fabricación de un dispositivo nace la necesidad de establecer una configuración por defecto segura, a esto se le llama el concepto de SbD.

En su gran mayoría no se cumple con este estándar y esto es sumamente riesgoso, ya que un 86% de los usuarios no tienen conocimientos de configuración de seguridad de su dispositivo, por este motivo el 86% de los dispositivos pueden mantener una configuración insegura (Evans, 2011).


**Figura 18.** Violaciones de Datos

**Tomado de:** (Freire, 2015)

Otra vulnerabilidad muy común en este tipo de dispositivos es su ubicación física un ejemplo de esto son desde televisores, dispositivos Wearables, sensores en redes de detección de incendios, sistemas domóticos, etc. Adicionalmente a los riesgos de seguridad, este tipo de dispositivos lastimosamente si no son de calidad afectan a la seguridad física y salud de sus usuarios habituales.

### 2.3.1. Vulnerabilidad en la transmisión de datos

En vista que estos dispositivos están enfocados al envío y recepción de información entre ellos o a Internet puede sufrir ataques a la transmisión de datos. Una de las medidas más importantes será siempre la protección de la información en tránsito.

Analizando el entorno actual de las comunicaciones la conectividad requiere un elevado canal de datos que distribuyen sus servicios por medio de redes cableadas, inalámbricas y cualquier medio de transmisión. Todos estos medios de transmisión, especialmente las que se propagan inalámbricamente o por redes públicas son más sensibles de sufrir ataques en las comunicaciones (CSIRT, 2007).

De no proteger eficientemente el canal de comunicación con cifrado de datos, se pueden dar ataques de tipo Man In The Middle. Estos ataques se basan en capturar el tráfico, cambiarlo y aparentar ser el origen del mismo y enviarlo al servidor legítimo, es decir actúa como un punto intermedio en las comunicaciones. De esta el atacante manera obtiene la información que desee incluso modificarla o eliminarla para alterar el funcionamiento de cualquiera de los dos interlocutores.

Un ejemplo real y práctico de este caso sería un vehículo con el servicio de Chevy-star App que conectado por medio de una conexión celular muestra su ubicación, velocidad, estado, etc. a través de un servicio que mantiene el fabricante alojado en sus servidores. Si existiera una deficiencia en el intercambio de información entre el vehículo y el servicio de Chevy-star, un atacante podría interceptar la información suministrada por el vehículo y hacerla llegar al servidor del fabricante solo tomando lo necesario sin que el proveedor del servicio se dé

cuenta de esto. De esta manera el atacante podría conocer sin problemas toda la información que el vehículo enviara al servicio online, como por ejemplo la posición GPS, el domicilio o enviar comandos remotos como por ejemplo abrir o cerrar las puertas y de esta manera sustraerlo (Iiabspain, 2014).

El portal oficial de Chevy-star, muestra todos los servicios disponibles en sus vehículos como por ejemplo: bloqueo y apertura de puertas, estadísticas de ubicación del GPS, alertas de estacionado, activación de luces y bocinas, interacción por vía celular entre otros (Iiabspain, 2014).


**Figura 19.** Violaciones de Datos

**Tomado de:** (Iiabspain, 2014)

### 2.3.2. Vulnerabilidades en el software

El porcentaje de ataques al sistema operativo es bastante alto en América Latina y Ecuador, en algunos dispositivos se utilizan versiones reducidas y básicas para abaratar los costes de fabricación. Este hecho, es un riesgo de seguridad, ya que cuando se detectan vulnerabilidades, se facilita a los potenciales atacantes una puerta de entrada.

Otro vector de ataque bastante común son las interfaces web, por su uso frecuente en dispositivos IoT, por su pequeño tamaño y recursos de hardware limitados, permitiendo de esta manera su administración remota. Es importante destacar que en su gran mayoría estas interfaces web se publican directamente a Internet para

que sea más fácil la administración del dispositivo desde la red. En su gran mayoría se utilizan plataformas web comunes, por esta razón si existe un ataque, afecta a la seguridad de todos los dispositivos.

Para demostrar la problemática existente en este tipo de vectores de ataque, se considera el siguiente escenario: un sistema domótico en una vivienda, actualmente permite una gran cantidad de opciones, como controlar refrigeradoras, climatización, revisión de suministro de gas o agua, encender o apagar luces, etc. Normalmente se accede a estas aplicaciones mediante servidores intermedios como servicios en la nube. Cualquier posible deficiencia en el software empleado por los propios dispositivos IoT, apps móviles o el servicio cloud podría comprometer la información facilitada, así como permitir a un atacante potencial manipular a su antojo todos los dispositivos que se han mencionado con anterioridad.

### 2.3.3. Vulnerabilidades de Configuración

En el mundo de IoT, la mayoría de los dispositivos no siguen una política adecuada de SbD.

La mayoría de dispositivos habilitan muchas de sus funcionalidades en sus configuraciones por defecto, normalmente muchas más de las que emplea el usuario.

Un ejemplo real, en un router de acceso a Internet, como el que se puede encontrar en cualquier vivienda. En muchos casos disponen de acceso a su interfaz de administración con distintos protocolos: HTTP, SSH, TELNET, etc. Normalmente están habilitados todos los protocolos, estos representan una potencial brecha de seguridad. La solución para este problema es la autenticación en el acceso a los mismos, cifrando y validando correctamente el destino de la información antes de realizar cualquier envío (CSIRT, 2007).

### 2.3.4. Vulnerabilidad de hardware

La mayoría de las ocasiones suelen ser las vulnerabilidades menos frecuentes, normalmente cuando se producen tienen una criticidad alta y son con mucho las más difíciles de subsanar. Para realizar un ataque contra el hardware de un dispositivo se debe analizar la estructura y el comportamiento del dispositivo de acuerdo a sus capacidades.

El ataque al hardware se realiza cuando la seguridad del software es robusta o en sistemas localizados de redes aisladas o bien resguardadas de un acceso público vía Internet. Por ejemplo el acceso directo a los componentes de almacenamiento tanto volátil (memoria) como no volátil (disco duro, memoria flash) es una técnica de ataque habitual.

Así podría ser menos dificultoso el acceso a la memoria y la información que contiene todo dependiendo del diseño del dispositivo y de las protecciones implementadas en los datos de acuerdo al diseño del dispositivo.

## 2.4. RECOPILACIÓN DE INFORMACIÓN

El impacto de los fallos asociados a IoT es muy alto, en este apartado se presentan algunos de los incidentes más relevantes encontrados a fin de demostrar la afirmación anterior.

La compañía Tesla diseña, fabrica y vende coches eléctricos, sus componentes y sistemas de almacenamiento a baterías, además destaca por su conectividad, funcionalidad y acceso a Internet. El atacante controló de forma remota la funcionalidad de las bombillas de un vehículo desde la red doméstica sin ser un usuario autorizado (Proofpoint, s.f).

Es justo pensar que los posibles ataques que se pueden realizar son complejos y que no están al alcance de cualquiera. Esto no es así en todos los casos.

En agosto de 2014 se dio a conocer una vulnerabilidad en un dispositivo wearable de uso muy difundido, el reloj Pebblec. Es un smartwacth que se puede enlazar a

un Smartphone, mostrando por su pantalla las notificaciones recibidas. La vulnerabilidad podía provocar condiciones de denegación de servicio, así como en algunos casos borrar la memoria del dispositivo. El ataque únicamente consistía en enviar 1500 mensajes de WhatsApp al dispositivo en un periodo de 5 segundos (CSIRT, 2007).

## 2.5. PREVENCIÓN

Una vez analizado el estado del arte respecto a IoT, el siguiente paso será garantizar un uso seguro de las mismas. Se pueden aplicar una serie de medidas de seguridad que ayuden a mitigar en la medida de lo posible los riesgos de seguridad derivados del uso de estos dispositivos.

Por ello para afrontar el uso seguro de IoT se tratará los puntos de atención de la seguridad en IoT y las posibles salvaguardas aplicables (CNET).

### 2.5.1. Interfaces de acceso

La gran mayoría de dispositivos no disponen de interfaces directas como teclados o pantallas. Por esto es necesario implementar una interfaz web que permita configurar todos los parámetros del dispositivo, pero el problema es que su configuración es con credenciales de acceso por defecto sin mecanismos de autentificación. Por ello es fundamental que se sustituyan por credenciales generadas por el usuario con la mayor complejidad posible.

### 2.5.2. Actualización de Equipo

En muchas ocasiones, e independientemente de la configuración que pueda realizar el usuario, la propia implementación del dispositivo está afectada por diversas vulnerabilidades de seguridad que pueden comprometerlo. Para mitigar este riesgo, se recomienda mantener el dispositivo actualizado con la última versión de software o firmware facilitada por el fabricante.

En caso de que ya se disponga del dispositivo y no del soporte, o se trate de un soporte muy discontinuado, la recomendación será mantener el dispositivo oculto

dentro de una red local sin que se publique directamente a Internet, e implementar medios alternativos de acceso a dicha red que ofrezcan una conexión segura (VPN) si se requiere el acceso remoto, como se ha comentado con anterioridad (CSIRT, 2007).

### 2.5.3. Configuración Red de Datos Segura

Habitualmente, los fabricantes de los dispositivos habilitan múltiples puertos de acceso o gestión. Cuando se configura el acceso a un dispositivo de estas características a Internet, se debe controlar que únicamente se permita el acceso a los puertos estrictamente necesarios, de este modo se reducirán los riesgos de seguridad sustancialmente.

### 2.5.4. Control de Servicios Cloud

Un riesgo a tener en cuenta con dispositivos IoT es el de que los datos pueden acabar en Internet mediante el acceso a servicios en la nube o Cloud Services. En este caso, no es necesario que se abran puertos al exterior, ya que con únicamente un acceso a Internet normal el dispositivo podrá enviar información a sitios públicos en Internet. Otro caso común es que el dispositivo pueda ser gestionado externamente empleando un servicio web prestado por el propio fabricante.

# CAPITULO 3

# PROPUESTA DE PAUTAS A SEGUIR PARA DISEÑAR EFECTIVOS SISTEMAS DE GESTIÓN DE SEGURIDAD Y FALLOS

En el presente capítulo se elaborar una propuesta de lineamientos a seguir para la implementación de un sistema efectivo de gestión de seguridad y fallos para aplicaciones de Internet de las Cosas basados en el estándar 6LoWPAN. Se fundamenta lo expuesto de forma teórica en los capítulos anteriores y se brinda un ejemplo práctico de la provisión de servicios de la Internet de las Cosas sobre redes de sensores basadas en 6LoWPAN.

## 3.1. CRITERIOS PARA IMPLEMENTAR SISTEMAS DE GESTIÓN DE SEGURIDAD Y FALLOS EN IoT MEDIANTE 6LOWPAN

Como se analizó en el capítulo anterior un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software o en el hardware.

Los sistemas de Internet de las cosas suelen ser muy complejos y requieren soluciones de seguridad integrales que puedan distribuir capas de conectividad en la nube, los dispositivos de Internet de las cosas son recursos restringidos y no suelen tener el poder suficiente para admitir las soluciones de seguridad tradicionales.

La seguridad, en su aspecto más técnico, se puede definir como aquellas actividades enfocadas a proteger un determinado dispositivo o servicio, así como todo aquello con lo que interactúa e intercambia con otros dispositivos o servicios, ya sea información, datos, señales, etc. Utilizando como base la anterior definición, la seguridad de IoT se podría definir como aquellas actividades encaminadas a la protección de los objetos y sus comunicaciones o interacciones con otros objetos.

La seguridad de IoT es controversial por un lado plantean que no parece un tema que haya llamado especialmente la atención de los investigadores y por otro afirman que las tecnologías sobre las que se basa la Seguridad en el Internet de las Cosas son tan seguras por definición que no se requieren nuevos esfuerzos para mejorar lo ya existente. El investigador coincide en que es necesario prestar mayor atención a la seguridad en el IoT.

### 3.1.1 Criterios para la seguridad en redes inalámbricas

A la hora de proponer los lineamientos a tomar en cuenta para desarrollar sistemas de seguridad y fallos en IoT, es necesario tener en cuenta las normas básicas para configurar una red inalámbrica puesto que IoT se basa en redes Wireless y está condicionada a todas sus vulnerabilidades. Según Simal, (2011) las consideraciones más importantes son las siguientes:

- **Cambiar las configuraciones por defecto**: parámetros como las calves y usuarios o el nombre de red se mantienen inalterados. Es cierto que la en la mayoría de las instalaciones se cambia el nombre de la red, pero algo tan importante como la clave de acceso del administrador, en muchos casos, se mantiene inalterada, provocando un punto de acceso simple para cualquier intruso.

- **Activar encriptación**: es una de las prácticas claves y necesarias. Es el método básico y más inmediato de impedir accesos no autorizados a la red, así como capturas de tráfico y datos privados.

- **Uso de claves "fuertes":** puesto que es la llave a la red, las claves utilizadas han de ser suficientemente seguras y complejas de averiguar para asegurar la seguridad de la red. Es frecuente usar claves de solo letras, con palabras comunes y muy habitualmente referenciado a datos personales del administrador, como nombres de hijos, edades, etc. que hacen dicha clave fácil de averiguar.

- **Desactivar el anuncio del nombre de red**: aunque no es viable en todos los casos, la desactivación del anuncio del nombre de la red es un elemento

de seguridad añadido. Por un lado, impedirá al atacante identificar la naturaleza y propietario de la red, y por otro hará necesario introducir el nombre de la red manualmente para permitir la asociación a la red Wi-Fi, por lo que previamente deberá ser conocida por el atacante.

- **Filtrados de direcciones MAC**: En la mayoría de los puntos de acceso es posible especifica una lista de direcciones MAC que serán admitidas, siendo todas las demás rechazadas. La dirección MAC es una dirección de nivel 2 que lleva la tarjeta de red Wi-Fi grabada de fábrica (análoga a la dirección MAC-Ethernet). Por tanto, si se permite solo el acceso a las direcciones MAC pertenecientes a los equipos propios se impedirá que algún sistema externo pueda conectarse de forma accidental o premeditada.

- **Uso de direcciones IP estáticas**: No un problema real para un hacker con conocimientos, pero si dificulta el acceso a intrusos ocasionales. Es habitual tener en las redes Wi-Fi la asignación automática de direcciones IP, Gateway y DNS. La práctica de asignar las direcciones manualmente a los terminales inalámbricos tiene la ventaja de que el atacante ha de averiguar en primer lugar los datos de la red, y más importante, nos permite habilitar filtros de manera que solo las direcciones IP asignadas sean permitidas. En caso de que el atacante utilice alguna de las IP asignadas, eventualmente podrá ser detectado pues entrará en conflicto con los terminales legales.

- **VLAN propia para la red Wi-Fi:** Es interesante la implementación, en aquellos equipos que lo permitan, de una VLAN específica para la red Wi-Fi. Al ser una red insegura por su propia naturaleza, es recomendable mantenerla separada en todo momento de la red cableada. Así pues, si el punto de acceso, o el controlador asociado, es capaz de gestionar VLANs, mantener el tráfico proveniente de la red Wi-Fi en una VLAN distinta permitirá implementar mecanismos de seguridad y acceso suplementarios que controlen el acceso de los usuarios Wi-Fi a los datos de la red.

- **Instalación de un Firewall**: Relacionado con el punto anterior, el acceso de los clientes Wi-Fi a la red cableada debería ser gestionado por un Firewall,

ya sea actuando de puente entre las correspondientes VLAN's o como elemento físico de control, interponiéndose en flujo de tráfico Wi-Fi. En cualquier arquitectura, la inclusión de un firewall nos permitirá implementar políticas de acceso seguras y complejas que aseguren que, aunque algún intruso hubiera conseguido conectarse a la red inalámbrica, no progrese hasta tener acceso a datos sensibles.

### 3.1.2 Criterios de seguridad para el internet de las cosas

Las medidas del epígrafe anterior, correctamente implementadas proporcionan seguridad suficiente para entornos no sensibles. Sin embargo por la dimensión de IoT se pueden presentar problemas más complejos. Hasta el momento no están todas las soluciones a las brechas de seguridad pero expertos de la Comisión Europea, señalan como aspectos importantes a tener en cuenta los siguientes:

- Asegurar la continuidad y la disponibilidad en la provisión de servicios basados en IoT, tratando de evitar posibles fallos e interrupciones en el funcionamiento. Esto está muy relacionado con el modelo de arquitectura a utilizar en la prestación de los servicios basados en IoT: centralizado vs descentralizado.

- Consideraciones en el diseño de tecnologías IoT. Es muy conveniente tener en cuenta las cuestiones de seguridad y privacidad en la fase de diseño. Los objetos IoT no suelen disponer de recursos suficientes, memoria y procesamiento, como para implementar las protecciones necesarias de seguridad a posteriori, o al menos aplicar las medidas de seguridad tradicionales.

- Los riesgos son sensibles al contexto y aplicación. Dependiendo del contexto o ámbito de aplicación, los riesgos cambian dependiendo de lo que se requiera. La heterogeneidad de los objetos supone un gran problema en cuanto a tratar de crear soluciones de tipo más universal.

- Trazabilidad / análisis del rendimiento / tratamiento ilícito. El aumento de recopilación de datos puede plantear problemas de autenticación y confianza en los objetos.

- Reutilización de los datos / ampliación de la verdadera misión de los datos. Debido a la proliferación de cada vez más cantidad de datos en los entornos IoT, es posible que estos datos puedan llegar a utilizarse para otros propósitos para los que no fueron creados originalmente, algo que es necesario controlar.

- Ejercicio de los derechos de protección de datos para las personas y el cumplimento de la legislación para las organizaciones. Con las aplicaciones de los objetos IoT funcionando en “background”, no siempre las personas son conscientes de las capturas de información o el tratamiento que se le está dando a esa información. El acceso y control de datos, el permiso para recopilarlos y la frecuencia óptima para su recolección, son aspectos necesarios a tener en cuenta.

- Pérdida / violación de la privacidad y protección de datos de los individuos. Un ejemplo puede ser las nuevas tarjetas de crédito contactless, donde es posible leer el nombre y número de la tarjeta sin utilizar autenticación alguna, datos con los que un atacante podría llegar a realizar compras ilícitas.

- Realización de ataques maliciosos contra los dispositivos y sistemas IoT. Si no se utilizan los controles de seguridad adecuados esto se convierte en un problema grave que puede conducir a otros problemas como los anteriormente mencionados. Lo difícil aquí es identificar los controles más apropiados para los sistemas IoT, para los que todavía se desconoce su evolución futura. Podría ser necesario definir controles adaptados a cada sistema o arquitectura.

- Lock-in del usuario, en cuanto a que los usuarios se queden “bloqueados” en un proveedor específico de servicios IoT y les sea difícil migrar a otros proveedores, algo provocado por la no homogenización.

- Pérdida del control por parte del usuario / dificultad en la toma de decisiones. Uno de los principales objetivos de la IoT es dar cierta autonomía a los objetos y permitirles tomar decisiones de forma automática. Es necesario saber acotarlo en los casos que pueda suponer un problema y controlarlo adecuadamente para que no suponga riesgos o afecte a sus usuarios. Las decisiones tomadas de forma automática por dispositivos y aplicaciones, basadas en el enorme conjunto de datos obtenidos podría no ser transparente para los titulares de los datos y por lo tanto crear la sensación de pérdida de control sobre estos.

- Legislación aplicable. Dado el carácter global de IoT, otro problema es que los individuos y empresas se enfrentan a una serie de leyes de protección de datos nacionales / regionales que ofrecen distintos niveles de protección. Es necesario prestar especial atención a las leyes aplicables dependiendo del lugar donde se encuentren los objetos del IoT (ec.europa.eu, s.f).

## 3.2. VENTAJAS Y DESVENTAJAS DEL USO DEL ESTÁNDAR 6LoWPAN

Además de analizar los retos propios del Internet de las Cosas, se profundizan las vulnerabilidades del estándar 6LoWPAN y como se puede gestionar la seguridad y los fallos mediante su uso.

Entre los beneficios de 6loWPAN se encuentran: el fácil uso por ser un estándar abierto, confiable y estandarizado; integración transparente con internet, escalabilidad global, flujo en-to-end, el uso existente de la infraestructura de internet, uso mínimo de cogido y memoria, entre otros. (Diedrichs, 2013)

Además 6loWPAN incorpora el uso de Multicast en comunicaciones inalámbricas de baja potencia, lo que anteriormente no era soportado por las tecnologías de comunicación de radio existentes; permite utilizar de manera más fácil una red con topología malla y optimiza el uso de los estándares de Internet sobre redes inalámbricas de baja potencia.

Tomando en consideración que 6LoWPAN se utiliza en redes con un alto exponente de dispositivos conectados y se hace necesario reducir el uso que cada dispositivo hace de la red, para ello comprimen los 42 bytes de tamaño de cabecera de una IPv6 normal a solo 6 bytes en su mínima implementación y el servicio DHCP ha sido modificado de tal manera para que el consumo de los nodos sea el mínimo posible.

Si bien una de las ventajas de este protocolo es la facilidad de conexión de la red WPAN a Internet utilizando paquetes de tipo Ipv6 para simplificar la interface entre redes de sensores e Internet tiene como desventaja que los nodos de sensores tienen limitaciones en capacidad de procesamiento. IPv6 requiere soporte de paquetes más grande que lo que brinda IEEE 802.15.4. El Payload máximo de IEEE 802.15.4 es de 128 bytes contra 1280 bytes requeridos por IPv6 por lo que requiere una fragmentación. Para eso se agrega una capa en 6LoWPAN llamada capa de adaptación que fragmenta y rearma los paquetes.

Las versiones del protocolo IP (IPv4/IPv6) asumen que los dispositivos siempre están conectados a la red, a pesar de que no estén transmitiendo. En 6LoWPAN, los dispositivos sólo se conectan a la red cuando deben transmitir información, lo que permite un uso eficiente de la energía necesaria para dicha operación.

6LoWPAN tiene implementado cifrado mediante AES-128 necesario para brindar seguridad a los datos transmitidos.

### 3.2.1 Ejemplo de implementación de una red utilizando 6LoWPAN

En la Hacienda Cananvalle de la ciudad de Ibarra se diseñó una red inalámbrica de sensores a través de 6loWPAN para una agricultura de precisión, con el objetivo de brindar al sector agrario sistemas de optimización del agua de riego con fines productivos, por la escasez que se presenta en el sector y así poder dotar a los cultivos la cantidad adecuada que necesita para poder sobrevivir y producir. Con esta mejora en el sistema de riego se puede sembrar todo el año incluyendo las épocas de escasez de agua e inclusive regar toda la superficie sembrada.

Se pudo controlar y monitorear de forma manual, activando el riego a una determinada hora o dependiendo de los parámetros de las mediciones de los sensores, todo esto con la utilización de cualquier dispositivo ya sea una computadora personal o un dispositivo móvil inteligente. Para la recolección de las mediciones de la red de sensores inalámbricos se utiliza el estándar 6loWPAN y se plantea dos arquitecturas: una que es la implementación de nodos clientes que recolectan y envían la información y un nodo servidor que recolecta las mediciones por medio del protocolo de transporte UDP; y otra, una implementación de nodos clientes y nodo router-border que permite visualizar el estado actual de los sensores por medio de una página web que se encuentra almacenada en el nodo y utiliza el protocolo transporte TCP.

Otro ejemplo práctico para brindar servicios a través de una red de sensores 6LoWPAN se diseñó para monitorizar la temperatura y gestionar la iluminación en un hogar. Se realizó utilizando el Sistema Operativo Contiki y como kit de desarrollo el STM32W108C. Se decidió utilizar el driver nullmac_driver, sin CSMA/CA y el protocolo de enrutamiento RPL enfocado para redes LoWPAN que ofrece también el Sistema Operativo.

Para la comunicación entre nodos se configuró cada uno de ellos para que compartieran el identificador de red, canal, protocolo de direccionamiento y enrutamiento en el fichero en contiki-conf.h. Uno de los nodos funciona como servidor UDP y espera peticiones del otro nodo cliente. La aplicación se desarrolla con API de Contiki y con este se crean los sockets UDP y el intercambio de datagramas. Luego de conectar los dos sensores, el principal objetivo es ampliar el rango de acción, primero por una red ad-hoc a una red LoWPAN con interacción externa IPv6, para ellos uno de los nodos será el router de borde e implementará la capa de adaptación. Se utilizará un rpl-border-router. El router de borde tiene dos interfaces, LoWPAN y otra externa. La LoWPAN con plataforma MB951, donde corre rpl-border-router. Se utiliza SLIP con modificaciones realizadas en Contiki para adaptarlo a IPv6. (Romkey, 1988)

Para establecer la conexión se utilizó la herramienta tunslip6 que genera una interfaz virtual IPv6 mientras que la operativa transmite paquetes hacia la red LoWPAN. La operación de tipo READ dará a conocer los datos de temperatura y acelerómetro, también se podrán actualizar recursos por medio de UPDATE y de dos variables (ipDestino y periodoEnvio) que se usan para almacenar de manera automática los datos de monitorización, los nodos envían los datos a un servidor remoto. Para finalizar se tiene el control de iluminación, un led que es de tipo UPDATE.

# CONCLUSIONES Y RECOMENDACIONES

## CONCLUSIONES

El estudio de la bibliografía existente permitió evidenciar que los avances de internet han tenido un crecimiento exponencial en los últimos años. Uno de sus grandes retos lo constituye el Internet de las cosas donde objetos comunes pueden conectarse a Internet.

El Internet de las cosas facilita tareas diarias y mejora la productividad de las empresas.

El internet de las cosas utiliza las redes inalámbricas de baja potencia, pero se hace necesaria la utilización de nuevos protocolos para su implementación.

Los protocolos que destacan en la implementación de redes inalámbricas son TCP/IP, ZigBee, Z-Eave y 6loWpan.

Los sistemas de Internet de las cosas suelen ser muy complejos y requieren soluciones de seguridad integrales que puedan distribuir capas de conectividad en la nube.

Los dispositivos de Internet de las cosas son recursos restringidos y no suelen tener el poder suficiente para admitir las soluciones de seguridad tradicionales.

La seguridad de IoT se podría definir como aquellas actividades encaminadas a la protección de los objetos y sus comunicaciones o interacciones con otros objetos y es un tema que no ha sido explotado y tratado en su totalidad.

No existe una guía absoluta a seguir para implementar la seguridad en el internet de las cosas.

Como uno de los resultados de este trabajo se presenta una recopilación de los criterios y pautas que se deben tener en cuenta para implementar sistemas seguros en el Internet de las Cosas.

Una de las principales ventajas de aplicar el protocolo 6LoWPAN frente a otro tipo de protocolos de comunicación inalámbrica, es el uso de direcciones IP, específicamente IPv6.

Entre los beneficios de 6LoWPAN se encuentran su fácil uso por ser un estándar abierto, confiable y estandarizado. Reduce el uso que cada dispositivo hace de la red comprimiendo los 42 bytes de tamaño de cabecera de una IPv6 normal a solo 6 bytes y modifica el servicio DHCP para que el consumo de los nodos sea el mínimo posible.

Una desventaja del protocolo es que los nodos de sensores tienen limitaciones en capacidad de procesamiento y se hizo necesario agregar una capa de adaptación que fragmenta y rearma los paquetes.

Respecto a la seguridad 6lowpan tiene implementado cifrado mediante AES-128 necesario para brindar seguridad a los datos transmitidos.

# RECOMENDACIONES

Al iniciar la implementación del Internet de las Cosas, se debe realizar un buen alcance ya que existen varios campos de interacción de la sensorización masiva y se puede perder el verdadero objetivo del proyecto.

La seguridad es fundamental para evitar el mal uso o robo de la información que transmiten estos dispositivos. Realizar estudios futuros sobre el desarrollo y avance de este particular en el Internet de las cosas.

Realizar estudios comparativos de los protocolos estudiados, analizando sus ventajas y desventajas según las áreas de aplicación: domótica, salud, ambiente, industrias, etc.

Analizar los avances en cuanto a la disminución de las limitaciones de capacidad y procesamiento de los sensores, según fabricantes.

# REFERENCIAS

Adam Dunkels, O. S. (2005). *Using protothreads for sensor node.* In Proceedings of the REALWSN.

Amaral, M. S. (01 de 11 de 2011). *ISA.* Obtenido de ISA: https://www.isa.org/uploadedImages/Content/Standards_and_Publications/ISA_Publications/InTech_Magazine/2012/December/1---Fig1_ISA100_ARCH_eng.jpg

Andreu, J. (2011). *Gestión de servicios de correo electrónico (Servicios en red).* Editex.

Andreu, J. (2011). *Instalación de equipos de red: Configuración (Redes locales).* Editex.

Ávila, A. R. (2010). *Iniciación a la Red de Internet.* Ideaspropias Editorial S.L.

Bestuzhev, D. (11 de 06 de 2012). *kaspersky.* Obtenido de http://latam.kaspersky.com/mx/LatAmQ3malware2012

Cabello, A. L. (2015). *Implantación de aplicaciones web en entornos internet, intranet y extranet.* Malaga: IC Editorial.

Cabrera, C. (Marzo de 2016). *cesarcabrera.info*. Obtenido de http://cesarcabrera.info/blog/subneteo-en-ipv6/

Castillo, H. (2016).

Castro, A. M., Díaz, O. G., Alzórriz, A. I., & Ruiz, S. E. (2014). *Procesos y Herramientas para la Seguridad de Redes.* Madrid: Editorial UNED.

Chiles, D. (2014). *Guía de Usuarios de Internet: Navegación Segura y Exitosa.* Estados Unidos: Google Play Edición.

CNET. (s.f.). *Chinese hackers take command of Tesla Model S.* Obtenido de http://www.cnet.com/news/chinese-hackers-take-command-of-tesla-model-s/

Concejero, J. B., Mondejar, J. B., Romero, O. R., & Ternero, M. D. (2014). *Redes locales.* Ediciones Paraninfo, S.A.

Corazza, F. (s.f.). *http://www.slideshare.* Obtenido de http://www.slideshare.: http://www.slideshare.

Corletti, A. E. (2011). *Seguridad por niveles.* Madrid: DarFE Learning Consulting S.L.

CSIRT. (2007). Seguridad en Internet de las cosas. *Estado del arte*, 20-42. 48.

Desongles, J. C. (2006). *Técnicos de Informática Del Servicio Vasco de Salud-osakidetza.* Sevilla: MAD-Eduforma.

Dosideas. (13 de 11 de 2008). *http://www.dosideas.com/.* Obtenido de http://www.dosideas.com/: http://www.dosideas.com/images/stories/java/rest-servicio-web-stateless.png

Enrique Alba. (2014). *http://neo.lcc.uma.es/*. (NEO, Productor) Obtenido de http://neo.lcc.uma.es/: http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/http.html

ESET Security Report. (14 de 06 de 2014). *Eset-la.* Obtenido de http://www.eset-la.com/centro-prensa/articulo/2014/empresas-america-latina-sufrio-ataques-malware-ultimo-a%C3%B1o/3517

Evans, D. (2011). Internet de las cosas, Cómo la próxima evolución. *Cisco Internet Business Solutions Group (IBSG)*, 1-12.

Freire, J. (03 de Octubre de 2015). *Doctortecno.* Obtenido de http://www.doctortecno.com/noticia/ecuador-cuarto-pais-region-que-recibe-mas-ataques-ciberneticos

García, D. G. (2015). *Estudio de 6loWPAN para su aplicación a Internet de las Cosas.* La Laguna: Universidad de La Laguna.

Glen M. (2012). *https://sx-de-tx.wikispaces.com/ZIGBEE.*

Huembes, C. A. (2008). *TAF.* Argentina.

Hurtado, F. A., Velez, R. E., & Rios, J. A. (2008). *Sistema de gestión integral. Una sola gestión, un solo equipo.* Colombia: Universidad de Antioquia.

Liabspain, (2014). I Estudio anual de coches conectados. 2-3. kb.esds.co.in. (s.f.). *http://kb.esds.co.in/wp-content/uploads/2013/11/IPv6-total-address-blog2.jpg*.

Kovatsch, M. (s.f.). *Californium (Cf) CoAP framework in Java.*

Lombardero, L. (2015). *Trabajar en la era digital: Tecnología y competencias para la transformación digital.* Madrid: LID Editorial.

Matthias Kovatsch, S. D. (2011). A low-power coap for contiki. *In Proceedings of the 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems.* Valencia: MASS.

McAneney, C. (2015). *La Seguridad en Internet (Online Safety).* New York: The Rosen Publishing Group. 49

Mieres, J (2009). Ataques informáticos Debilidades de seguridad comúnmente explotadas. Obtenido de http://ec.europa.eu/index_es.htm

Simal, T. (2011). MONOGRÁFICO: Redes Wifi - Seguridad en redes Wi-Fin Obtenido de http://recursostic.educacion.es/observatorio/web/en/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi?start=7

Tenealive. (s.f). Zwave. http://www.tenealive.com/zwave

Zwave. (s.f). Acerca de Z-Wave**.** http://www.z-wave.com/