SOLUCIÓN TECNOLÓGICA DE INTERNET DE LAS COSAS APLICADO A SMART HOMES SEGURAS

JULIAN CAMILO MORALES SOLANO

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA – UNAB
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
GRUPO DE INVESTIGACIÓN EN TECNOLOGÍAS DE INFORMACIÓN - GTI
LÍNEA DE INVESTIGACIÓN EN TELEMÁTICA
BUCARAMANGA, 31 DE OCTUBRE DE 2016

SOLUCIÓN TECNOLÓGICA DE INTERNET DE LAS COSAS APLICADO A SMART HOMES SEGURAS

JULIAN CAMILO MORALES SOLANO

Director:
Diana Teresa Parra Sánchez
Co-Director:
César D. Guerrero

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA – UNAB
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
GRUPO DE INVESTIGACIÓN EN TECNOLOGÍAS DE INFORMACIÓN - GTI
LÍNEA DE INVESTIGACIÓN EN TELEMÁTICA
BUCARAMANGA, 31 DE OCTUBRE DE 2016

Nota de aceptación

Aprobado por el Jurado de Trabajo de Grado en cumplimiento de los requisitos exigidos por la Universidad Autónoma de Bucaramanga para optar por el título de Ingeniero de Sistemas

Diana Teresa Parra Sánchez

Directora

Cesar D. Guerrero

Co-Director

x

Jurado

x

Jurado

x

Jurado

Bucaramanga, 31 de Octubre de 2016

A Dios.

A mis padres.

A esa persona que siempre estuvo presente.

AGRADECIMIENTOS

A la profesora Diana Teresa Parra Sánchez, la tutora de este proyecto de investigación, por su conocimiento, su dedicación, su paciencia y su apoyo en el proyecto.

A los miembros del Grupo De Investigación En Tecnologías De Información por los aportes realizados para la culminación del proyecto.

A mis padres por sus buenos deseos, por su confianza y por el apoyo incondicional.

A esa persona espeial, por su apoyo, su amor y su compañía.

TABLA DE CONTENIDO

INTRODUCCIÓN 11
1. OBJETIVOS 17
1.1. OBJETIVO GENERAL 17
1.2. OBJETIVOS ESPECIFICOS 17
2. ESTADO DEL ARTE 18
2.1. REVISIÓN SISTEMÁTICA DE LA LITERATURA 18
2.2. SMART HOMES EN EL MUNDO 20
2.3 SEGURIDAD EN SMART HOMES, INNOVACIÓN EN COLOMBIA 26
2.4 SOLUCIONES EXISTENTES EN EL MERCADO PARA SEGURIDAD EN IOT 29
3. MARCO REFERENCIAL 33
3.1. MARCO CONCEPTUAL 33
3.2. MARCO TEÓRICO 33
3.3. MARCO LEGAL 49
4. DISEÑO METODOLÓGICO 52
5. RESULTADOS 54
5.1. ESTADO DEL ARTE 54
5.2. TECNOLOGÍAS Y PROTOCOLOS PARA LA IMPLEMENTACIÓN DE SMART HOMES SEGURAS 54
5.3. ELEMENTOS HARDWARE Y SOFTWARE REQUERIDOS PARA EL DESPLIEGUE DE SMART HOMES SEGURAS EN COLOMBIA 62
5.4. DISEÑO DE UN ESCENEARIO SEGURO DE SMART HOMES BASADO EN LAS TECNOLOGIAS, PROTOCOLOS Y ELEMENTOS HARDWARE Y SOFTWARE SELECCIONADOS 69
Como Mantener un Smart Home Seguro 82
6. CONCLUSIONES 84
7. TRABAJO FUTURO 86
Referencias 87

LISTA DE FIGURAS

Figura 1.Dispositivos conectados a la red.....12
Figura 2. Número total de documentos por año 18
Figura 3. Numero de documentos por país.....19
Figura 4. Numero de documentos por tipo.....19
Figura 5. Numero de documentos por área de estudio. 20
Figura 6. Seguridad cifrada frente a diferentes ataques.....28
Figura 7. Solución SYMANTEC 31
Figura 8. Framework MOCANA 32
Figura 9. Modelo Capas IoT.....38
Figura 10.Suscriptores por segmento 40
Figura 11. Suscriptores por Departamento 41
Figura 12. Clasificación de Industrias 43
Figura 13. Interacción dispositivos IoT.....44
Figura 14. Host Kalilinux.....46
Figura 15. Seteo Payload.....47
Figura 16. Shikata Ga Nai 47
Figura 17. MsfConsole 48
Figura 18. MsfConsole 49
Figura 19.Diseño Metodológico.....52
Figura 20. Como funciona TLS 55
Figura 21. Sensores Smart Home.....56
Figura 22 Seguridad certificado 58
Figura 23. Transmisión segura IPv6 59
Figura 24. Etiqueta RFID.....59
Figura 25 Como funciona el protocolo SSH.....60
Figura 26 Como funciona ZigBee?.....61
Figura 27. Algoritmo Hash.....63
Figura 28. Vulnerabilidades Sensores 69
Figura 29. Interfaz Home I/O simulation.....70
Figura 30. Plano Escenario Smart Home (Piso1) 72
Figura 31. Escenario Smart Homes (Piso2).....72
Figura 32. Vista exterior Smart Home.....73
Figura 33. Habitación Secundaria.....75
Figura 34. Estudio 76
Figura 35. Sala Principal 78
Figura 36. Cocina 79
Figura 37. Garaje.....80
Figura 38. Seguro Principal.....81
Figura 39. Control desde el Smartphone 82

LISTA DE TABLAS

Tabla 1. Síntesis estado del arte 20
Tabla 2. Documentos según categoría.....24
Tabla 3 Área software, Firmware, Sistema Operativo y Aplicaciones.....45
Tabla 4.Area Memoria, Información y BD.....45
Tabla 5 Área Red.....45
Tabla 6 Area Actualización Software.....45
Tabla 7 Area método de autentificación 45
Tabla 8 Area Hardware.....46
Tabla 9 Area usuarios.....46
Tabla 10. Caracteristicas Dispositivos.....63
Tabla 11 Características TCG Versión 1.2 64
Tabla 12. Caracteristicas CryptoRF.....65
Tabla 13. Sensores Basicos Smart Homes 66
Tabla 14. Requerimientos Home I/O 70
Tabla 15. Requerimientos Smart Home Seguro.....71
Tabla 16. Tabla Sensores y dispositivos habitación Principal 74
Tabla 17. Tabla Sensores y dispositivos habitación Principal 75
Tabla 18. Tabla sensores y dispositivos estudio 76
Tabla 19. Sensores y dispositivos Sala Principal 77
Tabla 20. Sensores y dispositivos cocina.....79
Tabla 21. Sensores y dispositivos garaje 79
Tabla 22. Sensores y dispositivos seguros.....80
Tabla 23. Presupuesto Implementación Smart Home(Modelo) 81

SIGLAS Y ACRONIMOS

IoT: *Internet of Things.*

AUPS: *Authenticated Publish & Subscribe.*

DTLS: *Datagram Transport Layer Security.*

TLS: *Transport Layer Security.*

SSL: *Secure Sockets Layer.*

CoAP: *Constrained Application Protocol.*

RFID: *Radio Frequency Identification.*

MQTT: *Message Queue Telemetry Transport.*

FPGA: *Field Programmable Gate Array.*

ITU: Unión Internacional de Telecomunicaciones.

NFC: *Near field communication.*

TIC: Tecnologías de la información y la comunicación.

IBSG: *Internet Business Solutions Group.*

ECC: *Elliptic Curve Cryptography.*

P2P: *peer-to-peer.*

M2M: *machine-to-machine.*

IoE: *Internet of Everything.*

AES: *Advanced Encryption Standard.*

CCCE: Cámara Colombiana de Comercio Electrónico.

DANE: Departamento Administrativo Nacional de Estadística.

MINTIC: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

IP: *Internet Protocol.*

IPv4: *Internet Protocol versión 4*

IPv6: *Internet Protoco versión 6*

Ipsec: *Internet Protocol security*

BD: Base de datos

SSH: *secure Shell*

SHA: *secure hash authentication*

SO: Sistema operativo

WPAN: *wireless personal area network*

SOLUCIÓN TECNOLÓGICA DE INTERNET DE LAS COSAS APLICADO A SMART HOMES SEGURAS

Julián Camilo Morales Solano
Diana Teresa Parra Sánchez, Director
César D. Guerrero, Co-Director

RESUMEN

Internet de las Cosas ya es una realidad permitiendo ofrecer servicios avanzados de interconexión entre objetos, las Smart Homes le brindaran al usuario un estilo de vida más confortable, donde pueda automatizar todo su hogar y lo puedo controlar directamente desde su Smartphone, pero la innovación tecnológica trae consigo que cada día existan más vulnerabilidades y agujeros de seguridad que puedan ser explotados por terceros o atacantes maliciosos que puedan hacer un uso inapropiado de esta información exponiendo al usuario final a riesgos que podrían traer grandes consecuencias.

Con base en esto, se ha planteado un desarrollo de un proyecto de investigación que permita la elaboración de un escenario seguro de Internet de las Cosas basado en tecnologías, protocolos, requerimientos de tipo Software y Hardware que garanticen al usuario final una Smart Home segura.

Palabras clave – IoT, IoT Security, Seguridad, Privacidad, Smart Homes.

INTRODUCCIÓN

El Proyecto de Trabajo de Grado titulado “Solución Tecnológica de Internet de las Cosas aplicado a Smart Homes seguras”, es un proyecto de investigación desarrollado desde las actividades investigativas del Semillero de Investigación en Telemática (SINET) en la línea de investigación en Telemática, adscrito al Grupo de Investigación en Tecnologías de Información (GTI). El proyecto está articulado con las actividades investigativas llevadas a cabo en el Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT).

El Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT) es una alianza entre universidades, líderes tecnológicos mundiales y empresas ancla para potenciar el crecimiento económico del país desde el desarrollo tecnológico y la innovación a través del despliegue de soluciones tecnológicas en Internet de las Cosas, buscando resolver las necesidades de diferentes sectores productivos del país. El CEA-IoT es una iniciativa impulsada desde el Ministerio de las TIC, con el apoyo de Colciencias, y corresponde a una estrategia que busca posicionar a Colombia como líder regional en TIC. El Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT) es una alianza entre universidades, líderes tecnológicos mundiales y empresas ancla para potenciar el desarrollo económico del país desde el desarrollo tecnológico y la innovación a través de las tecnologías del Internet de las Cosas, buscando resolver las necesidades de diferentes sectores productivos del país. El CEA-IoT es una iniciativa impulsada desde el Ministerio de las TIC, con el apoyo de Colciencias, y corresponde a una estrategia que busca posicionar a Colombia como líder regional en TIC (Tomado de la Página http://www.cea-iot.org/).

La Universidad Autónoma de Bucaramanga[1] es una de las Universidades participantes en el CEA-IoT, que cuenta con la representación del Profesor César D. Guerrero como coordinador del Comité de Divulgación. Así mismo, están vinculados al CEA-IoT en representación de la UNAB tres investigadores planta, siete estudiantes de maestría y un investigador en Post-Doctorado; quienes están vinculados en las líneas del trabajo del CEA-IoT, a saber: (i) Salud; (ii) Logística; (iii) Industria; (iv) Vestibles; (v) Seguridad; (vi) Agroindustria y Medio Ambiente y; (vii) Gobierno.

Con el desarrollo del presente proyecto de investigación “Solución Tecnológica de Internet de las Cosas aplicado a Smart Homes seguras” se quieren presentar las posibles tecnologías y requerimientos tanto software como hardware para el diseño de un escenario seguro para Smart Homes. Este proyecto sirve como base para futuros proyectos de investigación que encuentren interés en el tema de IoT seguro aplicado a Smart Homes favoreciendo su ágil despliegue a nivel nacional e internacional.

[1] La Universidad Autónoma de Bucaramanga es una institución académica de orden privado del departamento de Santander. Cuenta con acreditación institucional de alta calidad por parte del Consejo Nacional de Acreditación a partir de diciembre de 2012 por un periodo de cuatro años.

Problema de investigación

Internet de las Cosas (por sus siglas en Inglés, *Internet of Things – IoT*) es una realidad en el mundo actual. Internet de las Cosas (a veces denominado Internet de los Objetos), ha sido considerado como la evolución de Internet, debido a sus capacidades para reunir, analizar y distribuir datos; los cuales serán procesados para convertirse en información, conocimiento y sabiduría (Ver). Con miras al futuro, Cisco IBSG prevé que habrá 25 mil millones de dispositivos conectados a Internet para 2015, y 50 mil millones para 2020. (Cisco, 2011).

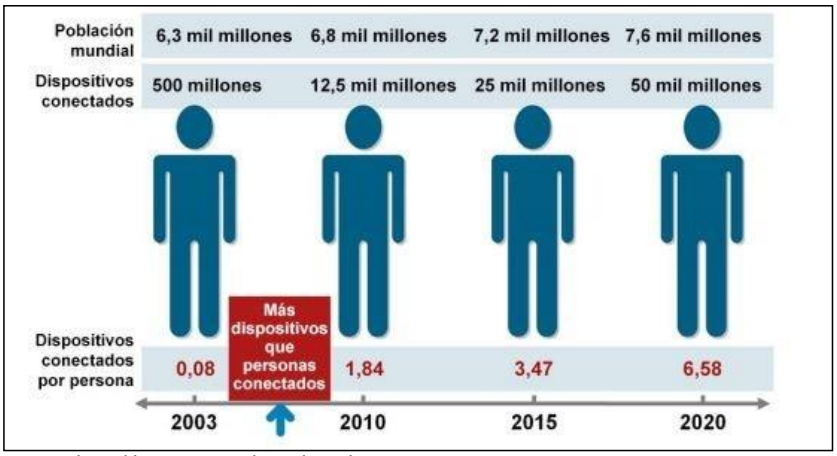

Figura 1.Dispositivos conectados a la red
Fuente: (Cisco, 2011)

Para el desarrollo del proyecto, se ha identificado un problema enfocado a la seguridad y la privacidad de los datos en IoT, donde se busca darle al usuario la confiabilidad de que todos los datos e información que este viajando a través de soluciones tecnológicas IoT van de manera segura, garantizando así que dicha información no tendrá acceso de terceros y que esta información no será modificada ni extraída por parte de un atacante.

Los diferentes dispositivos móviles y equipos requeridos para IoT, presentan vulnerabilidades que requieren ser atendidas por parte de fabricantes y miembros de los equipos encargados de llevar a cabo el despliegue tecnológico de IoT. En este sentido es importante destacar la necesidad de contar con normatividad en Colombia relacionada con seguridad en dispositivos IoT.

El Internet de las Cosas, brindará al usuario un estilo de vida más confortable. Ejemplo de ello, son las *Smart Homes* ya que facilitan la vida del usuario al brindarle la capacidad de controlar, por ejemplo, las puertas, los seguros, las luces, la temperatura del hogar y demás electrométricos mediante el uso de una solución tecnológica en Internet de las Cosas.

A nivel de soluciones tecnológicas basadas en Internet de las Cosas, existe especial preocupación en aspectos relacionados con seguridad informática y seguridad de la información. La seguridad de los datos está cada vez más

expuesta a terceros. Al respecto, la Comisión Europea y Estados Unidos han discutido las consecuencias que la privacidad y seguridad ocasiona en la conectividad de las “cosas” (IoT simple, 2015).

En cuanto al despliegue de IoT, existen desafíos relacionados directamente con aspectos de seguridad para la protección de la información de los usuarios[2]. Los ciberdelicuentes se enfocan en “blancos de ataque” tales como el robo de información confidencial los cuales pueden exponer la privacidad del usuario, y afectar a los fabricantes de los dispositivos para IoT. Cabe resaltar que en el despliegue de esta tecnología en Colombia se deben definir ciertas políticas de seguridad acerca de la información que se estará compartiendo y de qué forma será utilizada.

Uno de los escenarios de IoT que requiere la implementación de políticas de seguridad, son las *Smart Homes.* Este escenario en particular se caracteriza por brindar al usuario confort mediante la optimización de tareas a través del uso de un Smartphone o Tablet, que se comunican con objetos del hogar. En estos contextos, los delincuentes pueden aprovechar ciertas vulnerabilidades que actualmente tienen los electrodomésticos listos para IoT tanto a nivel de software, como a nivel de hardware ya que ellos pueden llegar a tener acceso remoto tomando el control de estos dispositivos.

Tomando en consideración toda la información que estará compartiendo el usuario de la solución tecnológica IoT a través de la red, la mejor manera de proteger los datos es mediante una arquitectura segura utilizando las tecnologías y protocolos apropiados para así evitar la pérdida de información sensible o modificación de esta. Actualmente la mayoría de esos dispositivos fallan en aspectos como la autenticación insuficiente e incluso inexistente; puntos débiles en la conexión y transferencia de datos a través de Internet y vulnerabilidades de hardware o software que los hacen susceptibles de sucumbir ante ataques potenciales. (Symantec, 2015).

Frente a los avances tecnológicos existentes actualmente en IoT, teniendo en cuenta las vulnerabilidades existentes a nivel hardware como a nivel software, se plantea la siguiente pregunta problema de investigación: ¿De qué manera es posible diseñar una solución tecnológica de IoT seguro aplicado al escenario de Smart Homes?

Los expertos afirman que en pocos años absolutamente todo estará conectado a Internet, por esto es importante que el gobierno colombiano esté preparado para llevar a cabo tareas relacionadas con aspectos propios de Internet de las Cosas, ligados con ciberseguridad.

¿Qué importancia tendrá la regulación en IoT para Colombia?

---

[2] Coincidiendo con la presentación de un informe de Ciberseguridad para IoT liderado por Telefónica, Chema Alonso, CEO de *ElevenPaths*, ha destacado la necesidad de que los fabricantes de dispositivos y sensores de este nuevo ecosistema implanten la seguridad desde la fase inicial de su diseño.

IoT tiene implica una arquitectura compleja cuyo desarrollo resultará de la interacción de dos áreas complementarias, como lo son el desarrollo tecnológico del mercado y la regulación, por esto IoT necesita de una visión integral para que se pueda dar una apropiada regulación enfocándose profundamente en la seguridad y privacidad de los datos como lo propone la siguiente frase.

"Las consideraciones clave de las políticas públicas deben ser hechas para la soberanía y privacidad de la información y para la seguridad." (Castonguay, 2016).

Propósito, enfoque y tareas

Este trabajo de grado, pretende formular una posible solución a las vulnerabilidades de IoT en Smart Homes. Se espera obtener una arquitectura segura basándose en los elementos de tipo software y hardware requeridos, también teniendo en cuenta las diferentes tecnologías y protocolos pertinentes que lleven a un diseño apropiado para un escenario seguro de IoT aplicado a Smart Homes.

Las tareas que serán realizadas para el desarrollo de un escenario seguro de Smart Homes, son las siguientes:

- Se elaborará un estado del arte sobre Smart Homes a nivel mundial.
- Se definirá las tecnologías y protocolos requeridos para la implementación de Smart Homes seguras.
- Se definirá los elementos hardware y software requeridos para el despliegue de Smart Homes seguras en Colombia.
- Se diseñará un escenario seguro de Smart Homes basado en las tecnologías, protocolos y elementos hardware y software seleccionados.

Para la apropiada solución de seguridad de IoT en Smart Homes, es indispensable conocer las diferentes vulnerabilidades y fallos de seguridad actuales en IoT, también se debe conocer sobre las soluciones actuales de seguridad ofrecidas en diferentes países.

Con el diseño de un escenario seguro de Smart Homes en Colombia, se brinda una posible solución a los problemas de seguridad en IoT, garantizándole al usuario la privacidad e integridad de la información en las Smart Homes.

Aportaciones de la tesis

IoT está evolucionando ágilmente en las Smart Homes debido a esto las amenazas y riesgos en la red evolucionan del mismo modo, con el objetivo de atacar este nuevo campo actualmente muy vulnerable debido a la falta de regulación en Colombia.

La rama IoT incluye la conectividad de diferentes tipos de dispositivos como sensores, seguros eléctricos, temperatura, cámaras de vigilancia y diferentes dispositivos electrónicos que trabajen bajo la misma red, la amplia variedad de dispositivos implica que existan día a día más vulnerabilidades.

Teniendo en cuenta lo anterior, el proyecto de grado brindará una solución de IoT segura e integral que permita garantizar al usuario que su información no tendrá acceso de terceros, debido a que esto podría afectar de manera importante el correcto funcionamiento de una Smart Home.

Otro plus que tiene la solución de IoT Segura será la protección de los datos y la disponibilidad de estos teniendo la seguridad de que esta información es auténtica y confiable.

Se tendrá en cuenta diferentes factores tales como la seguridad de los dispositivos a nivel hardware, y software, certificados de seguridad (autentificación) y diferentes análisis de seguridad.

Esta investigación consta de nueve capítulos, los cuales son presentados como sigue:

Capítulo 1: Planteamiento del Problema y Justificación
Se habla sobre el problema por el cual se está realizando el trabajo de investigación, sus implicaciones y la manera en la que se ve afectado el usuario final de IoT frente a los riesgos y vulnerabilidades a los cuales se ve expuesto en el despliegue de IoT.

Capítulo 2: Objetivos
Se proponen las metas a alcanzar mediante el diseño metodológico definido para el proyecto de grado teniendo en cuenta que los objetivos aportaran para el diseño final del escenario seguro de Smart Homes para IoT.

Capítulo 3: Estado del arte
Se recopilaron investigaciones relevantes en base al caso de estudio teniendo en cuenta los aportes que brindaban al proyecto de grado (tecnologías, seguridad a nivel software, seguridad a nivel hardware) y también se tuvo en cuenta las siguientes keywords (i) Smart Homes, (ii) Security y, (iii) IoT.

Capítulo 4: Marco Referencial
Este capítulo se encuentra divido en las siguientes subsecciones: (i) Marco conceptual: Se ubican los conceptos fundamentales del proyecto; (ii) Marco teórico: (iii) Marco legal: presenta las Leyes y documentos que contienen normas en Ciencia, Tecnología e Innovación en Colombia y el Mundo.

Capítulo 5: Diseño Metodológico
Se definen las actividades que permitirán dar cumplimiento a cada uno de los objetivos propuestos en el caso de estudio.

Capítulo 6: Resultados Obtenidos
Se presentan los resultados que se obtienen a partir de los objetivos propuestos en el trabajo tales como las tecnologías, los elementos de tipo hardware y software para el correcto despliegue del escenario de Smart Home seguro.

Capítulo 7: Discusión
Se presentan los hallazgos y dificultades que se presentaron a lo largo de la elaboración del proyecto de grado “Solución tecnológica de IoT aplicado a Smart Homes seguras.

Capítulo 8: Conclusiones
Se dan a conocer las conclusiones derivadas del proyecto donde basadas en la revisión de la literatura cuales son las tecnologías, requerimientos de tipo software y hardware adecuados para el correcto despliegue de un escenario de IoT seguro.

Capítulo 9: Trabajo Futuro
Este capítulo está dedicado a la posible investigación futura del proyectó.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Diseñar una solución tecnológica de IoT segura para el escenario de Smart Homes.

1.2. OBJETIVOS ESPECIFICOS

- Elaborar un estado del arte sobre Smart Homes a nivel mundial.
- Definir las tecnologías y protocolos requeridos para la implementación de Smart Homes seguras.
- Definir los elementos hardware y software requeridos para el despliegue de Smart Homes seguras en Colombia.
- Diseñar un escenario seguro de Smart Homes basado en las tecnologías, protocolos y elementos hardware y software seleccionados.

2. ESTADO DEL ARTE

Smart Homes, es un escenario de IoT que requiere la implementación de políticas de seguridad para la protección de la información de los usuarios. El desarrollo del estado del arte de la investigación, implicó el uso de palabras clave que permitieran la obtención de documentos que trataran los temas de Smart Homes, Internet of Things y seguridad.

2.1. REVISIÓN SISTEMÁTICA DE LA LITERATURA

Para el desarrollo de la revisión sistemática de la literatura, se definieron las siguientes palabras clave: (i) Smart Homes, (ii) Secure IoT y (iii) IoT. Los términos definidos fueron utilizados para realizar una búsqueda en la Base de Datos Académica Scopus.

El algoritmo de búsqueda utilizado para el desarrollo de la revisión sistemática de la literatura, se presenta como sigue:

TITLE-ABS-KEY (Smart homes; Secure IoT; IoT) AND PUBYEAR > 2011

Documentos recuperados: 200
Fecha de búsqueda: 17 de octubre de 2016
Rango de años de búsqueda: 2012 – 2016
Base de Datos Académica: Scopus

Entre los resultados obtenidos, se tiene lo siguiente:

El año 2016, ha sido el año con mayor número de publicaciones (69 en total). (Ver Figura 2).

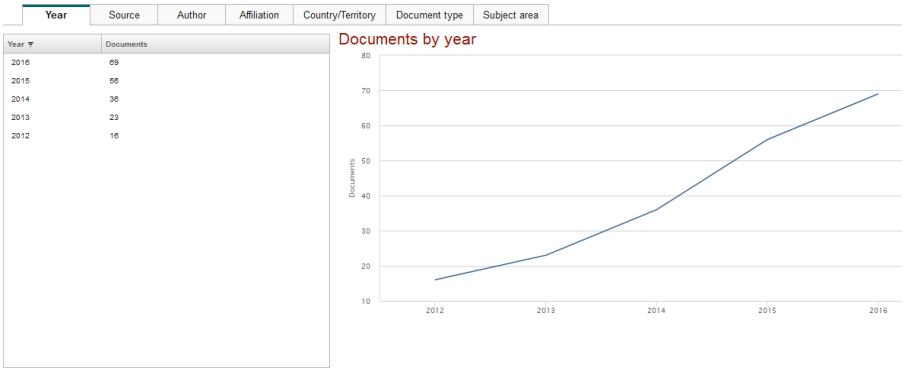

Figura 2. Número total de documentos por año
Fuente: Base de datos Scopus

Los países que lideran el tema de investigación son Estados Unidos (27 documentos publicados), India (24 documentos publicados) e China (22 documentos publicados). Ver Figura 3.

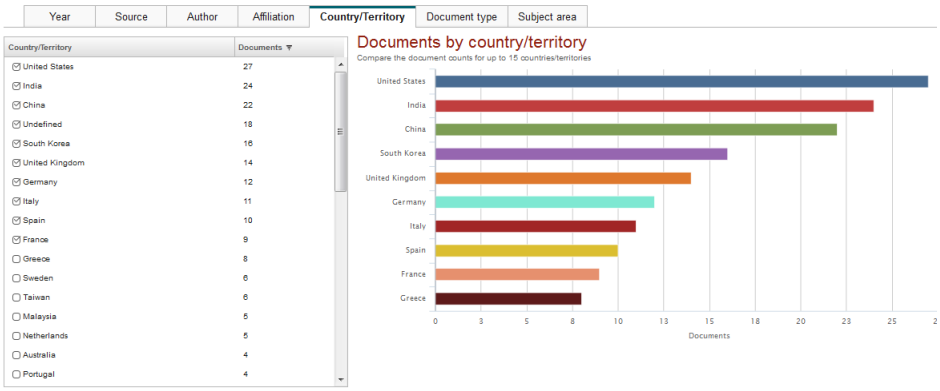

Figura 3. Numero de documentos por país
Fuente: Base de datos Scopus

El tipo de documentos publicados son artículos de conferencia (135 documentos), artículos (39 documentos) y reviews (4 documentos) entre otros. (Ver Figura 4.)

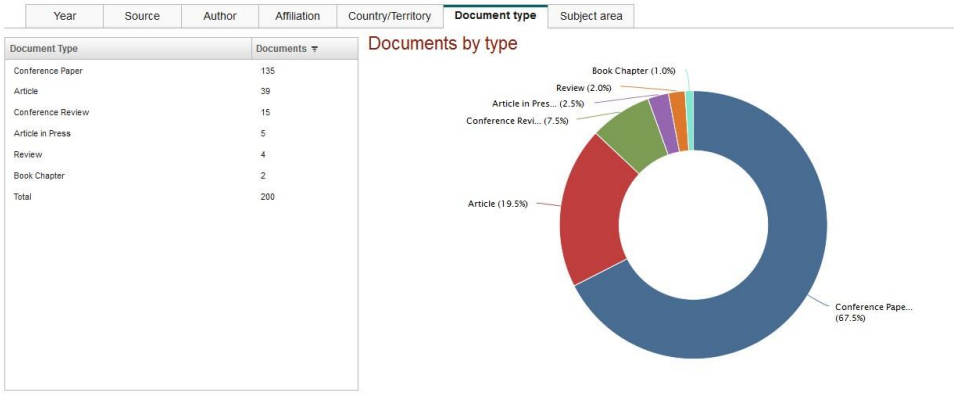

Figura 4. Numero de documentos por tipo.
Fuente: Base de datos Scopus

Las áreas de estudio con mayor cantidad de publicaciones son Ciencias de la Computación (171 documentos), Ingeniería (67 documentos) y, Matemáticas (22 documentos). Ver Figura 5.

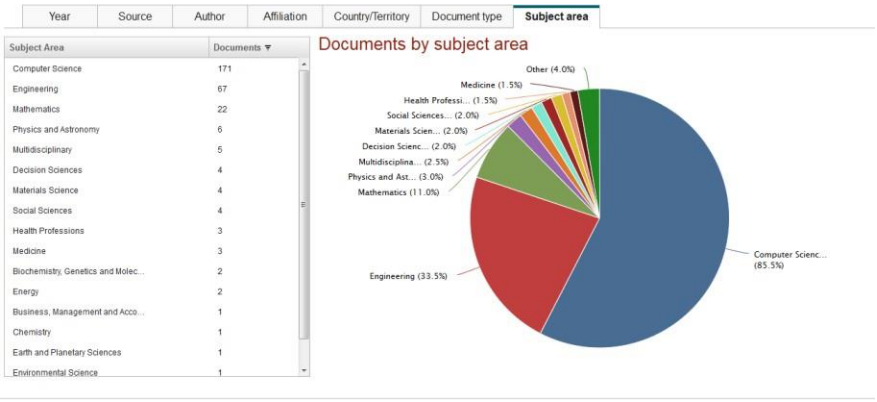

Figura 5. Numero de documentos por área de estudio.
Fuente: Base de datos Scopus

2.2. SMART HOMES EN EL MUNDO

En la **¡Error! No se encuentra el origen de la referencia.**, es presentada la síntesis d el estado del arte. En total se recuperaron 18 referencias que tratan temas relacionados con IoT y seguridad en Smart Homes. Se ha tenido en cuenta la presentación de la cantidad de citaciones obtenidas por el artículo al momento de efectuar la consulta.

Tabla 1. Síntesis estado del arte

Autor	Título	Fuente	Universidad País	Tipo Keywords	Citaciones
Rizzardi, A., Sicari, S., Miorandi, D., Coen-Porisini, A. (2016)art	AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things	Source of the Document Information Systems 62, pp. 29-41	Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria, via Mazzini 5, Varese, Italy	Internet of Things; Middleware ; MQTT; Prototype; Publish & Subscribe; Security	1
Shen, H., Shen, J., Khan, M.K., Lee, J.-H. (2016)art	Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things	Wireless Personal Communications pp. 1-14	School of Mathematics and Statistics, Wuhan University, Wuhan, China	Internet of things; Performance; RFID; Security	0

Autor	Título	Fuente	Universidad País	Tipo Keywords	Citaciones
Antonov, A.P., Filippov, A.S., Mamoutova, O.V. (2016)art	Next generation FPGA-based platform for network security	Conference of Open Innovation Association, FRUCT 2016-September, 7561501, pp. 9-14	Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russian Federation	Hardware architecture; Internet of Things (IOT)	1
Marktscheffel, T., Gottschlich, W., Popp, W., (...), Bilzhause, A., De Meer, H. (2016) art	QR code based mutual authentication protocol for Internet of Things	WoWMoM 2016 - 17th International Symposium on a World of Authentication; Internet of Things; Key Exchange; QR code; Usable SecurityWireless, Mobile and Multimedia Networks 7523562	Institute of IT-Security and Security Law (ISL), University of Passau, Germany	Authentication; Internet of Things; Key Exchange; QR code; Usable Security	1
Koley, S., Ghosal, P. (2016) art	Addressing hardware security challenges in internet of things: Recent trends and possible solutions	Proceedings - 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing	Department of Information Technology, Indian Institute of Engineering Science and Technology, Shibpur, Howrah, WB, India	Hardware Trojan; Internet of Things; Privacy; Security	1
(Urien, 2016)	Innovative DTLS/TLS security modules embedded in SIM cards for IoT trusted and secure services	2016 13th IEEE Annual Consumer Communications and Networking Conference, CCNC 2016 7444778, pp. 276-277	Telecom ParisTech, 23 avenue d'Italie, Paris, France	HCE; IoT; NFC; RACS; Security; TLS	1
Abdul Rahman, A.F., Daud, M., Mohamad, M.Z. (2016) conf	Securing sensor to cloud ecosystem using Internet of Things (IoT) security framework	ACM International Conference Proceeding Series 22-23-March-2016, a79	National Vulnerability Assessment Centre, (MyVAC), CyberSecurity Malaysia,	Framework; Information Security; Internet of Things (IoT); IoT Ecosystem;	1

Autor	Título	Fuente	Universidad País	Tipo Keywords	Citaciones
			Selangor, Malaysia	Security Threats	
Lessa Dos Santos, G., Guimaraes, V.T., Da Cunha Rodrigues, G., Granville, L.Z., Tarouco, L.M.R. 2016 conf pape	DTLS-based security architecture for the Internet of Things	Proceedings - IEEE Symposium on Computers and Communications 2016-February, 7405613, pp. 809-815	Institute of Informatics, Federal University of Rio Grande Do sul (UFRGS), Porto Alegre - RS, Brazil	CoAP; DTLS; handshaking delegation; Internet of Things; mutual authentication	2
Lesjak, C., Hein, D., Winter, J. 2016 conf pape	Hardware-security technologies for industrial IoT: TrustZone and security controller	IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society 7392493, pp. 2589-2595	Design Center Graz, Infineon Technologies Austria AG, Graz, Austria	IoT, Authentification System	0
Kwon, H., Park, J., Kang, N. (2016) conf pap	Challenges in deploying CoAP over DTLS in resource constrained environments	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9503, pp. 269-280	Digital Media Department, Duksung Women's University, Seoul, South Korea	Cooja simulator; DTLS; Energy consumption; Handshake; Internet of things	1
Singh, M., Rajan, M.A., Shivraj, V.L., Balamuralidhar, P.(2015) conf	Secure MQTT for Internet of Things (IoT)	Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015 7280018, pp. 746-751	TCS Innovation Labs, Bangalore, India	Electronic Commerce; Free Movement; Legal Protection; Personal Information	1
Huang, J.-J., Juang, W.-S., Fan, C.-I. 2015	A secure and efficient smartphone payment scheme in IoT/Cloud environments	Proceedings - 2015 10th Asia Joint Conference on Information Security, AsiaJCIS 2015	Department of Computer Science and Engineering, National Sun Yat-Sen University,	IoT, Payment, Security	0

Autor	Título	Fuente	Universidad País	Tipo Keywords	Citaciones
		7153941, pp. 91-96	Kaohsiung, Taiwan		
(Urien, 2016)	LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things	2013 IEEE 10th Consumer Communications and Networking Conference, CCNC 2013 6488560, pp. 845-846	Telecom ParisTech, 23 avenue d'Italie, 75013, Paris, France	NFC; P2P; Secure Element; Security; SSL; TLS	6
Lee, B., Lee, J.-H. 2016	Blockchain-based secure firmware update for embedded devices in an Internet of Things environment	Journal of Supercomputing	Protocol Engineering Lab., Sangmyung University, Cheonan, South Korea	Blockchain; Embedded device; Firmware verification and update	1
Santoso, F.K., Vun, N.C.H. 2015	Securing IoT for smart home system	Proceedings of the International Symposium on Consumer Electronics, ISCE 2015-August, 7177843	School of Computer Engineering, Nanyang Technological University, Singapore, Singapore	authentication; IoT; smart home	2
Feng, L., Yao, X. 2016	RFID system mutual authentication protocols based on ECC	Proceedings - 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing	School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), Beijing, China	Authentication; ECC; RFID	1
Nadargi, A., Thirugnanam, M. 2016	Addressing identity and location privacy of things for Indoor—case study on internet of everything's (IoE)	Smart Innovation, Systems and Technologies 49, pp. 377-386	School of Computing Science and Engineering, VIT University, Vellore, Tamilnadu, India	Authentication; Authorization; Internet of everything's; Internet of things; Location privacy; Network enforced policy;	1

Autor	Título	Fuente	Universidad País	Tipo Keywords	Citaciones
				Secure analytics	
Vinayaga Sundaram, B., Ramnath, M., Prasanth, M., Varsha Sundaram, J. 2015	Encryption and hash based security in Internet of Things	2015 3rd International Conference on Signal Processing, Communication and Networking, ICSCN 2015 7219926	Department of Information Technology, Madras Institute of Technology, Anna University Chennai, India	Internet of Things; Security; Smart Homes; Wireless Sensor Networks	1
Fuente Elaboracion Propia					

En la Tabla 2, es presentada la síntesis del estado del arte donde cada uno de los documentos se dividió según su área de cubrimiento teniendo en cuenta los objetivos 2 y 3 del trabajo de investigación, los documentos se dividieron en las siguientes categorías:

- Tecnología
- Protocolos
- Software
- Hardware

Tabla 2. Documentos según categoría

Documento	Tecnología	Protocolos	Software	Hardware
Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things	X			
AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things	X			
Next generation FPGA-based platform for network security				X
QR code based mutual authentication protocol for Internet of Things	X	X		
Addressing hardware security challenges in internet of things: Recent trends and possible solutions				X
Innovative DTLS/TLS security modules embedded in SIM cards for IoT trusted and secure services		X		
Securing sensor to cloud ecosystem using Internet of Things (IoT) security framework	X			

DTLS-based security architecture for the Internet of Things		X		
Hardware-security technologies for industrial IoT: TrustZone and security controller				X
Challenges in deploying CoAP over DTLS in resource constrained environments		X		
Secure MQTT for Internet of Things (IoT)		X		
A secure and efficient smartphone payment scheme in IoT/Cloud environments	X	X		
LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things		X		
Blockchain-based secure firmware update for embedded devices in an Internet of Things environment			X	
Securing IoT for smart home system	X	X	X	X
RFID system mutual authentication protocols based on ECC	X			
Addressing identity and location privacy of things for Indoor—case study on internet of everything's (IoE)				X
Encryption and hash based security in Internet of Things	X	X		X
Fuente: Elaboración Propia				

La seguridad en Internet de las Cosas, es un factor determinante al momento de hacer el despliegue de una solución tecnológica, ya que la información es un recurso valioso. A nivel mundial, algunos investigadores afirman que las amenazas de seguridad y privacidad ante el despliegue de Internet de las Cosas, están aumentando considerablemente, y los sistemas actuales aún no están preparados para ofrecer opciones robustas a los usuarios. En este sentido, el uso compartido de información en la red, hace del Internet de las Cosas un ecosistema vulnerable.

Una de las mayores preocupaciones para el Internet de las cosas es que los usuarios y fabricantes no están teniendo en cuenta la seguridad de los dispositivos que se conectan, porque a pesar de tener protecciones integradas son susceptibles y vulnerables a atacantes por su poca implementación en protocolos y tecnologías que brinden seguridad a los dispositivos.

Desde el punto de vista del usuario, la situación es compleja, debido a que no son usuarios avanzados en el tema tecnológico, por ende, desconocen aspectos relacionados con seguridad informática, seguridad de la información, y técnicas para protegerse en caso de amenaza. Lo anterior implica, que se deben implementar estrategias de socialización por parte de los fabricantes y organizaciones dedicadas al despliegue de IoT, para que los usuarios del sistema

manejen buenas prácticas al momento de hacer uso de una solución tecnológica de Internet de las Cosas en sus hogares.

2.3 SEGURIDAD EN SMART HOMES, INNOVACIÓN EN COLOMBIA

El tema de seguridad enfocado a Smart Homes es un tema tendencia en el contexto colombiano, el cual está siendo objeto de estudio en grupos de investigación en telecomunicaciones y telemática, quienes han visto en este escenario una oportunidad que puede ser atendida desde la investigación básica y aplicada, y en el establecimiento de alianzas con actores estratégicos para la propuesta de soluciones tecnológicas de Smart Homes basadas en IoT.

Luego de una búsqueda rigurosa en fuentes primaria de información, se tiene que en el ámbito nacional no han sido publicados trabajos que hagan referencia a temas específicos como la implementación de protocolos y tecnologías que brinden seguridad en el escenario de Smart Homes, ni requerimientos de tipo software y hardware que permitan implementar dispositivos IoT seguros.

Haciendo referencia a Internet de las Cosas aplicado a escenarios de Smart Homes, y tomando el tema de seguridad informática y de la información como aspecto relevante al momento de implementar una solución tecnológica que brinde comodidades a los usuarios finales, se ha establecido el desarrollo de un Trabajo de Investigación orientado a formular una posible solución a las vulnerabilidades de IoT en Smart Homes. Se espera obtener una arquitectura segura basándose en los elementos de tipo software y hardware requeridos, también teniendo en cuenta las diferentes tecnologías y protocolos pertinentes que lleven a un diseño apropiado para un escenario seguro de IoT aplicado a Smart Homes.

La innovación tecnológica en Internet de las Cosas, es un tema de especial preocupación, debido a que la información de los usuarios del sistema queda expuesta, lo que implica retos asociados con normatividad en cuanto a delitos informáticos perpetrados en sistemas IoT; así como la presentación de orientaciones que ayuden a que usuarios no avanzados en el uso de los sistemas, y sin conocimientos en el tema, no queden expuestos, y tomen precauciones pertinentes.

Algunos autores en el mundo ante la preocupación de que los sistemas puedan ser vulnerados por atacantes, han dirigido sus investigaciones hacia el tema de seguridad y privacidad de la información. Por ende, algunos documentos recuperados presentan protocolos, tecnologías, software y hardware que pueden contribuir de manera importante en el Trabajo de Investigación.

El despliegue de IoT está permitiendo a los nuevos paradigmas de provisión de servicio, el uso de diferentes protocolos para la adopción y difusión de dispositivos IoT. Uno de los más utilizados es el MQTT, el cual es utilizado para la comunicación M2M (*machine to machine*) en IoT. Este protocolo permite la comunicación de sensores; se caracteriza por tener bajo consumo de banda ancha y, se puede utilizar

en una alta gama de dispositivos electrónicos que tengan bajos recursos tales como (almacenamiento, CPU, memoria RAM, entre otros) permitiendo así la comunicación con diferentes nodos de la Smart Home (es muy útil para lugares donde el ancho de banda y los requerimientos son muy escasos).

Mediante RFID (identificación por radiofrecuencia) se tiene como objetivo principal la transmisión de la identidad de un "objeto, es decir, el número único de identificación que este tendrá a través de ondas de radio que podría ser como una dirección MAC o de autentificación del dispositivo que brinda al usuario la "garantía" de que el dispositivo es auténtico.

Las etiquetas RFID son dispositivos pequeños muy parecidos a un "sticker" que pueden ser incorporadas al objeto, estas poseen antenas para garantizar la comunicación de envió y respuesta por radio frecuencia. En el artículo *"Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things"* se propone un Nuevo esquema de autentificación RFID utilizando criptografía de curva elíptica (ECC). ECC es uno de los métodos criptográficos más fuertes que requieren poco esfuerzo computacional, en cuanto a recursos ya que muchos de los dispositivos de las Smart Homes no contaran con los requerimientos suficientes para trabajar con métodos criptográficos que tengan altos requerimientos computacionales.

Entre otros documentos importantes en la búsqueda de la literatura se encuentra "*Next generation FPGA-based platform for network security*". El propósito de este documento es el de asegurar las redes frente a las amenazas emergentes y las vulnerabilidades existentes mediante una nueva plataforma de hardware para los diferentes servicios de seguridad.

El documento *"Addressing hardware security challenges in internet of things: Recent trends and possible solutions"* busca garantizar la seguridad durante este intercambio de información voluminosa, el cual es un problema crítico en este contexto. Se aplica por igual tanto a la comunicación de dispositivos, señales de control, y el intercambio de información. En este trabajo se ha realizado un enfoque para identificar los principales problemas de seguridad y privacidad existentes en la IO dispositivos especialmente desde la perspectiva de hardware habilitado, y de este modo presentar posibles soluciones a los retos existentes para la conversión de 'Internet de las cosas' en 'Internet de las cosas seguras'.

Uno de los protocolos importantes para tener una arquitectura segura de IoT se ve reflejado en el siguiente artículo *"Innovative DTLS/TLS security modules embedded in SIM cards for IoT trusted and secure services"* el cual aporta una posible solución mediante una plataforma innovadora de IoT basada en módulos de seguridad DTLS y TLS.

DTLS es el protocolo capaz de evitar que se escuchen los datos mediante fuentes externas (*eavesdropping*), como también busca evitar las modificaciones de los datos o los accesos no permitidos por el usuario.

Este protocolo tiene como base TLS que es un protocolo criptográfico que permite las comunicaciones seguras en la red. Como se menciona anteriormente su seguridad está ubicada en la capa de transporte, esto permitirá cifrar el flujo de datos entre los objetos en diferentes aplicaciones tales como:

- ✓ Navegación Web
- ✓ Información Confidencial(registros)
- ✓ Mensajería Instantánea
- ✓ Voz sobre IP

Aun así el protocolo TLS debe ser actualizado constantemente debido a a la cantidad de vulnerabilidades que enfrenta, hasta el momento como se puede ver en la siguiente figura son algunas de las versiones actuales de TLS enfrentadas con los ataques informáticos más conocidos:

CIFRADO	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
AES CBC	-	-	-	Seguro	Seguro
AES GCM	-	-	-	-	Seguro

Figura 6. Seguridad cifrada frente a diferentes ataques
Fuente: Elaboración Propia

Teniendo en cuenta la Figura 6, actualmente uno de los estándares de cifrado más poderosos son el AES y CBC, el primero de ellos es un estándar de cifrado, uno de los más utilizados en criptografía simétrica.

Algunas ventajas del AES:

- Libres para cualquier usuario
- Ser un algoritmo de cifrado simétrico y soportar bloques de como mínimo, 128 bits.
- Las claves de cifrado podrían ser de 128, 192 y 256 bits.
- Se puede implementar en hardware y software.

El despliegue de Internet de las Cosas trae consigo retos y dificultades, los cuales deben ser atendidos por parte de los participantes del ecosistema IoT. Como se ha mencionado anteriormente, una de las principales dificultades, está asociada con el tema de seguridad y privacidad de la información. Actualmente, existen en el mercado soluciones de seguridad implementadas por algunas empresas, tales como: SYMANTEC, MOCANA y TELEFONICA. Sin embargo, estas soluciones no garantizan un entorno seguro debido a la ausencia de algunos protocolos y tecnologías importantes para la implementación de un escenario seguro de Smart Homes.

2.4 SOLUCIONES EXISTENTES EN EL MERCADO PARA SEGURIDAD EN IOT

Se presentan tres soluciones de Internet de las Cosas actuales por parte de tres empresas diferentes, las cuales mediante ciertos requerimientos buscan proteger la información y los datos de los usuarios, aplicando algunas tecnologías que le brinden al usuario interfaces y comunicaciones seguras para IoT

TELEFONICA (Telefonica, 2016)

Hacking contra cámaras, discos duros, redes IP, Smart meters o coches. Televisores inteligentes que escuchan y emiten conversaciones sin cifrar en Internet. O lo que es lo mismo, millones de dispositivos conectados entre sí y a Internet, accesibles, y ofreciendo información en tiempo real. Cuando la información, tanto personal como empresarial, salta sin ningún tipo de filtro ni seguridad en la red, no existe segunda oportunidad. Cuando millones de dispositivos conectados utilizan diferentes tecnologías, el verdadero reto es ofrecer soluciones de seguridad escalables que permitan responder a las necesidades de heterogeneidad y escalabilidad que nos impone Internet of Things.

Trusted Public Key

Identidad y seguridad de la conexión.

En el mundo físico, nuestro DNI o Pasaporte nos identifican, pero en IoT ¿cómo aseguramos que los dispositivos son quién dicen ser?

Trusted Public Key Infrastructure permite identificar de forma única los dispositivos IoT a través de certificados digitales, ofreciendo una fuerte autenticación entre los objetos conectados a la red y los servicios del cliente (instalaciones de TI) reforzando la seguridad ya existente en las comunicaciones.

CyberThreats

Seguridad contra amenazas externas.
Smartmeters o contadores inteligentes que ponen en riesgo tus datos personales.
¿Sabes quién está detrás de acceder a tu información personal?De nuestra solución CyberThreats, te presentamos su nueva capacidad para detectar de manera temprana e identificar el modus vivandi de los cibercriminales, que utilizan técnicas de ataques contra las infraestructuras IoT de las organizaciones o contra su red de proveedores.

Vamps powered by Faast
Seguridad en infraestructuras IoT.

Webcams, impresoras, o teléfonos IP conectados a la red corporativa, se intercomunican con el resto de sistemas y también con servidores externos. Vamps

ahora también detecta las amenazas de seguridad en todos los dispositivos IoT de tu entorno corporativo.

Security Monitoring

Seguridad en los dispositivos.

Cámaras IP utilizadas para generar ataques de denegación de servicio o farolas de una Smart City modificando la configuración de los semáforos.

Security Monitoring permite identificar comportamientos anómalos de los dispositivos IoT basándose en su tráfico de red y en sus logs de funcionamiento.

Además, gracias a la tecnología FaasT, realizamos un escaneo continuo de tus sistemas descubriendo los dispositivos IoT conectados a tu red, detectando cualquier error de configuración o fallo de seguridad que permita a un usuario no autorizado acceder a tus datos.

Incident Response

Respuesta ante incidentes de seguridad.

Infraestructuras críticas (energía, salud, transporte, o telecomunicaciones), que son vulneradas y requieren una respuesta inmediata para evitar daños personales.

Incident Response cuenta con un equipo de expertos que evalúan el impacto de una vulneración de tu infraestructura, elaborando un plan de acción y ayudándote a prevenir potenciales riesgos de seguridad.

SYMANTEC (Symantec, 2016)

Servicios ofrecidos

Los sistemas de Internet de las cosas presentan grandes diferencias, según el sector, pero tienen muchos requisitos de seguridad comunes. Symantec ofrece una variedad de soluciones básicas para la identidad y la seguridad de los dispositivos de Internet de las cosas de la actualidad. Además, aprovechamos nuestras soluciones y tecnologías existentes para ofrecer una plataforma completa de seguridad, administración y análisis integrales para Internet de las cosas. Esta solución integral autentica la comunicación, protege las aplicaciones y los dispositivos, busca anomalías en todo el sistema y administra y actualiza los dispositivos de forma remota incluso en entornos con recursos limitados. Actualmente, Symantec cuenta con soluciones para proteger y autenticar dispositivos y códigos en entornos de Internet de las cosas (IoT):

- Seguridad de dispositivos: bloquee los dispositivos de Internet de las cosas para evitar riesgos de ataques

- Certificados de dispositivos para la autenticación: autentique los dispositivos de Internet de las cosas y cifre los datos transmitidos mediante sistemas y redes de Internet de las cosas

- Raíces de confianza y protección de códigos: Verifique que todos los códigos ejecutados en cada dispositivo de Internet de las cosas (IoT) estén autorizados para ese dispositivo y protegidos por una raíz de confianza segura

- Estamos desarrollando nuestras ofertas de Internet de las cosas existentes para ofrecer las siguientes soluciones adicionales en el futuro:

- Análisis de seguridad: detecte proactivamente conductas anormales que puedan indicar ataques sofisticados u ocultos en redes de Internet de las cosas

- Plataforma de Internet de las cosas: actualice y configure los dispositivos de Internet de las cosas de forma remota, recopile la telemetría y permita a los clientes compartir datos de Internet de las cosas de forma segura con sus partners preferidos de análisis de otros fabricantes (Ver Figura 42)

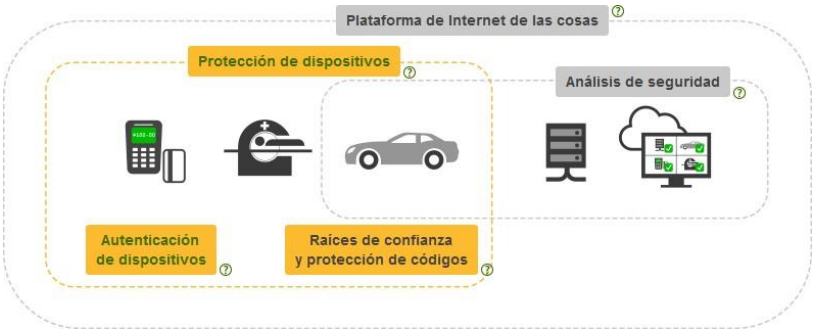

Figura 7. Solución SYMANTEC
Fuente:(Symantec, 2016)

MOCANA (MOCANA, 2016)

La compañía Mocana ofrece una alternativa de seguridad para el internet de las cosas mediante un framework que permite resolver algunos ataques a dispositivos Iot mediante: (Ver Figura 43)

- ✓ Certificate Management
- ✓ Cryptographic Engine

- ✓ Security for IP communication (IPsec)
- ✓ SSH client/server solution
- ✓ Secure Data Transport
- ✓ Firmware Update
- ✓ EAP Transport Layer Security

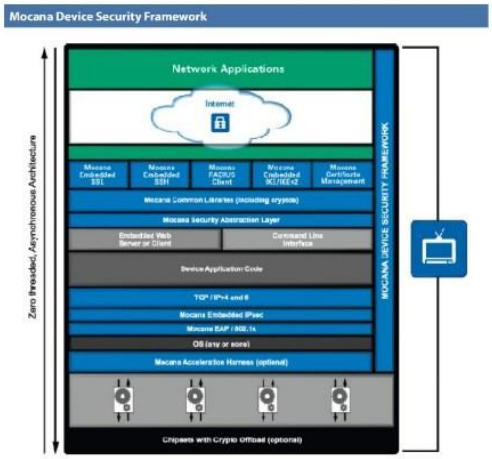

Figura 8. Framework MOCANA
Fuente: (MOCANA, 2016)

En síntesis, el Trabajo de Investigación llevado a cabo es pertinente y apropiado para el contexto colombiano. debido a que busca dar garantías a los usuarios de Smart Homes de que su información se mantendrá segura mediante la implementación de protocolos y tecnologías que brinden seguridad a soluciones tecnológicas basadas en Internet de las Cosas.

3. MARCO REFERENCIAL

En esta sección se presenta el Marco Conceptual, Marco Teórico y Marco Legal del Anteproyecto de Investigación.

3.1. MARCO CONCEPTUAL

El contexto teórico del proyecto se ubica en cinco conceptos fundamentales (i) IoT, (ii) *IoT security,* (iii) *Smart homes*, (iv) Seguridad de la información y (v) Privacidad.

4.1.1. IoT**.** Puede concebirse como una infraestructura global de la sociedad de la información, que permite ofrecer servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación (TIC) presentes y futuras. (ITU, 2012).

4.1.2. IoT Security. Es el área que busca proteger los dispositivos y redes conectadas en el Internet de las Cosas (Rouse, 2015)

4.1.3. Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información. (ITU, 2012)

4.1.4. Privacidad. La protección de datos, también llamada privacidad de información, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros. (Rouse, 2014)

4.1.5. Smart Homes. Es el término comúnmente utilizado para definir una residencia que tiene electrodomésticos, iluminación, calefacción, aire acondicionado, televisores, computadoras, entretenimiento de audio y sistemas de vídeo, seguridad y sistemas de cámaras que son capaces de comunicarse entre sí y pueden ser controlado a distancia por un programa de tiempo, desde cualquier habitación de la casa, así como de forma remota desde cualquier lugar del mundo por teléfono o Internet. (Smart Home Usa, 2016).

3.2. MARCO TEÓRICO

4.2.1. IoT Beneficios en *Smart Homes.* Las *Smart Homes* están equipadas con una tecnología llamada IoT que permite controlarla de forma remota mediante la programación de dispositivos electrónicos dentro del hogar, automatizando sus aplicaciones.

Los beneficios de estas se ven reflejados en la reducción de los costes de energía, el aumento de la productividad de los dispositivos electrónicos y mejorar la toma de decisiones en toda la organización o del hogar.

La integración es la clave para la construcción inteligente, ya que es la vinculación de los sistemas de construcción juntos, de conectar el sistema de automatización en las *Smart Homes* y en el control de toda la información que Internet de las Cosas (IoT) pueda gestionar en una sola plataforma.

Hay algunos pasos simples que deben tenerse en cuenta para utilizar esta plataforma: conectar los dispositivos, recopilar datos, y gestionar los dispositivos y datos.

IoT está cambiando el futuro y es por eso la expansión del mercado de las *Smart Homes* ya está disponible para facilitar la vida a sus usuarios y consumidores aprovechando la cantidad de dispositivos conectados.

Permitiéndole al usuario sin necesidad de estar físicamente allí y hacer un seguimiento de todos los dispositivos conectados en su *Smart Home* de una manera eficiente.

4.2.2. Protección en dispositivos IoT. El internet de las cosas da vida a todos los objetos o dispositivos que se puedan conectar a la red, pero es importante como usuarios tener en cuenta que los avances tecnológicos traen consigo vulnerabilidades y riesgos.

Es evidente que el avance de la tecnología y la cantidad de dispositivos que se conectan a Internet han aumentado el índice de ataques y posibles riesgos de seguridad que enfrentan tanto las empresas como los usuarios en sus hogares. En este sentido, la protección ya no es una problemática de unos pocos ni una práctica especializada, sino que comienza a volverse parte de la vida cotidiana. (Colombia Digital, 2016).

Hoy en día como se mencionó antes el avance de la tecnología es cada vez más rápido, y ya IoT está muy cerca y se encontrará presente no solo en los hogares, si no en bancos, empresas particulares, empresas del gobierno e instituciones educativas.

En conclusión, la información que se almacenará y se transmitirá en la red debe ser confidencial por lo tanto requiere de medidas para protegerla, estas deben ser establecidas por iniciativa propia o por proveedores, clientes o gobiernos que serán los encargados de la regulación de las medidas para así evitar la pérdida, fuga o robo de información confidencial.

3.2.3. Seguridad en IoT

Cuando se quiere hablar de seguridad informática o de la información es importante tener en cuenta los posibles riesgos, amenazas o vulnerabilidades a las que está expuesto para el caso de estudio IoT, por eso es importante en este proyecto encontrar un diseño de una arquitectura segura que tenga en cuenta que la información confidencial del usuario y que todos los datos que viajen a través del IoT son de carácter sumamente confidencial, para esto también es importante pensar como atacante, es decir de qué manera un tercero o un

cyberdelincuente podría alterar la seguridad de nuestros dispositivos en nuestra Smart Home y aprovecharse de ello.

La pregunta de muchos usuarios de IoT es: ¿Qué queda en riesgo?, ¿Qué tipo de información queda vulnerable a terceros? (Microsoft, 2016)

- ✓ Procesos (servicios web, servicios Win32, demonios * nix, etc.). Tenga en cuenta que algunas entidades complejas (por ejemplo, sensores y puertas de enlace de campo) se pueden resumir como procesos cuando no es posible explorar estas áreas en profundidad.
- ✓ Almacenes de datos (todos los lugares donde se almacenan los datos, como un archivo de configuración o una base de datos).
- ✓ Flujo de datos (donde los datos se mueven entre otros elementos de la aplicación).
- ✓ Entidades externas (todo lo que interactúa con el sistema, pero que no está bajo el control de la aplicación; algunos ejemplos incluyen los usuarios y las fuentes de satélite).

Pero a que se refiere con “bases de datos, flujos de datos, y demás” realmente el usuario final en su Smart Home tendrá vinculado su Smartphone con la mayoría de “objetos, es decir la información que se estará compartiendo será de un gran volumen, por esto la información que quedaría vulnerable para un tercero o un atacante seria:

- ✓ Información Personal
- ✓ Fotos, Videos, Archivos multimedia personales
- ✓ Base de datos de contactos
- ✓ Base de datos de mensajes
- ✓ Acceso a correos electrónicos
- ✓ Redes sociales
- ✓ Alteración y/o modificación de datos
- ✓ Cuentas bancarias asociadas
- ✓ Alteraciones software

Eso en cuanto a la información digital, pero las Smart Home debido a la gran cantidad de sensores que manejan ponen riesgos aún más preocupantes tales como imaginar que algún día decidimos viajar con nuestra familia a otra ciudad, el problema sería que si nuestro sistema no tiene una arquitectura lo suficientemente segura podría estar expuesto a muchos riesgos ya que un atacante informático podría entrar al sistema de su Smart Home, podría desactivar las alarmas y desactivar seguros, eso implicaría a que el usuario podría ser víctima no de únicamente robo digital de información, sino de un robo físico en su hogar.

Los dispositivos conectados de uso especial tienen un importante número de posibles áreas de superficie de interacción y patrones de interacción, y todos ellos deben considerarse a la hora de proporcionar un marco para proteger el acceso digital a los dispositivos. El término "acceso digital" se usa aquí para establecer la diferencia con las operaciones que se llevan a cabo a través de la interacción directa de dispositivos en las que la seguridad del acceso se

proporciona a través del control físico del acceso. Por ejemplo, colocar el dispositivo en una sala con una cerradura en la puerta. Aunque el acceso físico no se puede denegar mediante software y hardware, se pueden tomar medidas para evitar que el acceso físico provoque interferencia en el sistema. (Microsoft, 2016)

¿A qué tipo de amenazas está expuesto IoT?

Suplantación de identidad: un atacante puede extraer material criptográfico clave de un dispositivo en el nivel de hardware o en el de software y, posteriormente, tener acceso al sistema con un dispositivo físico o virtual diferente bajo la identidad del dispositivo del que se ha tomado el material clave. Un buen ejemplo son los mandos a distancia que pueden encender cualquier televisor y que son herramientas populares para gastar bromas.

Denegación de servicio: un dispositivo se puede representar como incapaz de funcionar o comunicarse al interferir con frecuencias de radio o cortar hilos. Por ejemplo, una cámara de vigilancia cuya alimentación o conexión de red se han interrumpido intencionadamente cubriendo no notificarán datos.

Manipulación: un atacante puede reemplazar total o parcialmente el software que se ejecuta en el dispositivo, lo que potencialmente permite que el software reemplazado use la identidad genuina del dispositivo si el material clave o las instalaciones criptográficas que contienen materiales clave estaban disponibles para el programa ilícito. Por ejemplo, un atacante puede sacar provecho del material clave extraído para interceptar y suprimir datos del dispositivo en la ruta de acceso de comunicación y reemplazarlos por datos falsos que se han autenticado con el material clave robado.

Divulgación de información: si el dispositivo ejecuta software manipulado, dicho software puede proporcionar datos a partes no autorizadas. Por ejemplo, un atacante puede sacar provecho del material clave extraído para inyectarse a sí mismo en la ruta de acceso de comunicación entre el dispositivo y un controlador o la puerta de enlace del campo o la puerta de enlace en la nube para desviar información.

Elevación de privilegios: se puede forzar a un dispositivo que realiza una función específica a realizar otra función. Por ejemplo, se puede obligar a una válvula programada para abrirse a la mitad a abrirse completamente.

3.2.4. Requisitos Dispositivos IoT. A continuación, se indican los requisitos de alto nivel para IoT (ITU, 2012):

- Conectividad basada en la identificación: IoT necesita que se establezca conectividad entre un objeto e IoT con arreglo al identificador del objeto. Para ello puede ser necesario además procesar de manera unificada identificadores posiblemente heterogéneos.

- Compatibilidad: Es indispensable garantizar la compatibilidad entre sistemas heterogéneos y distribuidos para el suministro y consumo de diversos tipos de información y servicios.

- Redes automáticas: Es necesario que las funciones de control de red de IoT soporte las redes automáticas (en particular técnicas y/o mecanismos de autogestión, autoconfiguración, autor establecimiento, auto optimización y autoprotección), a fin de adaptarse a los diferentes dominios de aplicación, diferentes contextos de comunicación y números y diferentes tipos de dispositivos.

- Configuración automática de servicios: Es preciso poder configurar los servicios a partir de los datos de los objetos adquiridos, comunicados y procesados automáticamente con arreglo a las reglas configuradas por los operadores o personalizadas por los clientes. Los servicios automáticos pueden depender de las técnicas de fusión y minería de datos automáticas.

- Capacidades basadas en la ubicación: IoT debe dar soporte a capacidades basadas en la ubicación. Las comunicaciones y servicios relacionados con objetos dependerán de la información sobre la ubicación de los objetos y/o los usuarios. Es necesario detectar y rastrear automáticamente la información sobre la ubicación. Las comunicaciones y servicios basados en la ubicación pueden estar limitados por leyes y reglamentos y deben cumplir los requisitos de seguridad.

- Seguridad: En IoT, todo “objeto” está conectada lo que conlleva considerables amenazas de seguridad, en ámbitos tales como la confidencialidad, autenticidad e integridad de datos y servicios. Un ejemplo esencial de los requisitos de seguridad es la necesidad de integrar diferentes técnicas y políticas de seguridad para la diversidad de dispositivos y redes de usuario en IoT.

- Protección de la privacidad: Muchos objetos tienen sus propietarios y usuarios. Los datos detectados de los objetos pueden contener información privada acerca de sus propietarios o usuarios. IoT tiene que dar soporte a la protección de la privacidad durante la transmisión, combinación, almacenamiento, minería y procesamiento de datos. La protección de la privacidad no debe ser un obstáculo a la autentificación de las fuentes de datos.

- Servicios relacionados con el cuerpo humano de calidad y seguridad elevadas: IoT debe dar soporte a estos servicios. Cada país aplica leyes y reglamentos diferentes a estos servicios.

- La adquisición, comunicación y procesamiento de datos relativos a las características estáticas del cuerpo humano y el comportamiento dinámico con o sin la intervención humana.

- Autoconfiguración (*plug and play*): IoT debe soportar la autoconfiguración que permite generar, componer o adquirir sobre la marcha configuraciones semánticas para la integración paulatina y la cooperación de los objetos interconectadas con aplicaciones, y para atender las necesidades de las aplicaciones.

- Capacidad de administración: IoT debe dar soporte a la capacidad de administración para garantizar el funcionamiento normal de la red. Las aplicaciones IoT suelen trabajar automáticamente sin la intervención humana, pero el proceso global de funcionamiento deben poderlo gestionar las partes pertinentes.

3.2.5. Modelo de referencia IoT. En el siguiente modelo propuesto por la ITU, abarca 4 capas y 2 capacidades tales como la de seguridad y la de gestión (Ver Figura 7).

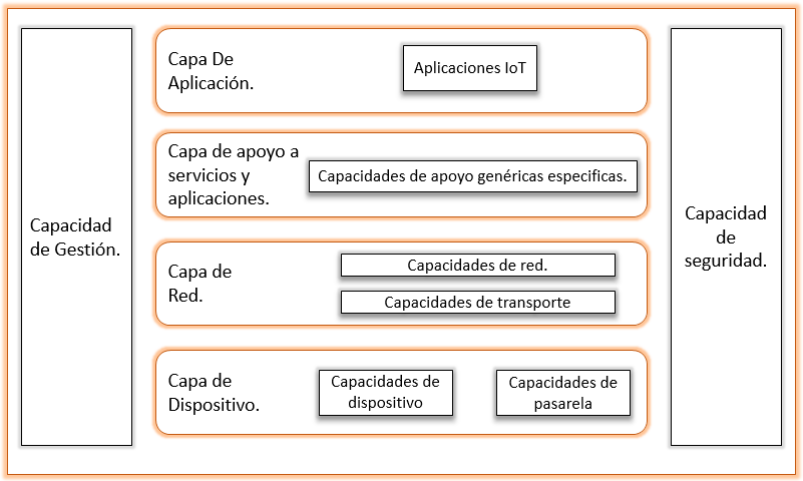

Figura 9. Modelo Capas IoT
Fuente: (ITU, 2012)

En la capa de aplicación como su nombre lo refiere, se encuentran las aplicaciones IoT en ámbitos tales como la automatización de tareas, el uso de sensores y la comunicación entre dispositivos electrónicos conectados a la red.

Luego se encuentra la capa de apoyo a servicios y aplicaciones que abarca las capacidades de apoyo genéricas las cuales se ocupan de capacidades frecuentes como lo son el procesamiento de datos y el almacenamiento de datos, mientras que en las capacidades específicas como su nombre da a entender se ocupan de necesidades más particulares de las aplicaciones de IoT.

En la capa de red se encuentra las capacidades de red y de transporte, la primera de ellas abarca las funciones de conexión a la red, controles de acceso y algunos protocolos de seguridad tales como la autentificación, autorización y

contabilidad, en cuanto a las capacidades de transporte abarca la conexión de red que se suministra para el transporte de datos, servicios de aplicaciones IoT.

Las capacidades de gestión se ocupan de la activación y desactivación de dispositivos remotos, actualización de software y firmware, gestión de la topología de red.

Las capacidades de seguridad abarcan tres capas: la de aplicación en la cual se ocupa de la autentificación, la autorización y la confidencialidad de los datos y/o información, protección de la integridad y de la privacidad de esta información, en la capa de red se ocupa de la autorización, autentificación y confidencialidad de los datos que estén viajando a través de la red y por último en la capa del dispositivo la autentificación, la autorización y la validación de la integridad del dispositivo.

3.2.6. Impacto despliegue IoT para Colombia (BdigitalStudio, 2015)

El despliegue de nuevas tecnologías en Colombia debe ir junto a las iniciativas de apropiación tecnológica que impulse el uso adecuado de las diferentes herramientas para el desarrollo de estas tecnologías.

Como se ha mencionado anteriormente la falta de políticas es un factor muy importante para que se maneje un correcto despliegue de IoT en Colombia, El despliegue generalizado de Internet de las Cosas tanto a nivel nacional como internacional debe ir de la mano de políticas claras sobre el manejo de la información y de la seguridad de la misma, para generar un ambiente de confianza en los usuarios y tener mayor facilidad de adopción y utilización de este.

Un aspecto que vale la pena destacar, corresponde al impacto económico que tendrá el despliegue de IoT en hogares (escenario: Smart Home).Para ello es importante conocer las necesidades de los hogares, saber que tan importante es para los usuarios realizar actividades como: (i) Vigilancia del hogar desde su oficina o desde cualquier otro lugar, utilizando un dispositivo móvil, (ii) Control de seguros (acceso al hogar), (iii) Revisión de la temperatura del hogar y, (iv) Control de electrodomésticos.

Para predecir la posible apropiación de IoT en el contexto colombiano, es importante tener en cuenta algunos datos estadísticos recuperados por el [3]DANE, [4]MINTIC, y la [5]CCCE que se han venido incrementado gracias al plan "Vive Digital"

Vive Digital, es el plan de tecnología para los próximos cuatro años en Colombia, que busca que el país dé un gran salto tecnológico mediante la masificación de Internet y el desarrollo del ecosistema digital nacional.

---

[3] DANE: Departamento Administrativo Nacional de Estadística

[4] MINTIC: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

[5] CCCE: Cámara Colombiana de Comercio Electrónico

l Plan responde al reto de este gobierno de alcanzar la prosperidad democrática gracias a la apropiación y el uso de la tecnología. Vive Digital le apuesta a la masificación de Internet. Está demostrado que hay una correlación directa entre la penetración de Internet, la apropiación de las Tecnologías de la Información y las Comunicaciones (TIC), la generación de empleo y la reducción de la pobreza. El plan Vive Digital conlleva entonces importantes beneficios sociales y económicos.

Según estudios de Raul Katz, de la Universidad de Columbia, en el caso Chileno aumentar en 10% la penetración de Internet generó una reducción en el desempleo del 2%. Según el UNCTAD *Information Economy Report* 2010, en países en desarrollo como Filipinas e India, por cada empleo generado en la industria TIC se generan entre 2 y 3.5 empleos adicionales en la Economía. Según el Banco Mundial y el reporte del Foro Económico Mundial, *The Global Information Technology Report* 2010, hay una correlación directa entre el *Network Readiness Index,* que mide el uso y desarrollo de las TIC, y su competitividad internacional.

Encontramos que Colombia debe superar diversas barreras para lograr la masificación de Internet. Tenemos barreras en todas las partes del ecosistema digital, es decir, en infraestructura, servicios, aplicaciones y usuarios. En esta propuesta de Vive Digital analizamos éstas barreras y proponemos diversas iniciativas para superarlas. (MINTIC, 2015)

Teniendo en cuenta esto se revisaron algunas estadísticas importantes que se pueden tener como base al despliegue de IoT en Colombia.

En la Figura 8, se puede evidenciar un avance en cuanto a la conexión de internet dedicada en los hogares independientemente de su estrato social. Basado en esto se puede afirmar que en la actualidad cada vez más hogares tienen conexión a internet.

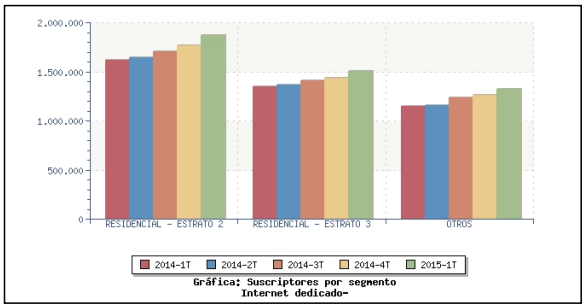

Figura 10.Suscriptores por segmento
Fuente (MINTIC, 2015)

En la Figura 9 se puede observar el número de Suscriptores con Internet dedicado por departamentos, se puede concluir que en la mayoría de departamentos las cifras son dominadas por los estratos 2,3 y 4.

	2015-1T								
NOMBRE	CC - OTROS COMPARTEL	CORPORATIVO	RESIDENCIAL - ESTRATO 1	RESIDENCIAL - ESTRATO 2	RESIDENCIAL - ESTRATO 3	RESIDENCIAL - ESTRATO 4	RESIDENCIAL - ESTRATO 5	RESIDENCIAL - ESTRATO 6	CAFÉ INTERNET
ANTIOQUIA	188	82.779	67.264	284.820	297.978	96.829	62.879	30.840	N.R
ATLANTICO	N.R	16.469	32.583	97.317	57.418	31.431	8.028	11.000	9.348
DISTRITO CAPITAL	N.R	138.389	67.100	474.363	525.066	220.313	56.956	49.391	1
BOLÍVAR	165	15.394	25.823	53.109	22.529	20.115	5.343	4.100	N.R
BOYACÁ	224	7.718	6.597	34.807	19.047	4.030	722	12	N.R
CALDAS	97	10.017	6.464	28.915	32.812	10.448	3.452	5.889	109
CAQUETÁ	1	2.141	6.316	5.435	1.555	230	1	1	N.R
CAUCA	7	4.165	6.229	22.033	14.325	4.918	1.379	444	N.R
CESAR	47	5.984	11.605	25.030	10.596	3.257	964	571	N.R
CORDOBA	127	11.350	19.373	24.695	8.812	2.541	908	1.044	N.R
CUNDINAMARCA	185	16.726	22.914	128.353	73.378	16.271	1.041	1.865	19
CHOCÓ	2	1.195	8.661	2.571	1.636	4	1	N.R	N.R
HUILA	6	8.751	13.044	43.073	10.870	3.907	486	55	N.R
LA GUAJIRA	21	2.807	4.760	12.556	3.268	191	31	1	N.R
MAGDALENA	164	7.154	7.119	22.916	18.078	5.183	890	1.445	5
META	50	10.571	8.702	32.424	29.274	3.789	1.487	612	N.R
NARIÑO	142	7.342	11.078	33.817	13.593	4.714	1.258	30	N.R
NORTE DE SANTANDER	171	12.640	14.238	52.315	23.405	13.363	1.711	303	N.R
QUINDÍO	10	6.867	9.481	28.791	18.151	6.574	3.966	1.597	16
RISARALDA	45	22.893	14.613	66.235	52.815	29.567	15.112	10.937	3
SANTANDER	234	26.501	23.586	85.129	71.089	60.252	8.427	6.744	16
SUCRE	42	4.628	9.798	19.818	3.905	1.619	132	290	N.R
TOLIMA	70	11.635	12.674	66.898	26.607	7.053	530	309	3
VALLE DEL CAUCA	138	44.593	54.963	210.222	158.955	68.696	31.398	14.020	4
ARAUCA	10	977	2.091	2.714	866	109	N.R	N.R	N.R
CASANARE	13	3.194	3.515	11.915	3.778	545	4	3	3
PUTUMAYO	7	785	2.890	2.271	200	N.R	N.R	2	N.R
SAN ANDRÉS	5	842	388	919	747	229	131	55	8
AMAZONAS	N.R	252	21	120	80	48	N.R	N.R	N.R
GUAINÍA	N.R	49	N.R	N.R	N.R	N.R	N.R	N.R	N.R
GUAVIARE	4	55	N.R	N.R	N.R	N.R	N.R	N.R	N.R
VAUPÉS	N.R	43	N.R	N.R	N.R	N.R	N.R	N.R	N.R
VICHADA	N.R	105	N.R	N.R	N.R	N.R	N.R	N.R	N.R

Figura 11. Suscriptores por Departamento
Fuente (MINTIC, 2015)

Al término del cuarto trimestre de 2015, las conexiones a Internet de Banda Ancha presentaron un crecimiento absoluto de 1.337.517 conexiones y una variación porcentual de 12,1%, cifras con referencia al primer trimestre de 2015. Por su parte, los accesos a Internet móvil soportados sobre redes de tercera generación 3G y cuarta generación 4G presentaron un crecimiento absoluto de 1.010.318 conexiones, y un crecimiento porcentual del 17,0% con relación al primer trimestre del año 2015 (MINTIC, 2015, p. 10).

En Colombia existen limitadas iniciativas alrededor de este tema, por ejemplo, Colciencias y “MinTIC” crearon una convocatoria que finalizó el 16 de enero de 2015 para la creación de centros de excelencia y apropiación en internet de las cosas. Esta convocatoria fue diseñada para empresas líderes y universidades.

> *“El Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT) es una alianza entre universidades, líderes tecnológicos mundiales y empresas ancla para potenciar el desarrollo económico del país desde el desarrollo tecnológico y la innovación a través de las tecnologías del Internet de las Cosas, buscando resolver las necesidades de diferentes sectores productivos del país. El CEA-IoT es una iniciativa impulsada desde el Ministerio de las TIC, con el apoyo de Colciencias, y corresponde a una estrategia que busca posicionar a Colombia como líder regional en TIC.”*

Entre las cuales, La Universidad Autónoma de Bucaramanga es una de las Universidades participantes en el CEA-IoT, que cuenta con la representación del Profesor César D. Guerrero como coordinador del Comité de Divulgación. Así mismo, están vinculados al CEA-IoT en representación de la UNAB tres

investigadores planta, siete estudiantes de maestría y un investigador en Post-Doctorado; quienes están vinculados en las líneas del trabajo del CEA-IoT, a saber: (i) Salud; (ii) Logística; (iii) Industria; (iv) Vestibles; (v) Seguridad; (vi) Agroindustria y Medio Ambiente y; (vii) Gobierno.

3.2.7. Principales inconvenientes para el despliegue de IoT (Internet of Things)

Con la llegada de IoT se impulsará la automatización de tareas, comodidad y facilidad para el uso en Smart Homes. Un alto porcentaje de profesionales del *Future Trends Forum* opinan que los mayores desafíos en la adopción del Internet de las Cosas son las lagunas en torno a la privacidad y seguridad, la falta de estándares globales y una infraestructura incapaz de soportar el ritmo de crecimiento.

Para esto es importante un proyecto como este que encuentre los requerimientos necesarios a nivel software, hardware, tecnologías y protocolos para el adecuado desarrollo de un escenario seguro de IoT aplicado a Smart Homes garantizándole al usuario final una infraestructura segura.

Como se menciona anteriormente uno de los factores más importantes a tener en cuenta será la elección de estándares, tecnologías, protocolos, software y hardware que serán los encargados de garantizar la seguridad y la privacidad de la información que el usuario este compartiendo con la red.

La falta de estándares y protocolos se considera un gran problema o amenazada debido a que IoT no cuente actualmente con ningún estándar permite a que sus fabricantes opten por usar sus propios adaptadores, sus bandas de frecuencia, y software que puede llegar a ser vulnerable amenazando al usuario final dejando a la disponibilidad de un tercero toda su información importante y confidencial.

En la Figura 10 Se puede evidenciar una clasificación de las industrias en las cuales se ha promovido el despliegue en el internet de las cosas en diferentes países, algunas de las industrias más relevantes son:

- Aeroespacial, aviación y automoción
- Telecomunicaciones
- **Hogares y edificios inteligentes**
- Tecnología medica
- Logística
- Utilidades
- Seguridad y privacidad
- Monitorización energía y entorno

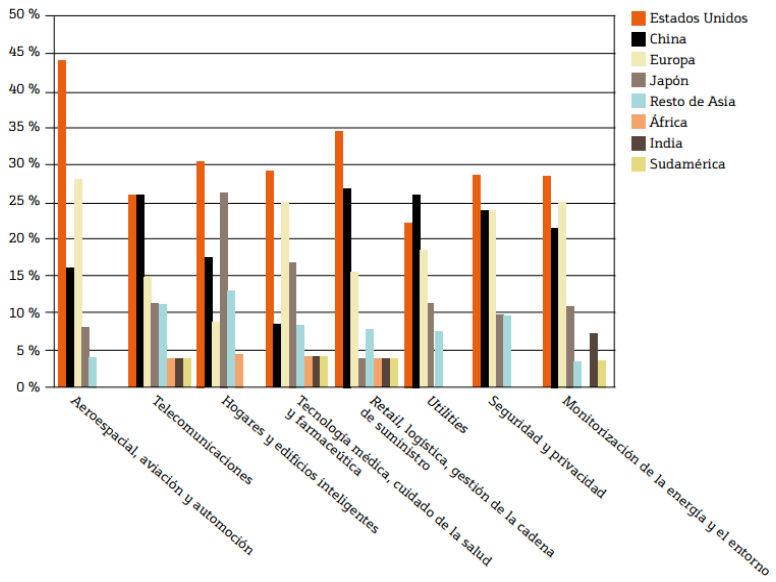

Figura 12. Clasificación de Industrias
Fuente: (Forum, 2016)

Como se puede observar en la figura anterior el internet de las cosas ha tenido un progreso evidenciable en algunos países como Estados Unidos, China, Europa y Japón, enfocando más el caso de estudio que sería la industria de los hogares y los edificios inteligentes se puede evidenciar mediante la figura el progreso nulo del internet de las cosas en Sudamérica, debido a esto se infiere que en el caso particular del progreso en Colombia se ha limitado por la falta de estándares y normatividad que permita que el internet de las cosas sea confiable para el usuario final.

Para Cisco, una de las empresas líderes en telecomunicaciones, hay varios obstáculos que podrían retrasar el desarrollo del IoT. De todos ellos, los tres más importantes son la implementación de IPv6, la energía de los sensores y un acuerdo sobre los estándares. Estándares. Si bien se ha avanzado mucho en el ámbito de los estándares, es necesario obtener más logros, especialmente en lo que a seguridad, privacidad, arquitectura y comunicaciones se refiere. IEEE es solo una de las organizaciones que trabajan para solucionar estos problemas, asegurándose de que los paquetes IPv6 puedan enviarse a través de diferentes tipos de redes. (Evans, 2011).

Otro obstáculo importante que no se ha mencionado es que teniendo en cuenta que todos estos dispositivos tecnologías que funciones con IoT y se encuentren en las Smart Homes serán controlados mediante dispositivos móviles como Smartphone y Tabletas, pero ¿Cuál es el verdadero obstáculo que no se ha tenido en cuenta?

La duración de la batería de los dispositivos es uno de los limitantes, debido a que estos deberán estar sometidos permanentemente no solo a una conexión a Internet, sino al envió y a la recepción de paquetes, es decir la interacción del dispositivo móvil o tableta con todos los dispositivos y electrodomésticos que están en la Smart Home.

Básicamente la forma en la que interactuarían este dispositivo se podría ver evidenciada en la Figura 11:

Figura 13. Interacción dispositivos IoT
Fuente (Peak, 2016)

3.2.8. Principales Vulnerabilidades en IoT

El despliegue de IoT trae consigo tanto avances como vulnerabilidades para esta, ya sea de tipo software o hardware, para esto se hizo una clasificación mediante tablas de las vulnerabilidades más conocidas que puedan afectar la información confidencial del usuario de la Smart Home.

Una de las áreas más vulnerables para IoT tiene que ver el software como se puede observar en la Tabla 3, ya que en esta el riesgo de un ataque malicioso es muy alto, es decir un atacante mediante un ataque Backdoor podrá de manera remota tomar acceso de cualquiera de nuestros dispositivos como se mostrara más adelante.

Área Vulnerable	Riesgos
Firmware Software Sistema Operativo Aplicaciones	Ataques Backdoor Malware Certificados Falsos

Tabla 3 Área software, Firmware, Sistema Operativo y Aplicaciones

En la Tabla 4 se tiene el área de memoria, información y bases de datos que incluirá toda la información importante y confidencial que este viajando en la Smart Home, ya sean datos personales como nombres de usuario, contraseñas como también información confidencial, mensajes, fotos, videos entre otros.

Área Vulnerable	Riesgos
Memoria Información BD	Usuario y Passwords sin cifrar Información confidencial sin cifrar Códigos criptográficos

Tabla 4.Area Memoria, Información y BD

En la Tabla 5 se puede observar uno de los aspectos más importantes para el correcto funcionamiento de IoT es la red debido a que este será el canal por donde viajen los datos, se debe tener rigurosas tecnologías y protocolos que garanticen al usuario final que su información seguirá integra de extremo a extremo.

Área Vulnerable	Riesgos
Red	Información sin cifrar Servicios red Extracción y alteración de información Protocolo [6]UPnp (no requiere autentificación)

Tabla 5 Área Red

La actualización de software mediante el fabricante legítimo ayudara mucho a fortalecer la seguridad de los dispositivos debido a que se solucionaran ciertas vulnerabilidades que puedan afectar la integridad de los datos como se puede observar en la Tabla 6.

Área Vulnerable	Riesgos
Actualización Software	Actualizaciones Maliciosas Actualizaciones Falsas Actualizaciones alteradas por atacantes

Tabla 6 Area Actualización Software

En la Tabla 7 se abordará el área de los métodos de autentificación que será uno de los factores más influyentes para una implementación segura en el Internet de las Cosas.

Área Vulnerable	Riesgos
Método de autentificación	Autentificación entre sensores Autenticación entre objetos IoT

Tabla 7 Area método de autentificación

[6] UPnP: conjunto de protocolos de comunicación que permite a periféricos en red, como ordenadores personales, impresoras, pasarelas de Internet, puntos de acceso Wi-Fi y dispositivos móviles, descubrir de manera transparente la presencia de otros dispositivos en la red y establecer servicios de red de comunicación, compartición de datos y entretenimiento.

En la Tabla 8 se menciona el área del hardware, las alteraciones que pueden existir en los dispositivos por parte de los fabricantes, desarrolladores o atacantes con fines maliciosos.

ea Vulnerable	**Riesgos**
Hardware	Alteración por parte de fabricante Alteración por parte de un atacante

Tabla 8 Area Hardware

Teniendo en cuenta la información encontrada en la revisión de la literatura, uno de los eslabones más importantes de la seguridad viene por parte del usuario final (ver Tabla 9), es decir la manera que los usuarios de la Smart Home utilicen de manera correcta IoT, por esto se consideró en la tabla no. Que los usuarios también son un área vulnerable para la seguridad en las Smart Homes.

Area Vulnerable	**Riesgos**
Usuarios	Contraseñas débiles Información Suministrada a terceros Baja seguridad Información sin cifrar

Tabla 9 Area usuarios

3.2.8. Ejemplo Backdoor ataque KaliLinux

En esta sección del documento se dará a conocer de qué manera un dispositivo móvil funcionando en *android* puede hacer que el usuario final se vuelva vulnerable ya que la automatización de los objetos se realizara desde el Smartphone y si este resulta estar infectado el atacante podría acceder de manera remota a su dispositivo y controlar todos los servicios de automatización asociados a la Smart Home.

La metodología para crear el *backdoor* es la siguiente:
Lo primero que haremos será definir la IP local (HOST) y el puerto por defecto que vamos a utilizar, estos dos serán por decir así el destino o escucha de la APK infectada, equipo donde llegarán todos los datos de nuestra víctima. Como se evidencia en la Figura 12.

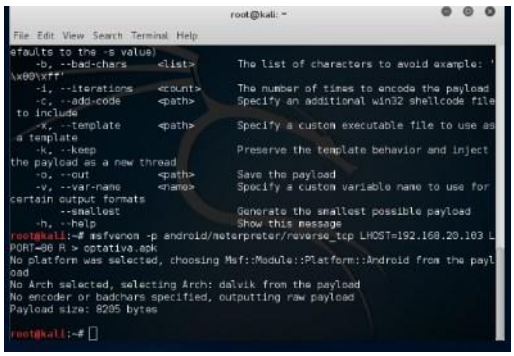

Figura 14. Host Kalilinux
Fuente: Elaboración Propia

A partir de este paso se procederá a la creación del payload y de la APK infectada, decidiremos mediante la ruta en que destino queremos crearla y

deberá tener una extensión ".apk" para su correcta instalación en el dispositivo Android.

Se "setearan" los payload para poder darle una correcta ejecución definiéndole la IP local y el puerto de escucha particularmente a este payload. (Ver Figura 13)

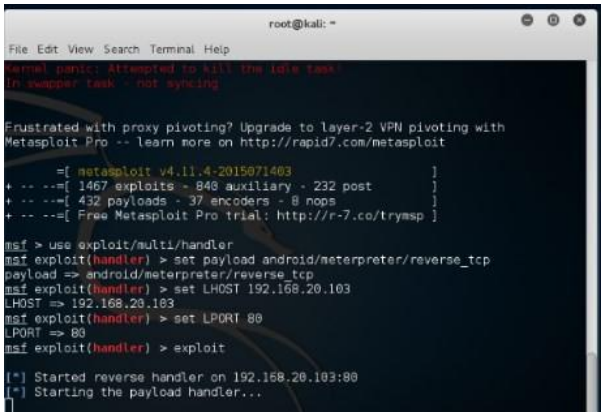

Figura 15. Seteo Payload
Fuente: Elaboración propia

En casos particulares que queramos afectar a usuarios Android que conozcan un poco más o tenga algunos conocimientos básicos de la informática será un poco más difícil lograr que la víctima instale la apk infectada ya que podrá revisar que esta aplicación está solicitando más permisos de los necesarios cosa que hará sospechosa y desistirá de instalarla, para esto lo que debemos es utilizar un "encoder" en este caso el shika ga nai y lo fusionaremos con otra aplicación que podría ser un juego que llamara la atención por ejemplo "angry birds" o algo similar, de tal manera que el usuario(victima) al instalar la aplicación , luego procederá a ejecutarla pero en realidad estará activando tanto nuestra backdoor(Se demuestra que los sensores, que se despliegan para evitar fallos, pueden ser explotados para insertar troyanos) pero también el juego, y por tal motivo no tendrá razones para sospechar que se trata de un virus. (Ver Figura 14)

Figura 16. Shikata Ga Nai
Fuente: Shikata Ga Nai

Luego de tener ya creada nuestra ".apk" infectada se procederá a elegir la victima cual será infectada mediante una técnica de Ingeniería Social (es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos) [8]. Con la cual la que queremos es conocer los gustos de la víctima, las personas con las que se relaciona, donde trabaja donde estudia, y asi poder lograr de una manera más sencilla poder lograr que la víctima instale la aplicación en su dispositivo móvil Android.

Al tener la victima ya instala la aplicación en su dispositivo móvil le será muy complejo poder detectarla debido a que el atacante podrá tomar posesión del teléfono sin que la víctima se dé cuenta, y además la aplicación queda instala como un proceso muy similar a los que corre el sistema operativo Android por defecto como lo podemos ver en la figura n°5.

En cuanto a la consola de ataque tendremos las siguientes opciones con las cuales podremos interactuar con el dispositivo infectado, pudimos observar que luego de realizar extracción de mensajes de texto, libretas de direcciones, imágenes y demás, la víctima no sufre ninguna alerta ni alteración en su dispositivo que le permita percatarse de que algo extraño está ocurriendo o que debe alarmarse por algún motivo.
En la figura no. Podremos conocer algunos de los comandos que podremos ver directamente desde el pc del atacante en la msfconsole, esta es tan solo unas de la gran cantidad de accesos que podremos vulnerar con esta apk infectada. (Ver Figura 15 & 16)

Figura 17. MsfConsole
Fuente: Elaboración propia

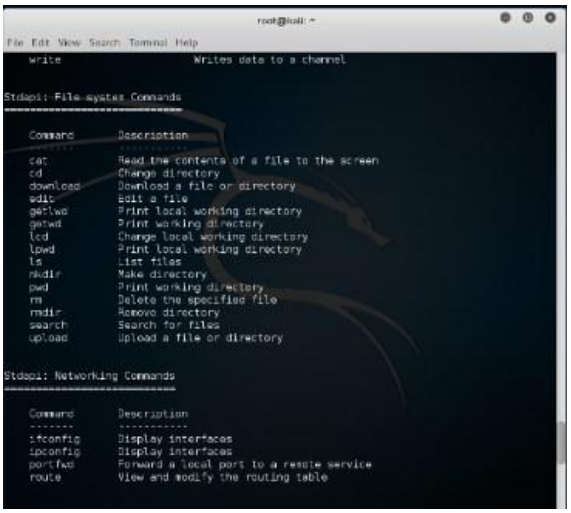

Figura 18. MsfConsole
Fuente: Elaboración propia

En conclusión, se debe tener en cuenta tanto la seguridad de la red como la de los dispositivos móviles ya que como se puede observar en la metodología para el *backdoor* el atacante puede tener acceso remoto y control total al dispositivo donde también podría controlar todos los servicios IoT asociados al teléfono móvil.

3.3. MARCO LEGAL

3.3.1. Estándares internacionales:

- **ISO/IEC 27000 2014** (*Information technology — Security techniques — Information security management systems — Overview* and *vocabulary*, 2014)

- **UIT-T Y.2060** (Serie y: infraestructura mundial de la información, aspectos del protocolo internet y redes de la próxima generación, 2012, Redes de la próxima generación – Marcos y modelos arquitecturales funcionales)

3.3.2. Estándares nacionales. La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

- **Artículo 269A: Acceso abusivo a un sistema informático.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- **Artículo 269C: Interceptación de datos informáticos.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269D: Daño informático.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269E: Uso de software malicioso.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F: Violación de datos personales.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos

personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

4. DISEÑO METODOLÓGICO

El Proyecto e Investigación se enmarca metodológicamente en cuatro etapas relacionadas entre sí, que permiten cumplir con los objetivos específicos, los cuales en su conjunto garantizan el cumplimiento del objetivo general de la investigación. Para tal fin, se realizaron un conjunto de actividades que permitieron dar cumplimiento a cada uno de los objetivos específicos definidos (Ver Figura 17).

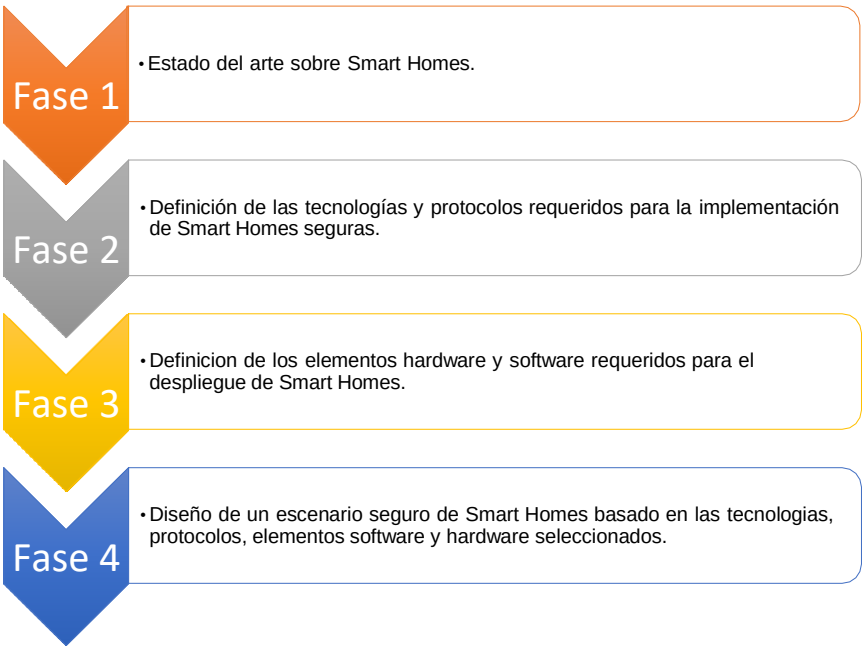

Figura 19.Diseño Metodológico
Fuente Elaboración Propia

Actividades asociadas al objetivo específico 1 (“Elaborar un estado del arte sobre Smart Homes a nivel mundial”):

- Recolección de información de fuentes bibliográficas académicas sobre Smart Homes a nivel mundial.
- Selección y síntesis de los documentos recuperados en la revisión de la literatura.
- Definición de criterios de inclusión y exclusión para la selección de referencias que serán parte del estado del arte de la investigación.
- Documentación del estado del arte de la investigación.

Actividades asociadas al objetivo específico 2 (“Definir las tecnologías y protocolos requeridos para la implementación de Smart Homes seguras”):

- Búsqueda de documentos científicos sobre tecnologías y protocolos empleados para el despliegue de Smart Homes seguras.

- Revisión de los documentos seleccionados sobre tecnologías y protocolos empleados para el despliegue de Smart Homes seguras.

- Selección de las tecnologías y protocolos empleados para el despliegue de Smart Homes seguras en el contexto colombiano.

Actividades asociadas al objetivo específico 3 (“Definir los elementos hardware y software requeridos para el despliegue de Smart Homes seguras en Colombia”).

- Selección de dispositivos hardware para el despliegue de Smart Homes seguras.

- Selección de software requerido para el despliegue de Smart Homes seguras.

- Documentación de los requerimientos necesarios para el diseño de un escenario seguro de Smart Homes.

Actividades asociadas al objetivo específico 4 (“Diseñar un escenario seguro de Smart Homes basado en las tecnologías, protocolos y elementos hardware y software seleccionados”).

- Presentación de tecnologías y protocolos seleccionados para el diseño de un Smart Home seguro.

- Presentación de elementos hardware y software seleccionado para el diseño de un Smart Home seguro.

- Diseño del escenario seguro de Smart Homes basado en las tecnologías, protocolos y elementos hardware y software seleccionados.

5. RESULTADOS

Los resultados esperados con el desarrollo del proyecto titulado “Solución tecnológica de Internet de las Cosas aplicado a Smart Homes seguras” son los siguientes:

- Estado del arte sobre Smart Homes a nivel mundial.
- Estudio sobre las tecnologías y protocolos requeridos para la implementación de Smart Homes seguras.
- Estudio sobre los elementos hardware y software requeridos para el despliegue de Smart Homes seguras en Colombia.
- Diseño de un escenario seguro de Smart Homes basado en las tecnologías, protocolos y elementos hardware y software seleccionados.

5.1. ESTADO DEL ARTE

El estado del arte de la investigación es presentado en la Sección 2.2.

5.2. TECNOLOGÍAS Y PROTOCOLOS PARA LA IMPLEMENTACIÓN DE SMART HOMES SEGURAS

En esta sección se dan a conocer las tecnologías y protocolos pertinentes para un adecuado despliegue de IoT en Colombia. La selección de estos fue llevada a cabo a partir de la revisión de la literatura, y de la búsqueda de vulnerabilidades y ataques existentes que afectan el Internet actual.

TLS (Transport Layer Security) (RFC5246, 2008)

Según el proceso investigativo uno de los ataques más comunes, es la suplantación de identidad, donde un delincuente informático busca tener acceso al sistema con el fin de extraer información confidencial tales como contraseñas o credenciales que le permitan luego ingresar al sistema en reemplazo del usuario final, para esto se ve importante la autentificación de los dispositivos mediante TLS (capa de transporte).
Son protocolos criptográficos que proporcionan comunicaciones seguras por una red, el protocolo TLS le garantizara al usuario de la Smart Home que la información que este compartiendo mediante la red cliente-servidor viajara por un canal seguro y cifrado, autentificando las claves de cifrado para poder realizar una transmisión segura.

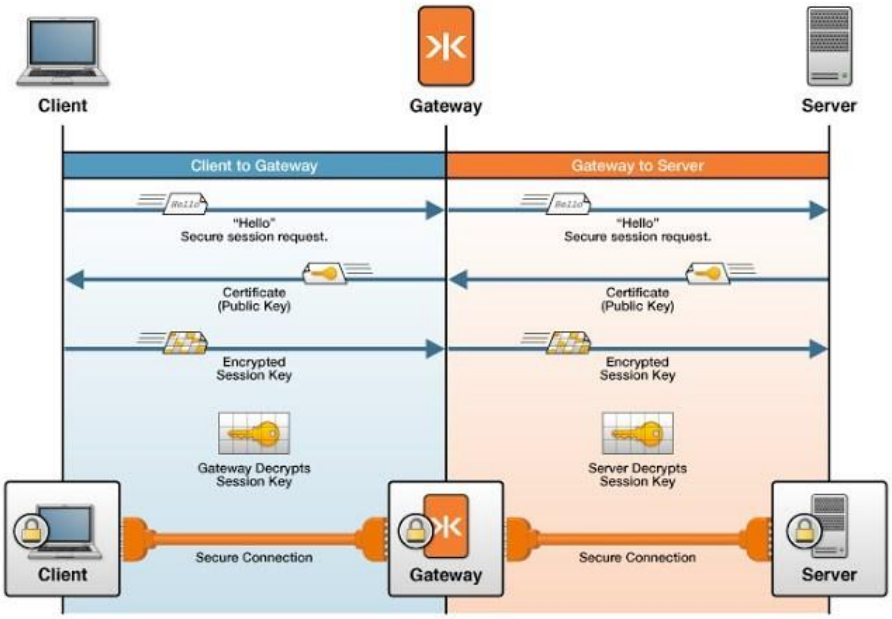

Figura 20. Como funciona TLS
Fuente: CCNA

Opciones de cifrado:

ECC[7] (ANSIX9.63, 2001)

Una de las opciones de cifrado que brinda mayor protección al usuario final, conocida como cifrado basado en curva elíptica, es un cifrado aprobado por el gobierno de los Estados Unidos.

También está aprobado como estándar por FIPS[8]

DTLS (RFC6347, 2012)

En cuanto a tema de seguridad también se debe tener en cuenta la implementación de **DTLS (Datagram Transport Layer Security)** evitando así las escuchas de terceros.

Estos protocolos con el fin de cifrar toda la información o tráfico que exista en la red, ya sea información confidencial, imágenes, videos, contraseñas, cuentas, almacenamiento de información de sensores, seguros eléctricos, control de cámara de vigilancia, entre otras.

[7] ECC: Elliptic Curve Cryptography
[8] Fips: Estándar US Federal Information Processing

En la siguiente figura se puede apreciar que elementos son los más comunes a ser alterados en las Smart Homes.

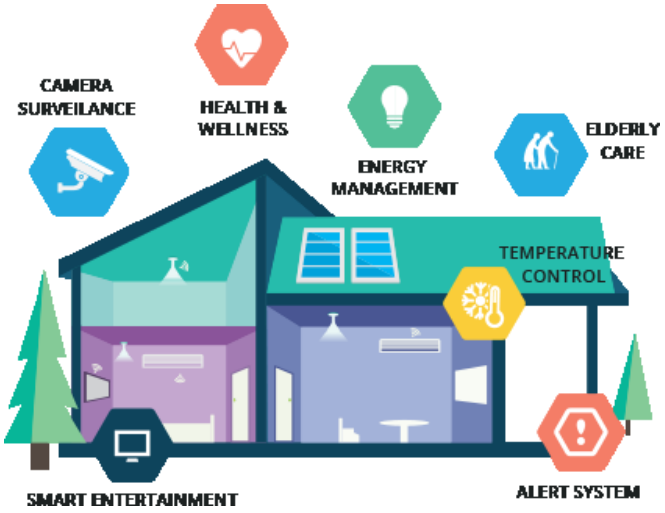

Figura 21. Sensores Smart Home
Fuente: WEBnms

Teniendo en cuenta la figura anterior, IoT básicamente es una red de sensores por eso es importante definir un protocolo que brinde seguridad a estos sensores con base al proceso investigativo se definió el protocolo MQTT *(Message Queuing Telemetry Transport)*. (OASIS, 2014)

Este protocolo brinda muchas ventajas tales como:

- ✓ Está especialmente adaptado para utilizar un ancho de banda mínimo.
- ✓ Es ideal para utilizar redes inalámbricas.
- ✓ Consume muy poca energía.
- ✓ Es muy rápido y posibilita un tiempo de respuesta superior al resto de protocolos web actuales.
- ✓ Permite una gran fiabilidad si es necesario.
- ✓ Requiere pocos recursos procesadores y memorias.

Está diseñado para redes de comunicación poco fiables y es interesante comentar que posee tres modos de funcionamiento o “calidad de servicio” (QoS)
.

- ✓ oS0 (*At most once*): El modo menos fiable pero también el más rápido. La publicación se envía, pero no se recibe confirmación.
- ✓ QoS1 (*At least once*): Se asegura que el mensaje es entregado al menos una vez, pero pueden recibirse duplicados.
- ✓ QoS2 (*Exactly once*): El modo más fiable y que más ancho de banda consume. Se controlan los duplicados para garantizar que el mensaje es entregado una única vez.

IoT en las Smart Homes intercambiara información muy importante, información confidencial y diferentes bases de datos, debido a esto es importante garantizar la seguridad de la información mediante diferentes tipos de autentificación la más sencilla de estas, será un nombre de usuario y contraseña que deberá conocer únicamente el usuario final, esta información viajara en la red mediante certificados SSL y TLS.

SSL (RFC6176, 2011)

Un certificado SSL(*secure sockets layer)* posee claves digitales que protegen la integridad de los datos en el momento de enviar y recibir la información, este dará la garantía al usuario final de que su sistema autentico, real y confiable, es decir que en él puede introducir información personal de manera segura.

El protocolo SSL tiene como fin 2 objetivos:

- Los datos deben viajar de manera íntegra en la red.
- Los datos deben viajar de manera segura por la red.

Mediante algoritmos matemáticos se cifrara toda la información confidencial y un sistema de claves que solo será identificado por el usuario final y el servidor en la Smart Home.

Por medio de un certificado SSL, nuestros datos estarán encriptados en ese momento se puede garantizar que la información que estén comunicando los “objetos” en la Smart Home, no tendrá accesos de terceros.

Un factor muy importante es que cada vez que tengamos una transacción de dinero en algún dispositivo móvil se revise el certificado SSL ya que este garantizara que la información que se esté enviando van dirigidas al servidor correcto.

Cuando se está navegando por el *Smart TV*, o el *Smartphone* si no se tiene el certificado SSL tendremos una alerta como se observa en la figura no., y no se debe continuar ya que nuestra información podría estar siendo dirigida a otros servidores.

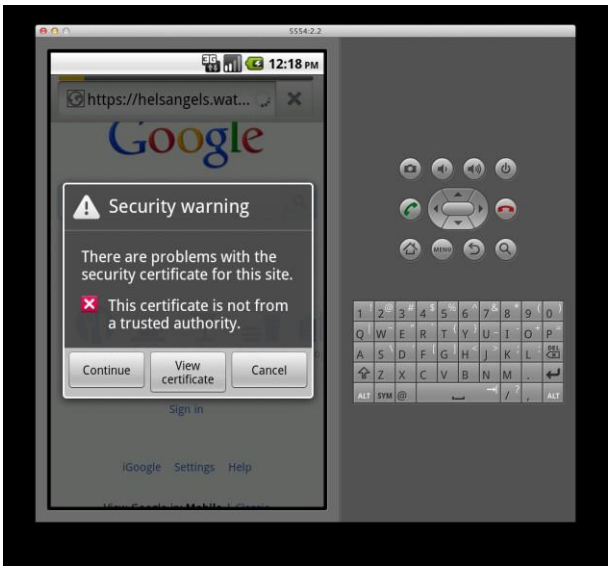

Figura 22 Seguridad certificado
Fuente: Chromiux

CoAP (RFC7252, 2014)

Otro protocolo relevante para la implementación de una Smart Home segura es el protocolo CoAp (protocolo de aplicación restringida), permite la comunicación de los diferentes nodos en el hogar mediante internet, realiza intercambio de mensajes por medio del protocolo UDP, Funciona en aplicaciones M2M (machine-to-machine) adaptándose al formato de nodos y sensores.

Constrained Application Protocol, CoAP, está diseñado para trasladar el modelo HTTP a dispositivos y redes restrictivas.

Permite la comunicación mediante las redes 6LoWPAN fragmentando los paquetes en tramas de capa 2.

6LoWPAN (RFC6282, 2011)

Hablando de temas de seguridad utilizar el estándar 6LoWPAN trae consigo muchas ventajas ya que este permite el uso de IPv6 *(Internet Protocol Version 6)* el cual es el sucesor de IPv4(*Internet Protocol Version 4),* entrando al tema que interesa para el caso de estudio mediante IPsec (*Internet protocol security)* se cifrará la información y también se hará la autentificación IP. Una de las mayores características por lo cual se decidió trabajar con el protocolo IPv6 se

dio debido a que el IPsec viene ya por defecto con el protocolo, mientras que con su antecesor simplemente era una opción de seguridad que muchas veces no se implementaba y dejaba el sistema vulnerable a terceros.

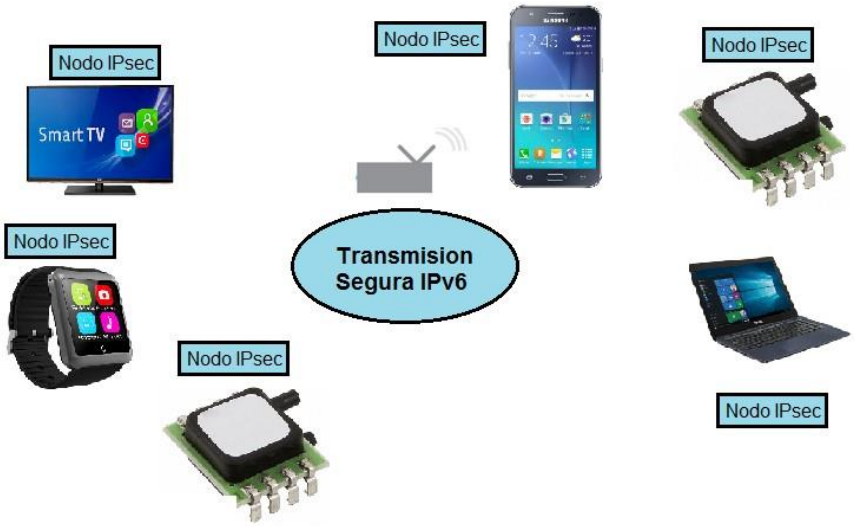

Figura 23. Transmisión segura IPv6
Fuente: Elaboración Propia

RFID (ISO, 2004)

La tecnología RFID (*Radio Frequency IDentification*) se utiliza para enviar la identificación de una persona o de un objeto en la Smart Home a través del uso de ondas de radio de manera inalámbrica, mediante un número de identificación único, es decir es un tipo de identificación automática.

Como se puede observar en la figura no. una etiqueta RFID es un CHIP que contiene una antena que es la que permite la comunicación con las ondas de radio, pueden almacenar cualquier tipo de información y almacenan alrededor de 2 Kilobytes.

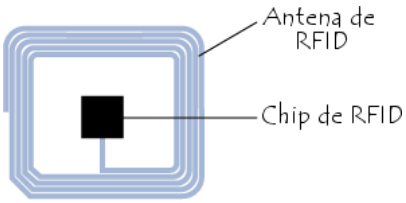

Figura 24. Etiqueta RFID
Fuente: RFIDLAB

SSH (Secure Shell) (RFC4253, 2006)

El protocolo SSH será imprescindible en las Smart Homes permitirá el acceso remotamente a través de la red, este protocolo permite manejar un dispositivo o objeto de la Smart Home mediante comandos, en cuanto a la seguridad el protocolo SSH utiliza técnicas de cifrado que permiten que la información que este viajando a través de la red este de manera no legible, garantizando así al usuario final que atacantes o terceros no tendrán acceso a dicha información.

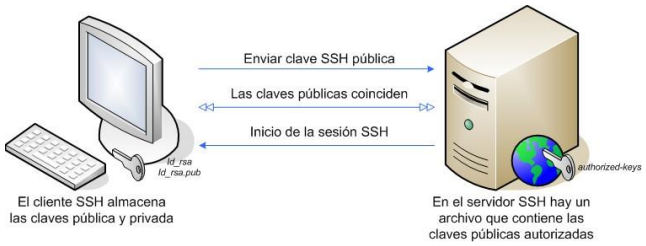

Figura 25 Como funciona el protocolo SSH
Fuente: (Hostalia, 2013)

El funcionamiento de este protocolo se puede resumir en los siguientes pasos: (Hostalia, 2013)

- El cliente inicia una conexión TCP sobre el puerto 22 del servicio. Este puerto es el que utiliza por defecto el protocolo, aunque como veremos en siguientes puntos, se puede modificar.
- El cliente y el servidor se ponen de acuerdo en la versión del protocolo a utilizar, así como el algoritmo de cifrado utilizado para el intercambio de la información.
- El servidor, que tiene en su poder dos claves (una privada y una pública), manda su clave pública al cliente.
- Cuando el cliente recibe la clave enviada por el servidor, la compara con la que tiene almacenada para verificar su autenticidad. El protocolo SSH exige que el cliente la confirme la primera vez.
- Con la clave pública del servidor en su poder, el cliente genera una clave de sesión aleatoria, creando un mensaje que contiene esa clave y el algoritmo seleccionado para la encriptación de la información. Toda esa información es enviada al servidor haciendo uso de la clave pública que envió en un paso anterior de forma cifrada.
- Si todo es correcto, el cliente queda autenticado, iniciando la sesión para comunicarse con el servidor.

ZigBee (IEEE802.15.4, 2006)

Es el grupo de protocolos de comunicación inalámbrica que se eligió para comunicación inalámbrica en la Smart Home, está basado en el estándar IEEE 802.15.4, su objetivo es garantizar la comunicación segura en redes WPAN (*wireless personal area network).*

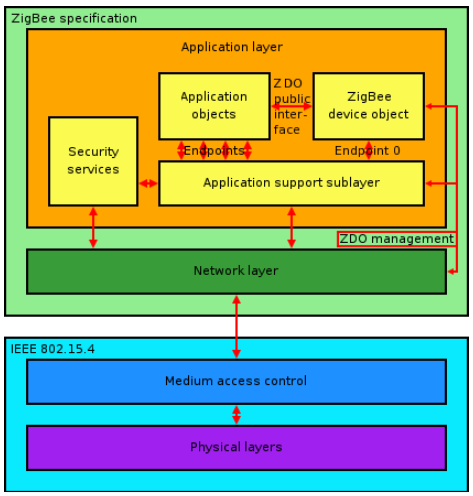

Figura 26 Como funciona ZigBee?
Fuente: ZigBee Alliance

ZigBee la seguridad de este protocolo está basada en la criptografía de clave simétrica, con 3 tipos de claves diferentes las cuales son:

Master key: mediante esta se generan las diferentes claves de enlace

Link key: esta es la encargada de cifrar las comunicaciones punto a punto, esta clave solo se comparte con dos elementos de la red.

Network key: esta es la clave que es utilizada a nivel de red y la que comparten todos los elementos en la Smart Home.
Es muy importante como se ha podido evidenciar que toda la información y los datos que viajen en la red deben ir cifrados deben existir garantías que le garanticen al usuario que su información ira de extremo a extremo sin acceso de terceros.

Otro factor importante a mencionar será la seguridad en la Nube, los controles de seguridad son elementos de red que pueden alterar el comportamiento de los objetos en la Smart Home, por ejemplo mediante un comando pueda desactivar los seguros de la casa, debido a esto los controles tienen muchas restricciones de privacidad en los sensores.

5.3. ELEMENTOS HARDWARE Y SOFTWARE REQUERIDOS PARA EL DESPLIEGUE DE SMART HOMES SEGURAS EN COLOMBIA.

Un factor muy importante en cuanto al software es mantener actualizado el sistema operativo de los dispositivos u objetos que trabajen en la red, esto con el fin de que cada actualización vaya solucionado vulnerabilidades.

Entre otras, adicionalmente las actualizaciones al software incluyes mejoras al sistema, y a las diferentes aplicaciones que se ejecuten en este, su función principal es dar el funcionamiento óptimo del dispositivo o de objeto, reparar fallas y errores que este pudiera tener en versiones anteriores.

Las actualizaciones en muchas ocasiones también pueden influir en el rendimiento de los “objetos”.

En cuanto al hardware relacionándolo con los aspectos de seguridad basado en la investigación con el objetivo de proteger las Smart Homes, se encontraron algunas soluciones tales como:

Soluciones a nivel Hardware

Solución ATMEL

La confianza es lo que la seguridad es realmente todo sobre la actualidad. Atmel productos de seguridad hacen que la "confianza" fácil de integrar en cualquier sistema. La flexibilidad, características avanzadas, arquitecturas rentables innovadoras, y los mecanismos de defensa de hardware ultra-seguras hacen que los dispositivos de seguridad basada en hardware Atmel una forma ideal para añadir confianza, por diseño.

5.3.1 Atmel CryptoAuthentication ™ - ofrece a los diseñadores de productos de una capacidad de autenticación de hardware extremadamente rentable, fácil de diseñar, pequeño y ultra-seguro.

Con el almacenamiento de claves basado en hardware garantizan que un producto, los consumibles que utiliza, el firmware que se ejecuta, los accesorios que lo soportan, y los nodos de la red que se conecta no se clonan, falsificado o manipulado.

Esto se da basado en SHA (*secure hash algoritm)* que es un algoritmo de cifrado de la familia de las funciones hash (Ver Figura 25).

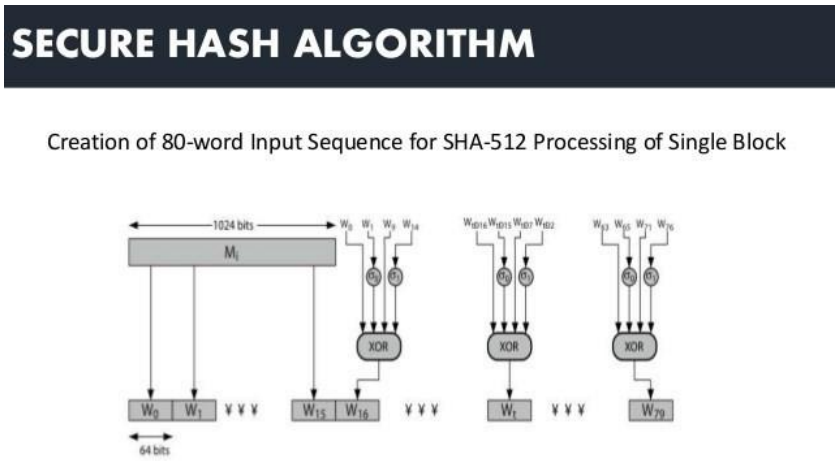

Figura 27. Algoritmo Hash
Fuente: SecureHash

En la Tabla 10 se puede observar alguna de las características de estos dispositivos en cuanto a beneficios, las tecnologías que maneja, los parámetros clave, y las aplicaciones en las cuales pueden ser implementados, para nuestro caso de estudio nos interesa la parte de hogar y automatización de edificios, que sería el área en la cual están incluidas las Smart Homes.

Device Family	Summary Benefit	Applications	Technologies	Key parameters
SHA-based Devices	Fast authentication Easy key management	Clone prevention Home and Building Automation Controlled access Industrial control Mobile accessories Lighting White Goods	HMAC Limited use keys for consumables	1MHz I2C Interface Single wire interface 256 bit key size

Tabla 10. Caracteristicas Dispositivos
Fuente: (ATMEL, 2016)

5.3.2 Trusted Platform Module - El módulo de plataforma Atmel segura (TPM) proporciona la clave pública sólida de seguridad basada en hardware (RSA) en un único dispositivo para ordenadores personales y tabletas, así como los sistemas basados en procesadores embebidos.

En la Tabla 11 se pueden conocer las características y beneficios del dispositivo, las tecnologías que manejan y parámetros clave.

Device Family	Summary Benefit	Applications	Technologies	Key parameters
TCG Version 1.2	Standards-based hardware security Network authentication Internet 'compatible' Turnkey solution Full TCG compliance High performance Software support libraries Two interfaces – LPC and 2-wire	System, device and network authentication Intellectual property protection, system integrity and secure communications.	AVR Microcontrollers EEPROM technology Hardware Security technology Cryptographic accelerator Random Number Generator Anonymous ID	TPM Trusted Platform Module PC security Tablet security TCG Trusted Computing Group RSA, PKI

bla 11 Características TCG Versión 1.2
Fuente: (ATMEL, 2016)

5.3.3 Atmel CryptoRF - Atmel CryptoRF® es una familia de dispositivos RFID de 13,56 MHz que emplea un motor de cifrado de hardware integrado de 64 bits, autenticación mutua, y hasta 64Kbits de memoria de usuario.

Atmel CryptoRF® es una familia de dispositivos RFID de 13,56 MHz (identificación por radiofrecuencia), equipado con un motor de cifrado de hardware integrado de 64 bits, capacidad de autenticación mutua, y hasta 64Kbits de memoria de usuario. Estos chips de bajo costo son prácticamente imposibles de copiar y ofrecer seguridad de hardware que es superior a las soluciones de software de seguridad.

Características:

- Más seguro que las contraseñas - La autenticación mutua entre el servidor y el cliente se lleva a cabo con un criptograma único que se genera aleatoriamente para cada transacción.

- Aislamiento Ataque - El sistema de claves a la diversificación limita cualquier ataque a una sola unidad.

- Niveles de acceso múltiple - Memoria de usuario se pueden dividir en un máximo de 16 secciones separadas, lo que permite diferentes niveles de lectura y escritura.

- Diversos paquetes - Los chips están disponibles en muchas formas y tamaños diferentes; etiquetas en una variedad de formas pueden ser desarrollados para aplicaciones de gran volumen.

- Simplicidad del host - El chip Atmel CryptoCompanion ™ ofrece simple, plug-and-play de autenticación en un dispositivo host (interrogador).

- Herramientas de desarrollo - diseños de referencia completas, kits de demostración, y software de aplicación facilitar la aplicación en productos existentes.

En la Tabla 12 se pueden conocer las características y beneficios del dispositivo, las tecnologías que manejan y parámetros clave.

Device Family	Summary Benefit	Applications	Technologies	Key parameters
CryptoRF	Secure RFID solution High frequency 13.56MHz ISO 14443 Type B protocol EEPROM densities up to 64 kbits 64-bit embedded hardware encryption engine Flexible security feature set to meet a wide variety of applications Mutual authentication capability	Product authentication Contactless payment Patient safety Anti-cloning of consumables Loyalty and patron management.	64-bit Cryptographic Algorithm Secure EEPROM technology Hardware Security technology ISO 14443 Type B protocol 13.56MHz Secure RFID	ISO 14443 Type B 13.56MHz RFID Hardware Security Authentication Secure EEPROM

Tabla 12. Caracteristicas CryptoRF
Fuente: Basado en (link) (ATMEL, 2016)

Seguridad en sensores IoT

En cuanto a IoT la seguridad debe ir desde un inicio, es decir los fabricantes de los objetos y/o sensores deben verificar desde su fabricación que estos cumplan con ciertos parámetros de seguridad que le den garantías al usuario de que su información está segura y que no será vulnerada por terceros.

Para esto es importante la implementación de políticas de seguridad para IoT en Colombia para regular ciertos parámetros mínimos de seguridad para los fabricantes de dispositivos IoT, ya que esto está provocando que al no existir aun tales parámetros en Colombia, los fabricantes no se tomen en el tiempo de realizar dispositivos seguros.

Los sensores que deberán mantenerse de una manera rigurosa seguros en la Smart Home son los siguientes: (SmartHome, 2016)

En la Tabla 13 se presenta algunos de los principales sensores que deben ser implementados en las Smart Homes para una adecuada implementación en cuanto a automatización de servicios, Es importante que sensores como los que se presentan se les implemente una serie de pruebas de seguridad, es decir que no puedan ser atacados o vulnerados por terceros, ya que esto podría tener repercusiones fatales para el usuario final de las Smart Homes.

Tabla 13. Sensores Basicos Smart Homes

	Remote Control Portable Thermostat Todos los teléfonos inteligentes y Tablet PC es el propietario se convierte en un mando a distancia. No importa si usted está ocultando bajo las sábanas en una mañana fría de invierno o llegando tarde fuera de la oficina en una noche de verano, ardiente, se puede ajustar la temperatura desde cualquier lugar.
	Carbon Monoxide and Smoke Detector with Voice El sensor viene equipado con una voz real que habla el tipo y la ubicación de peligro en su casa. Está monóxido de carbono y humo de alarma First Alert es perfecta, porque todo el mundo quiere ser notificado de inmediato donde el peligro está en su casa, para tomar las mejores decisiones en una situación de emergencia.

	Hidden Door Sensor Con este sensor podrá tener siempre desde su SmartPhone la información de si su puerta o garaje se ha abierto o si se olvidó de cerrar.
	Wireless Driveway Probe Alert Es un kit de alarma de entrada que detecta los vehículos que entran en un camino de entrada. El transmisor funciona con una batería de 9 voltios (no incluida) y tiene 50 pies de cable enterrado directo que conectan la sonda a la caja exterior.
	Open/Close Sensor Insteon ser su perro guardián. Con una serie de sensores Insteon En su hogar, puede recibir alertas instantáneas por correo electrónico o notificaciones al momento en que algo anda mal.
	Slim Line Door and Window Sensor Es ideal para su uso en aplicaciones de puertas y ventanas estrechas
	SmartGuard Dual-Head LED PIR Sensor Light with Camera Sensor para protegerse de posibles amenazas en su propiedad, recibe toda la informacion en tiempo real directamente a su SmartPhone o correo electronico, y ofrece advertencias pre grabado.

	Temperature/Humidity Sensor Controlar la temperatura y la humedad en la sala de servidores, equipos de armario, o área de trabajo utilizando un dispositivo simple y fiable. La temperatura USB THUM / Sensor de humedad se conecta a su PC a través de un puerto USB disponible, la entrega de datos precisos de temperatura y humedad en tiempo real sin ninguna interacción requerida.
	Window Alarm System Es una alarma de 120dB sonará cuando se abre una puerta o ventana. El sistema se activa o desactiva utilizando un código de teclado 4 dígitos.
	Degree ULTRAEYE Motion Sensor La fotocélula incorporada permite al usuario determinar cuando el detector de movimiento dará lugar a las luces o aparato de cable en función del nivel de luz detectado por la fotocélula.
	Pwr Savr Maestro Wireless RF Daylight Sensor Sensor inalámbrico funciona con una batería montaje en el techo de la fotocélula se utiliza para controlar automáticamente la iluminación y electrodomésticos.
uente: (SmartHomesStore, 2016)	

Es importante tener en cuenta que mediante todos los sensores que están implementados en las *Smart Homes* el riesgo que existe es muy grande como se puede observar en la Figura 41.

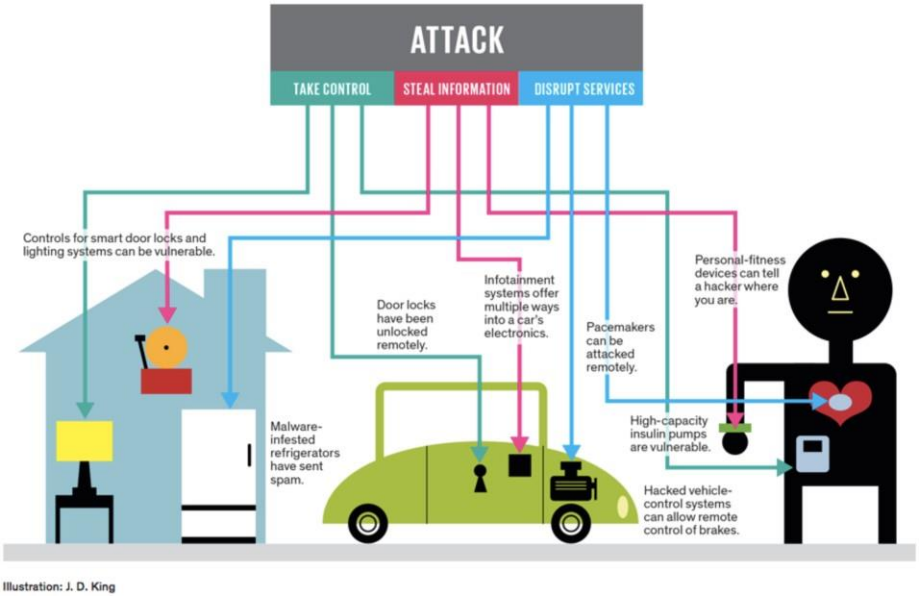

Figura 28. Vulnerabilidades Sensores
Fuente: (Pubnub, 2015)

5.4. DISEÑO DE UN ESCENEARIO SEGURO DE SMART HOMES BASADO EN LAS TECNOLOGIAS, PROTOCOLOS Y ELEMENTOS HARDWARE Y SOFTWARE SELECCIONADOS.

En esta sección se dará a conocer el escenario seguro de Internet De las Cosas enfocado a Smart Homes teniendo en cuenta toda la información recopilada en la revisión de la literatura.

Se utilizó un simulador de Smart Homes para mostrar de una manera más gráfica y atractiva como seria la posible implementación de una Smart Home.

El software a utilizar fue una versión de prueba de 30 dias, el simulador es “Interactive Smart Home Simulation” de la compañía Real Games.

Es una simulación interactiva de una casa inteligente y el medio ambiente circundante. Fue diseñado para cubrir una amplia gama de objetivos del plan de estudios en Ciencia, Tecnología, Ingeniería y Matemáticas. Los estudiantes aprenderán sobre la automatización del hogar, comportamiento térmico, la eficiencia del consumo de energía y muchos otros temas que son parte de la vida cotidiana.

Antes de instalar el Software se deben tener en cuenta los requerimientos mínimos del sistema para el uso adecuado de la herramienta de simulación de

lo contrario no se podrá tener una buena experiencia en la Smart Home.(Ver Tabla 14).

Sistema operativo	Windows Vista o superior.
Procesador	Intel Core 2 Duo a 2GHz, o AMD Athlon 64 x2 2 GHz o superior.
Memoria	1gb
Disco Duro	500mb
Video	Las tarjetas de NVIDIA desde 2007 (GeForce 8 Series), tarjetas de AMD desde 2007 (Radeon Serie 2xxx), tarjetas Intel desde 2008 (GMA 4500); soporte para Shader Model 3.0 o superior.
Sonido	Tarjeta de sonido compatible.
Directx	9.0c

Tabla 14. Requerimientos Home I/O
Fuente: (RealGames, 2016)

Para instalar el software se deben seguir unos sencillos pasos los cuales son los siguientes:

1. Ejecutar el programa de instalación con privilegios de administrador y si se le pregunta por el Control de cuentas de usuario, haga clic en Sí.
2. Siga las instrucciones del instalador.
3. Microsoft Visual C ++ 2010 es necesaria para el funcionamiento del simulador, y se recomienda que lo deje marcada.
4. Ahora es el momento de poner en marcha INICIO I / O, la activo o iniciar un juicio

Al finalizar estos pasos, tendrá acceso a una interfaz como se puede observar en la Figura

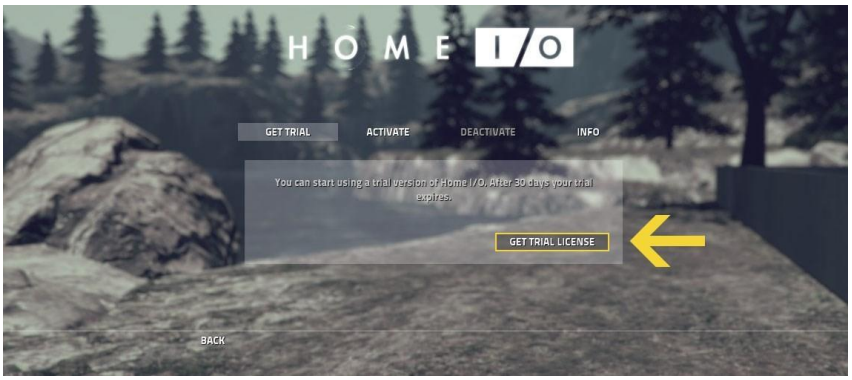

Figura 29. Interfaz Home I/O simulation
Fuente: (RealGames, 2016)

El siguiente escenario que se presentara es modelo, no válido para cualquier Smart Home (hogar), es un ejemplo (dependiendo de la arquitectura del lugar, se deben hacer ciertas variaciones).

Requerimientos Smart Home Seguro

Requerimiento	**Descripción**
Proveedor de servicio de internet (Wifi)	Telebucaramanga 10 Mbps
Tecnologías a Implementar	AUPS (Authenticated Publish & Subscribe) RFID (Radio Frequency Identification) Cloud Security NFC (Near field communication) SSL (secure sockets layer)
Protocolos a Implementar	TLS (Transport Layer Security) DTLS (Datagram Transport Layer Security) MQTT (Message Queue Telemetry Transport) CoAP (Constrained Application Protocol)
Software a Implementar	Firmware actualizado en Smartphone Firmware actualizado en dispositivos IoT Actualizaciones de Firmware con frecuencia
Hardware Seguro a Implementar	Solución ATMEL(Implementación a dispositivos IoT) Atmel CryptoAuthentication Atmel CryptoRF Trusted Platform Module
Sensores	Especificados posteriormente
Dispositivos IoT	Especificados posteriormente
Fuente: Elaboración Propia	

Tabla 15. Requerimientos Smart Home Seguro
Fuente: Elaboración Propia

Para el ejemplo de la implementación de un escenario IoT seguro se llevó a cabo en dos pisos, en el primer piso abarca la habitación principal, la sala principal, la cocina, el garaje y un baño. (Ver Figura)

Figura 30. Plano Escenario Smart Home (Piso1)
Fuente: Elaboración Propia

Para el segundo piso se destinó el estudio, la alcoba secundaria y un pequeño hall.

Figura 31. Escenario Smart Homes (Piso2)
Fuente: Elaboración Propia.

En la Figura se puede observar la Smart Home modelo desde el exterior.

Figura 32. Vista exterior Smart Home
Fuente: (RealGames, 2016)

5.4.1 Sensores Habitación Principal: En la habitación principal se tiene los siguientes sensores y dispositivos:

Sensor o Dispositivo	Descripción	Precio
Everspring ST814 Z-Wave Temperature & Humidity Sensor	Con este sensor se podrá controlar la temperatura de la alcoba directamente desde el Smartphone o Tablet que este asociada al Sistema, da la ventaja de fijar parámetros para cuando la temperatura en el exterior este de alguna manera determinada la interior varié según esto automáticamente.	$145.088
Smart Tv LG 42”	Televisor Smart Tv, te permite ver películas online, disfrutar de contenidos en la red, asociarlo a tu Smartphone y utilizar gran variedad de aplicaciones.	$1.469.000
Lutron LRF2-DCRB-WH Radio Pwr Savr Maestro Wireless RF Daylight Sensor, White	Sensor de luz que permite el ahorro de energía, reconoce por su tecnología el movimiento y según la hora del día puede ser programado para apagar las luces y así aumentar el ahorro de energía, controla las luces directamente desde el Smartphone.	$239.839
Motor 45/80 Motorized Drape Controller	Con este motor automáticamente según definamos las horas de despertar e irnos a dormir, se abrirán las persianas o de lo contrario se oscurecerán, pero en caso de que en cualquier otro momento se quiera hacer uso de ellas se hara directamente desde el Smartphone.	$269.449

Aire Acondicionado A 110v De 9.000btus Blanco Mabe Mmt09cabw	Aire acondicionado Apropiado para el tamaño de la habitación principal.	$791.900
Precio Total(Los precios son aproximados, pueden variar)		$2.915.276

Tabla 16. Tabla Sensores y dispositivos habitación Principal
Fuente: Elaboración Propia

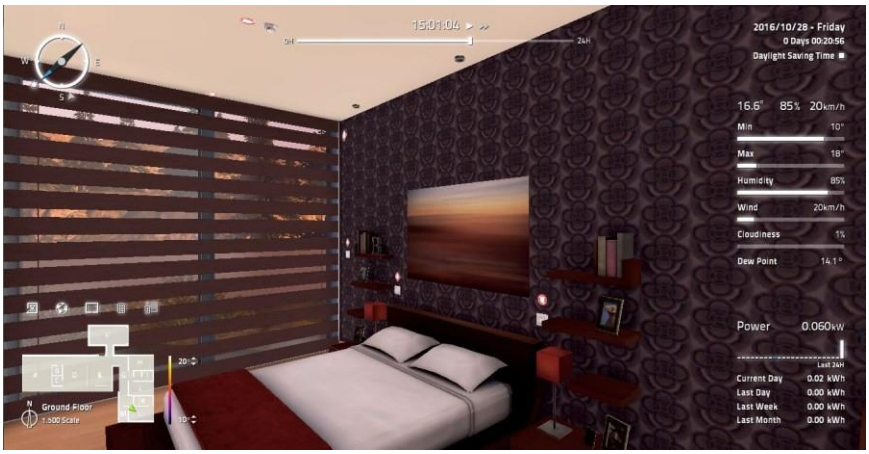

Figura 32. Habitación Principal
Fuente: (RealGames, 2016)

5.4.2 Sensores Habitación Secundaria: Para la habitación secundaria los sensores y dispositivos seleccionados son los siguientes:

Sensor o Dispositivo	Descripción	Precio
Everspring ST814 Z-Wave Temperature & Humidity Sensor	Con este sensor se podrá controlar la temperatura de la alcoba directamente desde el Smartphone o Tablet que este asociada al Sistema, da la ventaja de fijar parámetros para cuando la temperatura en el exterior este de alguna manera determinada la interior varié según esto automáticamente.	$145.088
Smart Tv LG 42”	Televisor Smart Tv, te permite ver películas online, disfrutar de contenidos en la red, asociarlo a tu Smartphone y utilizar gran variedad de aplicaciones.	$1.469.000
Lutron LRF2-DCRB-WH Radio Pwr Savr Maestro Wireless RF Daylight Sensor, White	Sensor de luz que permite el ahorro de energía, reconoce por su tecnología el movimiento y según la hora del día puede ser programado para apagar las luces y así aumentar el ahorro de energía, controla las luces directamente desde el Smartphone.	$239.839

Motor 45/80 Motorized Drape Controller	Con este motor automáticamente según definamos las horas de despertar e irnos a dormir, se abrirán las persianas o de lo contrario se oscurecerán, pero en caso de que en cualquier otro momento se quiera hacer uso de ellas se hara directamente desde el Smartphone.	$269.449
Aire Acondicionado A 110v De 9.000btus Blanco Mabe Mmt09cabw	Aire acondicionado Apropiado para el tamaño de la habitación principal.	$791.900
Precio Total(Los precios son aproximados, pueden variar)		$2.915.276

abla 17. Tabla Sensores y dispositivos habitación PrincipalFuente:
Elaboración Propia

Figura 33. Habitación Secundaria
Fuente: (RealGames, 2016)

5.4.3 Sensores Estudio: Para el estudio los sensores y dispositivos seleccionados son los siguientes:

Sensor o Dispositivo	Descripción	Precio
Everspring ST814 Z-Wave Temperature & Humidity Sensor	Con este sensor se podrá controlar la temperatura de la alcoba directamente desde el Smartphone o Tablet que este asociada al Sistema, da la ventaja de fijar parámetros para cuando la temperatura en el exterior este de alguna manera determinada la interior varié según esto automáticamente.	$145.088
Portatil Asus A550jx-dm342t - Ci7 - 1tb - Ram 12 Gb - Win 10	Los ASUS A550 trae procesadores Intel Core i7 de 4ª generación, una plataforma basada en la tecnología Ivy Bridge 22 nm con un excelente rendimiento para las tareas del día a día y multimedia.	$ 2.529.900

Lutron LRF2-DCRB-WH Radio Pwr Savr Maestro Wireless RF Daylight Sensor, White	Sensor de luz que permite el ahorro de energía, reconoce por su tecnología el movimiento y según la hora del día puede ser programado para apagar las luces y así aumentar el ahorro de energía, controla las luces directamente desde el Smartphone.	$239.839
Motor 45/80 Motorized Drape Controller	Control de persianas automáticamente, se pueden programar según horarios, o simplemente utilizar un switch desde el Smartphone para su uso.	$269.449
Aire Acondicionado 110v Y 12.000btus Negro Ge Mgi12cab2	Aire acondicionado Apropiado para el tamaño de la habitación principal.	$ 1.478.900
Precio Total(Los precios son aproximados, pueden variar)		$4.663.176

Tabla 18. Tabla sensores y dispositivos estudio
Fuente: Elaboración Propia

Figura 34. Estudio
Fuente: (RealGames, 2016)

5.4.4 Sensores Sala Principal: Para la sala principal los sensores y dispositivos seleccionados son los siguientes:

Sensor o Dispositivo	Descripción	Precio
Everspring ST814 Z-Wave Temperature & Humidity Sensor	Con este sensor se podrá controlar la temperatura de la alcoba directamente desde el Smartphone o Tablet que este asociada al Sistema, da la ventaja	$145.088

	de fijar parámetros para cuando la temperatura en el exterior este de alguna manera determinada la interior varié según esto automáticamente.	
TV LED Samsung 50" - Full HD - Smart TV - UN50J5500	Disfruta de un televisor smart de 50", te permite navegar en internet y conectarte con tus aplicaciones favoritas.	$1.539.800
Lutron LRF2-DCRB-WH Radio Pwr Savr Maestro Wireless RF Daylight Sensor, White	Sensor de luz que permite el ahorro de energía, reconoce por su tecnología el movimiento y según la hora del día puede ser programado para apagar las luces y así aumentar el ahorro de energía, controla las luces directamente desde el Smartphone.	$239.839
Motor 45/80 Motorized Drape Controller	Control de persianas automáticamente, se pueden programar según horarios, o simplemente utilizar un switch desde el Smartphone para su uso.	$269.449
Aire Acondicionado 110v Y 12.000btus Negro Ge Mgi12cab2	Aire acondicionado Apropiado para el tamaño de la habitación principal.	$ 1.478.900
Insteon Hidden Door Sensor	Este sensor le permitirá al usuario final recibir una alarma en su Smartphone cada vez que olvide cerrar una puerta o una ventana, igualmente será notificado de cuando cada una de estas se abran.	$115.478
egree ULTRAEYE Motion Sensor	Este sensor de movimiento trae incorporado unas fotocélulas que le darán la garantía al usuario que a cualquier movimiento tras ser activado recibirá notificación a su Smartphone, es decir tendrá un Smart Home Seguro.	$352.357
Precio Total(Los precios son aproximados, pueden variar)		$4.140.911

Tabla 19. Sensores y dispositivos Sala Principal
Fuente: Elaboración Propia

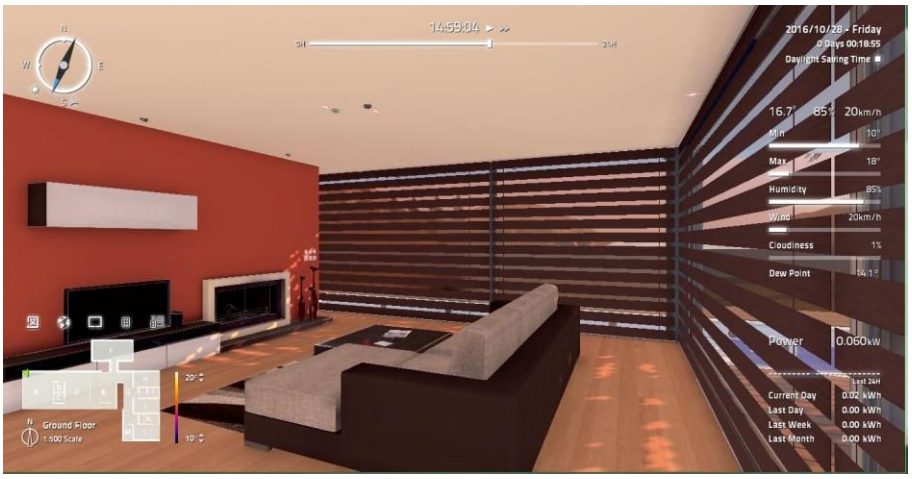

Figura 35. Sala Principal
Fuente: (RealGames, 2016)

5.4.5 Sensores Cocina: Para la cocina los sensores y dispositivos seleccionados son los siguientes:

Sensor o Dispositivo	Descripción	Precio
Everspring ST814 Z-Wave Temperature & Humidity Sensor	Con este sensor se podrá controlar la temperatura de la alcoba directamente desde el Smartphone o Tablet que este asociada al Sistema, da la ventaja de fijar parámetros para cuando la temperatura en el exterior este de alguna manera determinada la interior varié según esto automáticamente.	$145.088
Refrigerador Samsung Family Hub	El refrigerador tiene un diseño de cuatro puertas de aluminio inoxidable y su pantalla, que se encuentra en la puerta superior derecha, te permite colocar y compartir agendas, anclar fotos, ver videos y dibujos de tus hijos, al igual que para dejar notas -- todo desde tu celular.	$15.000.000
Lutron LRF2-DCRB-WH Radio Pwr Savr Maestro Wireless RF Daylight Sensor, White	Sensor de luz que permite el ahorro de energía, reconoce por su tecnología el movimiento y según la hora del día puede ser programado para apagar las luces y así aumentar el ahorro de energía, controla las luces directamente desde el Smartphone.	$239.839
Motor 45/80 Motorized Drape Controller	Con este motor automáticamente según definamos las horas de despertar e irnos a dormir, se abrirán las persianas o de lo contrario se oscurecerán, pero en caso de que en cualquier otro momento se quiera hacer uso de ellas se hara directamente desde el Smartphone.	$269.449

Samsung WW8500 AddWash	Incorpora diversas funciones inteligentes, que funcionan tanto con «smartphones» Android u otros sistemas operativos. Esto no sólo facilita monitorizar el progreso del programa de lavado, sino que también ofrece la opción de avisar a los usuarios en su propio teléfono justo antes de empezar una nueva fase del ciclo de lavado.	$7.402.000
recio Total(Los precios son aproximados, pueden variar)		$23.056.376

Tabla 20. Sensores y dispositivos cocina
Fuente: Elaboración Propia

Figura 36. Cocina
Fuente: (RealGames, 2016)

5.4.6 Sensores Garaje: Para el garaje los sensores y dispositivos seleccionados son los siguientes:

Sensor o Dispositivo	Descripción	Precio
Insteon Hidden Door Sensor	Este sensor le permitirá al usuario final recibir una alarma en su Smartphone cada vez que olvide cerrar una puerta o una ventana, igualmente será notificado de cuando cada una de estas se abran.	$115.478
Chamberlain MYQ-G0201 MyQ Garage Universal Smartphone Garage Door Controller	Sensor que permite el uso del garaje electrico desde la comodidad del Smartphone.	$393.811
Lutron LRF2-DCRB-WH Radio Pwr Savr Maestro Wireless RF Daylight Sensor, White	Sensor de luz que permite el ahorro de energía, reconoce por su tecnología el movimiento y según la hora del día puede ser programado para apagar las luces y así aumentar el ahorro de energía, controla las luces directamente desde el Smartphone.	$239.839
Garaje Electrico	Garaje eléctrico automatizado para funcionar con el sensor Chamberlain.	$4.000.000
Precio Total(Los precios son aproximados, pueden variar)		$4.749.128

Tabla 21. Sensores y dispositivos garaje
Fuente: Elaboración Propia

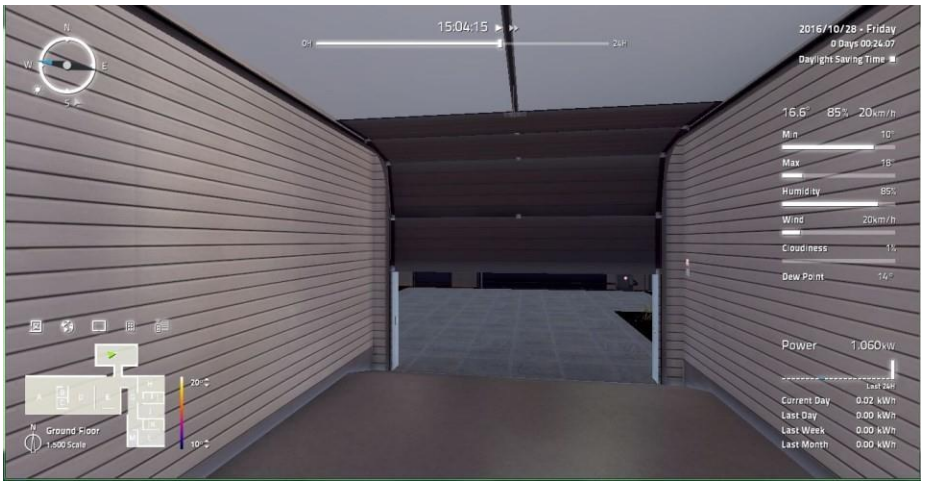

Figura 37. Garaje
Fuente: (RealGames, 2016)

5.4.1 Sensores Seguros: Para el estudio los sensores y dispositivos seleccionados son los siguientes:

Sensor o Dispositivo	Descripción	Precio
Skylink SC-1001 Total Protection Wireless Alarm System - Complete Kit	Sistema de seguridad complete inalámbrico, notificaciones al Smartphone(se conecta también con los sensores de puertas y ventanas)	$462.000
Insteon Wireless HD 720p IP Camera with Pan, Tilt & Night Vision - White (2-Pack)	Camaras de vigilancia de excelente resolución para la seguridad del interior de la Smart Home(incluyen visión nocturna)	$559.626
Insteon Wireless Outdoor HD 720p IP Camera with Night Vision (2-Pack)	Camaras de vigilancia de excelente resolución para la seguridad del exterior de la Smart Home(incluyen visión nocturna)	$672.144
Precio Total(Los precios son aproximados, pueden variar)		$1.693.770

Tabla 22. Sensores y dispositivos seguros
Fuente: Elaboración propia.

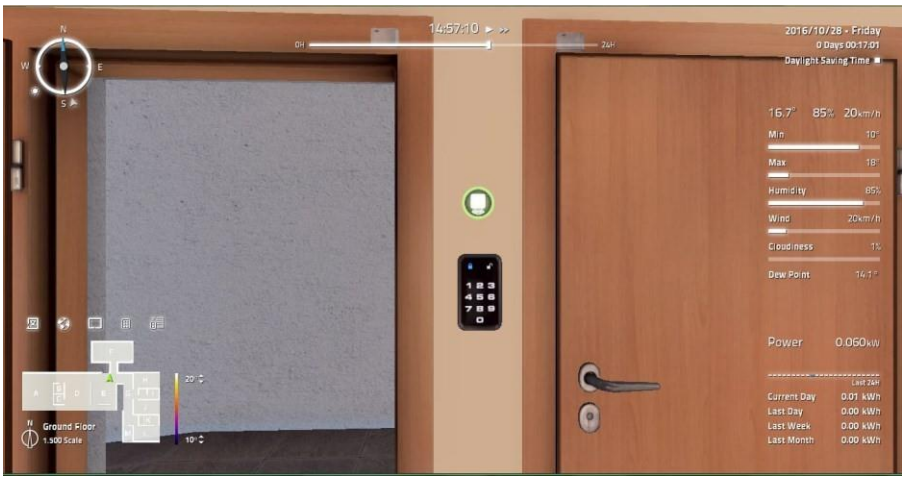

Figura 38. Seguro Principal
Fuente: (RealGames, 2016)

Área	Precio
Habitación Principal	$2.915.276
Habitación Secundaria	$2.915.276
Cocina	$23.056.376
Sala Principal	$4.140.911
Garaje	$4.749.128
Seguros	$1.693.770
Total	$44.219.865

Tabla 23. Presupuesto Implementación Smart Home(Modelo)
Fuente: Elaboración Propia

Todos los sensores y dispositivos mencionados anteriormente, podrán ser controlados por el usuario final desde la comodidad de su Smartphone, siempre y cuando estén conectadas a la red Wifi de la Smart Home, para el caso de la cámaras de vigilancia tanto exteriores como interiores están tienen la ventaja de poder ser monitoreadas por el usuario desde cualquier lugar con acceso a internet mediante una IP que le permitirá poder entrar al circuito de video y revisar que está ocurriendo en tiempo real en su Smart Home (Ver Figura 39)

Figura 39. Control desde el Smartphone
Fuente: (RealGames, 2016)

Como Mantener un Smart Home Seguro

A pesar de que se tenga implementado en el Smart Home los diferentes protocolos y tecnologías que le garanticen al usuario seguridad y privacidad de toda la información que este viajando mediante la red, existen otros factores muy importantes para garantizar estas protecciones, que provienen del eslabón más vulnerable en la seguridad, es decir el usuario.

Primero que todo se definieron ciertas prácticas en cuanto a contraseñas que son importantes tener en cuenta a la hora de tener una red segura, tales como:

- Las contraseñas deben tener al menos entre 8 a 30 caracteres, deben incluir una letra en mayúscula y al menos un número.
- No debe contener el mismo nombre de usuario.
- No debe coincidir con contraseñas utilizadas anteriormente.
- No es recomendado utilizar contraseñas como “123456789” o “asdfghjkl”.
- No se debe utilizar las mismas contraseñas para todas las cuentas, ya sean correos electrónicos, cuentas de acceso, entre otros.

- Las contraseñas deben ser cambiadas regularmente.

Por otro lado será importante revisar cada vez que el usuario final reciba adjuntos por el correo electrónico, o por redes sociales debido a que esto puede incluir un virus o un *backdoor* (Ver en la sección 3.2.8), con esto el atacante tendría acceso total al Smartphone, es decir tendría acceso a todos los dispositivos y sensores del Smart Home debido a que todos serán controlados directamente desde el móvil.

Instalar en el Smartphone un buen antivirus que pueda proteger al usuario de ciertas amenazas en la red, puede costar algo de dinero pero es mejor prevenir que lamentar debido a que día a día se está expuesto a miles de ataques que podrían ser fatales para el usuario final.

Otro factor importante como se mencionó en la sección anterior es mantener el software actualizado de cada uno de los dispositivos y del Smartphone debido a que las compañías y fabricantes con cada actualización van solucionando fallos y vulnerabilidades tanto de seguridad, como de interfaz y otros.

Es importante en cuanto a la configuración de la red modificar las contraseñas que vienen por defecto en los Routers, debido a que con la puerta de enlace si llegasen a tener las contraseñas por defecto, cualquier atacante podría entrar a la red.

En cuanto a las cámaras de seguridad que fueron implementadas en la Smart Home modelo, como se mencionó anteriormente estas van a ser una de las únicas que podrán tener acceso por el usuario desde otra red, por eso es importante mantener desactivada la opción “UniversalPlug&Play” debido a que de lo contrario quedarían expuestas a que terceros pudieran tener acceso a las cámaras de seguridad.

Identificar siempre que dispositivos y que usuarios están conectados a la red mediante software libre que se puede encontrar a la red, para así tener la garantía de que las únicas personas que estén conectadas a la red sean los miembros de la Smart Home, estas estarán definidas mediante una IP y el dispositivo desde el cual están accediendo a la red.

A la hora de instalar aplicaciones en el Smart Home, ha quedado claro que es uno de los dispositivos más importantes a la hora de mantener segura la Smart Home, es importante mantener la opción “No permitir instalación de terceros” activada en la configuración del dispositivo, y tener en cuenta que cada vez que se quiera instalar una aplicación revisar que permisos solicita esto, tener en cuenta que sería poco lógico que un juego de “carros” nos pidiera acceso a contactos, imágenes, realizar envío de mensajes etc.

6. CONCLUSIONES

Con base en el trabajo de este proyecto de investigación, se dio a entender la importancia de la seguridad y la privacidad de la información en la red, enfocada al caso de estudio de las Smart Homes, debido a que la pérdida o alteración de esta información podría afectar de manera fatal al usuario final perdiendo sus contraseñas de redes sociales, correos electrónicos, cuentas bancarias y lo que es aún peor dejando vulnerable la automatización de todos los dispositivos y sensores de Internet de las Cosas en la Smart Home.

Mediante los resultados obtenidos a lo largo del proyecto de investigación se logró resaltar que actualmente en Colombia no existen estándares de seguridad que le permitan al usuario final tener la garantía de que los dispositivos IoT o sensores que están adquiriendo vienen con parámetros de seguridad que permitan proteger dicha información.

Entre los diferentes aspectos revisados, se pudo tener como base que las soluciones que ofrecen algunas empresas actualmente para garantizar seguridad y privacidad al Internet de las Cosas aún son muy básicas, es decir que su falta de tecnologías y protocolos en la implementación no dan la seguridad total de ser una solución eficiente.

Con base al trabajo de investigación se pudo apreciar que es importante la seguridad tanto a nivel software como hardware, que los dispositivos o sensores siempre deberán estar actualizados constantemente, también la importancia de la red, el acceso a esta y toda la información que será almacenada en estos dispositivos.

A partir de las tecnologías, protocolos e implementación tanto de tipo Software y Hardware se seleccionaron las adecuadas para lograr tener un escenario seguro de Internet de las Cosas para las Smart Homes, donde el usuario pueda tener la tranquilidad de que toda la información que este viajando a través de la red, será de una manera cifrada, que requiere diferentes tipos de autentificaciones para que un tercero o un atacante pudiera llegar a tener acceso a esta.

Sin embargo como se mencionó anteriormente, uno de los eslabones de la seguridad más vulnerable son los usuarios finales ya que muchos de estos, no tienen en cuenta las recomendaciones mínimas de seguridad para no verse vulnerables frente a ataques, para esto se realizó una pequeña sección de buenas prácticas que los usuarios deberían tener en cuenta a la hora de buscar seguridad y privacidad de sus datos, ya que con el solo hecho de que un atacante pueda tener acceso al Smartphone asociado a la automatización de los servicios de la Smart Home podría estar controlando elementos muy importantes como el monitoreo de las cámaras de seguridad tanto exteriores como interiores en

tiempo real, la apertura del garaje eléctrico y la extracción de información confidencial que este viajando a través de la red.

Aun así sigue siendo importante la implementación de estándares y/o normas que puedan definir parámetros básicos de seguridad en el contexto colombiano para los desarrolladores o fabricantes, debido a que actualmente en el país no se está teniendo en cuenta aun la importancia, y los riesgos que esto podría traer de no cambiar en un periodo cercano.

Teniendo en cuenta la revisión de la literatura en cuanto a artículos científicos se tuvo como resultado que las investigaciones que tienen que ver con seguridad en Internet de las Cosas son nulas, lo que permite reflejar el desinterés actual por el tema.

Para concluir en un apropiado despliegue de un escenario seguro de Internet de las Cosas en las Smart Homes es importante tener en cuenta los protocolos y tecnologías requeridas para garantizar la seguridad en la red, tener en cuenta como usuario final que el hecho de que se tenga una apropiada implementación de seguridad no significa que se deben dejar de lado las buenas prácticas para mantener el sistema seguro, también es importante que se mantenga el firmware actualizado periódicamente, para lograr tener como usuario final una garantía de un escenario seguro de Internet de las Cosas aplicado Smart Homes.

7. TRABAJO FUTURO

La elaboración del trabajo de investigación “Solución tecnológica de Internet de las Cosas aplicado Smart Homes seguras” busca presentar las tecnologías, protocolos, requerimientos de tipo Software y Hardware para el diseño de un escenario seguro de Smart Homes. Este proyecto sirve como base para futuros proyectos de investigación que encuentren interés en el tema de Internet de las Cosas seguro aplicado a Smart Homes favoreciendo su ágil despliegue a nivel nacional e internacional.

Referencias

- Albarrán, C. (2015).
- Alohali, B. M. (2014). A secure scheme for a smart house based on Cloud of Things (CoT). . In Computer Science and Electronic Engineering Conference (CEEC), 2014 6th (pp. 115-120). IEEE.
- Amadeo, M. C. (2015). Information Centric Networking in IoT scenarios: The case of a smart home. In Communications (ICC), 2015 IEEE International Conference on (pp. 648-653). IEEE.
- ANSIX9.63. (2001). *DEVELOPMENT OF CORE ECC STANDARDS BY ANSI*. Obtenido de https://www.certicom.com/index.php/development-of-core-ecc-standards-by-ansi
- *Asociacion Española Para La Calidad*. (2015). Obtenido de http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion
- ATMEL. (2016). Obtenido de http://www.atmel.com/products/security-ics/embedded/default.aspx
- BdigitalStudio. (2015).
- Castonguay, A. (2016). *La importancia de la regulación en la IoT en Latinoamérica.*
- Chen, J. J. (2015). Design and Realization of an NFC-Driven Smart Home System to Support Intruder Detection and Social Network Integration. *Journal of Electronic Science and Technology, 2, 014.*
- ESET. (2014). *We live security*. Obtenido de http://www.welivesecurity.com/la-es/2014/07/31/internet-de-las-cosas-dispositivos-vulnerables/
- Evans, D. (2011). *Cisco.* Obtenido de http://www.cisco.com/c/dam/global/es_es/assets/executives/pdf/Internet_of_Things_IoT_IBSG_0411FINAL.pdf
- Forum, F. T. (21 de 09 de 2016). Obtenido de https://www.fundacionbankinter.org/documents/20183/42758/PDF+Resumen+Ejecutivo-+Internet+de+las+cosas/9c2a8598-3330-453a-b28e-758934877b52

- Gaikwad, P. P. (2015). A survey based on Smart Homes system using Internet-of-Things. .
- Hostalia. (2013). Obtenido de http://pressroom.hostalia.com/white-papers/configurar-protocolo-ssh
- IEEE802.15.4. (2006). *IEEE 802.15 WPAN*. Obtenido de http://www.ieee802.org/15/pub/TG4.html
- ISO. (2004). *A Summary of RFID Standards*. Obtenido de http://www.rfidjournal.com/articles/view?1335/2
- ITU. (2012). *UIT-TY.2060.*
- Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, 719-733.
- Kim, J. T. (2015). Attack Model on Smart Home Network under Internet on Things Surroundings.
- Koehler, M. &. (2014). Making Effective Home Security Available to Everyone-Towards Smart Home Security Communities. In Internet of Things. IoT Infrastructures (pp. 312-317). Springer International Publishing.
- Madakam, S. &. (2014). Smart Homes (Conceptual Views). In Computational and Business Intelligence (ISCBI), . 2014 2nd International Symposium on (pp. 63-66). IEEE.
- Microsoft. (2016). *Azure*. Obtenido de https://azure.microsoft.com/es-es/documentation/articles/iot-hub-security-architecture/
- MINTIC. (2015). *Boletín Trimestral de las TIC. Cifras cuarto trimestre de 2015.* Bogotá D.C. Obtenido de http://colombiatic.mintic.gov.co/602/articles-15179_archivo_pdf.pdf
- MOCANA. (2016). Obtenido de https://www.mocana.com/
- Molina, J. C. (24 de Septiembre de 2015). *Universidad de Antioquia*. Recuperado el 10 de Octubre de 2015, de http://educacion.udea.edu.co/notieducacion/?q=node/828
- Nadargi, A. &. (2016). Addressing Identity and Location Privacy of Things for Indoor—Case Study on Internet of Everything's (IoE).
- OASIS. (2014). *MQTT Version 3.1.1*. Obtenido de http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

- Peak, G. (2016). Obtenido de http://www.greenpeak.com/Application/SmartHome.html
- Pubnub. (2015). Obtenido de https://www.pubnub.com/wp-content/uploads/2015/04/Screen-Shot-2015-04-29-at-1.49.13-PM.png
- RealGames. (2016). Obtenido de https://realgames.co/documentation/display/HIO/Installation
- RFC4253. (2006). *The Secure Shell (SSH) Transport Layer Protocol*. Obtenido de https://tools.ietf.org/html/rfc4253
- RFC5246. (2008). *The Transport Layer Security (TLS) Protocol*. Obtenido de https://tools.ietf.org/html/rfc5246
- RFC6176. (2011). *Prohibiting Secure Sockets Layer (SSL) Version 2.0*. Obtenido de https://tools.ietf.org/html/rfc6176
- RFC6282. (2011). Obtenido de https://tools.ietf.org/html/rfc6282
- RFC6347. (2012). Obtenido de https://tools.ietf.org/html/rfc6347
- RFC7252. (2014). *The Constrained Application Protocol (CoAP)*. Obtenido de https://tools.ietf.org/html/rfc7252
- Rouse, M. (2014). *Search Data Center*. Obtenido de http://searchdatacenter.techtarget.com/es/definicion/Privacidad-de-datos-privacidad-de-informacion
- Rouse, M. (2015). Obtenido de http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security
- Santoso, F. K. (2015). Securing IoT for smart home system. In Consumer Electronics (ISCE), . 2015 IEEE International Symposium on (pp. 1-2). IEEE.
- *Smart Home Usa*. (2016). Obtenido de http://www.smarthomeusa.com/smarthome/.
- SmartHome. (2016). Obtenido de http://www.smarthome.com/lights-appliances.html?p=2
- SmartHomesStore. (2016). Obtenido de http://www.smarthome.com/
- Suresh, P. D. (2014). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In Science Engineering and Management Research (ICSEMR), 2014 Internat.

- Symantec. (2016). Obtenido de https://www.symantec.com/es/mx/iot/
- Telefonica. (2016). Obtenido de https://www.security.telefonica.com/es/services/cybersecurity/iot-security/
- Urien, P. (2016). Innovative DTLS/TLS security modules embedded in SIM cards for IoT trusted and secure services.
- Vinayaga Sundaram, B. R. ((2015, March).). Encryption and hash based security in Internet of Things. In Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference on (pp. 1-6). IE.
- Wang, M. Z. (2013). An IoT-based appliance control system for smart homes. In Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on (pp. 744-747). IEEE.
- Yoon, S. P. (2015). Security issues on smarthome in IOT environment. . In Computer Science and its Applications (pp. 691-696). Springer Berlin Heidelberg.