 Universidad Francisco de Paula Santander Ocaña - Colombia Vigilada Mineducación	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	Documento	Código	Fecha	Revisión
	FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	F-AC-DBL-007	10-04-2012	A
	Dependencia	Aprobado		Pág.
DIVISIÓN DE BIBLIOTECA		SUBDIRECTOR ACADEMICO		1(1)

RESUMEN – TRABAJO DE GRADO

AUTORES	LAURA MARCELA PÉREZ SÁNCHEZ
FACULTAD	INGENIERIAS
PLAN DE ESTUDIOS	INGENIERÍA DE SISTEMAS
DIRECTOR	TORCOROMA VELASQUEZ PÉREZ
TÍTULO DE LA TESIS	GUÍA DE BUENAS PRÁCTICAS EN TORNO A LA SEGURIDAD DE IOT PARA LAS SMART HOUSE.

RESUMEN

(70 palabras aproximadamente)

GUÍA DE BUENAS PRÁCTICAS EN TORNO A LA SEGURIDAD DE IOT PARA LOS DISPOSITIVOS QUE SE INVOLUCRAN CON LAS SMART HOUSE. SE PARTE DE UN ESTUDIO DE LAS CAPAS Y LOS PROTOCOLOS EXISTENTES EN IOT, EL PROYECTO OWASP Y LA ESTRUCTURACIÓN DE LOS COMPONENTES QUE CONFORMAN LA GUÍA. ESTA INVESTIGACIÓN PERMITE HACER UN APOORTE CON UN ANÁLISIS DEL FUTURO DEL INTERNET DE LAS COSAS Y EXPONER LAS CONSIDERACIONES SOBRE LA SEGURIDAD QUE INVOLUCRAN A ESTOS DISPOSITIVOS, TOMANDO COMO GUÍA LAS HERRAMIENTAS, DOCUMENTOS E INFORMACIÓN QUE PROPONE OWASP PARA EL DESARROLLO DE SISTEMAS DE ALTA CALIDAD EN SEGURIDAD.

COMO RESULTADO DE ESTA INVESTIGACIÓN SE DESEA PROPONER: UNA GUÍA DE BUENAS PRÁCTICAS EN TORNO A LA SEGURIDAD IOT PARA LAS SMART HOUSE.

CARACTERÍSTICAS

PÁGINAS: 121	PLANOS: 0	ILUSTRACIONES: 10	CD-ROM: 1
---------------------	------------------	--------------------------	------------------



GUÍA DE BUENAS PRÁCTICAS EN TORNO A LA SEGURIDAD DE IOT PARA LAS
SMART HOUSE

Autor:

LAURA MARCELA PÉREZ SÁNCHEZ

Anteproyecto realizado como requisito para optar por el título de Ingeniero de Sistemas

Director:

PhD. TORCOROMA VELASQUEZ PÉREZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIA

INGENIERIA DE SISTEMAS

Ocaña, Colombia

Julio de 2019

Dedicatoria

Dedico este logro principalmente a Dios, por haberme dado la oportunidad de nacer, de vivir, estudiar y permitirme llegar hasta este momento tan importante en mi formación como profesional que le suman un punto más a mi proyecto de mi vida.

A mis padres; Sergio Pérez Arévalo y a María Erika Sánchez, por ser quienes se encargaran de mi formación personal, académica, espiritual y por su apoyo incondicional en este tiempo.

A mi hermana Mariana Pérez Sánchez quien ha sido el ser más importante en mi desarrollo como persona, demostrándome siempre su cariño y apoyo incondicional. A mi sobrina Ariana Sofía por llenarme de mucha alegría.

Mis abuelos Ángel María Pérez (QEPD), Rosalía Arévalo y Dora Sánchez, por quererme y apoyarme siempre.

¡GRACIAS A TODOS!

Agradecimientos

Primeramente, a Dios por ser mi guía, por darme la capacidad, la fuerza, la valentía y la sabiduría para cumplir este uno de mis propósitos en mi proyecto de vida y lograr mi formación profesional para ser Ingeniera de Sistemas.

Agradezco enormemente a todas las personas que me han ayudado y apoyado a lo largo de estos años de carrera profesional. A mis padres y familiares por ser ellos quienes me impulsaron, me apoyaron, y me guiaron en este proceso para dar por terminada esta parte de mi proyecto de vida.

A los Ingenieros, Alveiro Alonso Rosado Gómez, Eduar Bayona Ibáñez, Andrés Mauricio Puentes Velásquez, Fabián Cuesta Quintero, Byron Cuesta Quintero, Magreth Rossio Sanguino y demás docentes que contribuyeron en gran parte en mi formación académica y profesional.

A la ingeniera Torcoroma Velásquez Pérez, quien, con su conocimiento, experiencia hizo su aporte significativo a mi interés por investigar, me asesoro en todo lo necesario para el desarrollo de mi proyecto.

A mi amigo Jesús Alberto Camargo Pérez, quien con su capacidad, habilidad, conocimiento y paciencia me guio en este proceso para que yo ampliara mis conocimientos, descubriera el mundo de la investigación, y lograra llevar a cabo el desarrollo de este proyecto.

Índice

Capítulo 1. Guía de buenas prácticas en torno a la seguridad de IoT para las Smart House.....	1
1.1 Planteamiento del problema.....	1
1.2 Formulación del problema	4
1.3 Objetivos	4
1.3.1 Objetivo general	4
1.3.2 Objetivos específicos.....	4
1.4 Justificación.....	5
1.5 Delimitaciones.....	7
1.5.1 Geográfica	7
1.5.2 Temporal.....	7
1.5.3 Conceptual.....	7
1.5.4 Operativo.....	7
Capítulo 2. Marco referencial	8
2.1 Marco histórico	8
2.1.1 Origen de los sistemas de información.....	8
2.1.2 Origen del Internet.....	9
2.1.3 Origen del Internet de las Cosas.....	9
2.2 Marco conceptual	10
2.2.1 Internet de las Cosas.....	10
2.2.2 Cloud Computing	11
2.2.3 Datos abiertos.....	11
2.2.4 Smart Cities.....	11
2.4.5 Modelos de despliegue	11
2.4.6 Cobit 5.0.....	12
2.4.7 ISO 30141.....	12
2.4.8 ISO 27001.....	13
2.4.9 Tratamiento de Datos.....	13
2.4.10 IEEE 2030.5.....	13

	viii
2.3 Marco teórico	13
2.3.1 Desafíos en la seguridad del IoT	13
2.3.2 Entendiendo las tres capas básicas del Internet de las Cosas	14
2.3.3 Principales barreras al IoT.....	15
2.3.4 Elementos de Seguridad.	16
2.3.5 Analisis Sistemático del Internet de las Cosas.	17
2.3.7 OWASP	19
2.4 Marco legal.....	20
Ley1273 de 2009.	21
Capítulo 3. Diseño Metodológico	23
3.1 Diseño Metodológico	23
3.1.1 Teoría Fundamentada	24
3.1.2 Características de quien trabaja con la teoría fundamentada.....	24
3.1.3 Calidad en teoría fundamentada	25
3.1.4 Técnicas de Recolección de la Información	25
3.1.5 Analisis de la Información.....	26
Capítulo 4. Resultados	27
5.1 Estudio de las capas de IoT	27
5.1.1 características generales del IO	27
5.1.2 Identificar el modelo de dispositivos IOT	32
5.1.3 Recopilar la información relacionada con las capas IoT	33
5.1.4 Analizar los protocolos utilizados en IoT.....	39
5.2 Proyecto OWASP de IoT	43
5.2.1 Recolectar la información relacionada con el proyecto OWASP de IoT	43
5.2.2 Identificar los marcos establecidos por el proyecto OWASP de IoT	46
5.3 Guía de buenas prácticas para los desarrolladores de sistemas IoT SmartHouse basados en el proyecto OWASP de IoT	49
Conclusiones	104
Recomendaciones	105

Lista de Figuras

Ilustración 1. Fases del IO.....	2
Ilustración 2: Capas del IoT.....	15
Ilustración 3. Elementos de Seguridad IoT.....	17
Ilustración 4. Características de los sistemas IO.....	19
Ilustración 5. Soluciones de seguridad en las comunicaciones.....	31
Ilustración 6. Bordes y Protocolos en una infraestructura IoT.....	34
Ilustración 7. Top 10 del IoT.....	45
Ilustración 8. Marcos de Seguridad establecido por el proyecto OWASP IoT.....	47
Ilustración 9. Evaluación de sistemas IoT Smart House.....	56
Ilustración 10. Analisis Bibliometrico.....	112

Lista de Tablas

Tabla 1: Requisitos de la IO	29
Tabla 2: Características de las comunicaciones.....	30
Tabla 3: Consideración de seguridad de IoT	46
Tabla 4: Evaluación de sistemas IoT Smart House.....	50
Tabla 5: Controles a Aplicar.....	57
Tabla 6: Consideraciones de Seguridad IoT – Controles.....	52

Capítulo 1. Guía de buenas prácticas en torno a la seguridad de IoT para las Smart House

1.1 Planteamiento del problema

El internet se construye a partir de 1969 cuando se estableció la primera red de computadores; aunque realmente esta gran era comienza en 1994 cuando se ofrece el servicio de (world wide web). Internet básicamente habla de una red de redes de ordenadores capaces de comunicarse entre ellos, entre otros conceptos el internet hace referencia a todos los dispositivos tecnológicos que de alguna manera se pueden conectar a la red y con los cuales se interactúa ya sea con el móvil o desde el computador, se define como cualquier cosa que se encuentra conectada a internet, esta se puede definir como una red altamente interconectada de entidades heterogéneas, tales como, etiquetas, sensores, dispositivos embebidos, dispositivos portátiles, entre otros, que interactúan y se comunican entre sí en tiempo real (Malina, Hajny, Fujdiak, & Hosek, 2016; Zhang & Green, 2015).

La Smart House se entiende como un hogar apoyado en la tecnología que da respuestas al confort que hoy en día exigen sus habitantes, dando al concepto de sostenibilidad no solo como una significación ambiental sino una noción económica, y planteando un modelo que puede ser extensivo a otros ámbitos de relación del ciudadano (Quesada & Pulido, n.d.), lleva por nombre casas inteligentes pues es una casa con un diseño arquitectónico y una tecnología avanzada que permite a las personas o familias alojarse en el interior de ellas y que al mismo tiempo se sientan seguros, relajados y satisfechos.

En la IO, cada aplicación se basa en su propia infraestructura TIC y en dispositivos dedicados, estos dispositivos no comparten ninguna característica para la gestión de servicios y

redes, lo que aumenta los costos. Las ciudades inteligentes buscan un enfoque flexible y horizontal, en el que la plataforma operativa común gestionara la red y los servicios, lo que permitirá abstraer un amplia gama de fuentes de datos para permitir que las aplicaciones funcionen correctamente, estas ya no funcionarían de forma aislada, sino que compartirían elementos de infraestructura, medio ambiente, red, y una plataforma de servicios comunes. Estas aplicaciones cuentan con una serie de fases que tienen lugar en la interacción entre el mundo físico-virtual:



Ilustración 1. Fases del IO

Nota. Fuente: Elaboración propia, Recuperada de (Borgia, 2014)

Cada una de estas fases se caracterizan por la diferenciación y la interacción de protocolos, estos tienen diferentes propósitos y funciones (Borgia, 2014).

La seguridad, la privacidad y la protección de la información son las preocupaciones fundamentales de los fabricantes de dispositivos IoT, pues no se tiene un alto grado de confiabilidad respecto a los estándares de seguridad, un nivel de seguridad bajo es claramente

inaceptable para los servicios domiciliarios en materia de seguridad operacional y salud de las personas. Por ejemplo, cuando nos salimos por algún tiempo, servicios innecesarios como aire acondicionado, luces, gas y otros electrodomésticos se pondrá en modo de espera o se apagará para ahorrar energía y proteger la seguridad de la casa, sin embargo, los atacantes puede enviar maliciosamente desde el exterior muchas peticiones falsas a algún dispositivo específico o servicio en la nube, por lo que amenaza seriamente la seguridad de la vivienda (tao, 2016).

Entre las principales características de la IO, se encuentra la seguridad esta es fundamental ya que pueden producirse a distintos niveles, invirtiendo tanto en tecnología como en aspectos éticos y de seguridad. Estas cuestiones de seguridad son de vital importancia ya que busca garantizar la seguridad de los datos, los servicios y todo el sistema de IO, en todo esto se presenta una serie de propiedades como; confidencialidad, integridad, autenticación, autorización, no repudio, disponibilidad y privacidad deben estar garantizados para ofrecer dispositivos altamente seguros (GhaffarianHoseini, Dahlan, Berardi & Makaremi, 2013).

Un estudio realizado por HP (Hewlett-Packard, 2015) arrojo que un 70% de los dispositivos de IoT no cifran sus comunicaciones, este porcentaje permite a un atacante identificar las cuentas de usuario válidas, el 60% de los que tienen interfaz de usuario son vulnerables a distintos ataques como secuencias de comandos en sitios cruzados (XSS). Considerando que estos dispositivos recopilan una gran cantidad de información sensible para los usuarios, esto se vuelve un gran riesgo de seguridad (Rahman et al., 2016). Por lo que se hace necesario proteger dichos dispositivos.

Es por esta razón que dentro de esta investigación se hace necesario abordar cada una de las fases del internet de las cosas, con el fin de analizar y estudiar cada una de ellas en relación a la seguridad, tomando como guía OWASP (Proyecto de seguridad de aplicaciones web abiertas), siendo este una organización que busca mejorar la seguridad del software, proporcionando herramientas de software y documentación basada en el conocimiento sobre la seguridad de las aplicaciones. Apoyándonos en OWASP, se propone el diseño de una guía que evalúe los problemas de seguridad a los que se enfrentan a diarios los dispositivos IoT.

1.2 Formulación del problema

¿Cuáles son los componentes que debe tener una guía de buenas prácticas para mejorar la seguridad en IoT?

1.3 Objetivos

1.3.1 Objetivo general. Proponer una guía de buenas prácticas entorno a la seguridad IoT para los dispositivos que se involucran con las SmartHouse.

1.3.2 Objetivos específicos.

Realizar un estudio de las capas de IoT.

Estudiar el proyecto OWASP de IoT

Diseñar la guía de buenas prácticas para los desarrolladores de sistemas IoT para SmartHouse basado en el proyecto OWASP IoT.

1.4 Justificación

Las tecnologías de la Información y comunicación se han convertido en una herramienta indispensable para el intercambio de información (Unión Internacional de Telecomunicaciones (UIT) - Ministerio de Ciencia y Tecnología), la convergencia de servicios televisión, telefonía, mensajería entre otros hacia una única red de comunicaciones hace que el Internet sea parte fundamental de nuestra vida cotidiana. El internet de las cosas es una innovación tecnológica que nos permitirá transformar todos nuestros objetos en “Smart-objetos”. Todas las cosas que nos rodean estarán conectadas en red transmitiendo y recibiendo información para facilitarnos la vida y volverla más eficiente, ya sea en consumos energéticos, en administración de finanzas e incluso en la utilización de nuestro tiempo (Gutiérrez, 2013). El internet de las cosas comienza a tener una gran acogida cada vez más en la población a nivel mundial, nacional y local, donde se implementan nuevas innovaciones tecnológicas para facilitar el diario vivir, es por esta razón que este ha tenido una aceptación extraordinaria en ese contexto.

La Internet de las cosas posee una serie de características en las que se encuentra; la inteligencia artificial, la conectividad, los sensores, la participación activa y el uso de implementos pequeños. Estas características permitirán el diseño de dispositivos confiables, ya que la IO se está convirtiendo categóricamente en una realidad (Chandra, Kumar, & Sureshabu, 2018). La IO habilitada con sistema de seguridad inteligente, permite a los usuarios monitorear

los parámetros de la casa como; la temperatura, el humo y la intensidad de luz. Estos pueden controlarse mediante la recolección y el intercambio de datos.

De igual manera así como se pueden obtener una gran cantidad de beneficios al implementar el internet de las cosas, también existen desafíos. En el momento en que un objeto se vuelve parte de un entorno interconectado, se hace necesario determinar si este dispositivo ha perdido seguridad física o lógica, ya que posiblemente se encontraran localizados en entornos poco seguros, lo cual facilitara a los individuos que esperan por hacer ataques malintencionados, estos atacantes podrían acceder a gran parte de la información que contienen los dispositivos, modificando la misma, incluso llegar a manipular el sistema de control y modificar la funcionalidad de estos. Las soluciones que proponen expertos para mejorar la seguridad son la autenticación y autorización segura, especialmente en tarjetas SIM, arranque seguro de objetos y transmisión de datos esta solución propone que se incluya la instalación y configuración de credenciales, claves y certificados en los dispositivos, la seguridad de los datos de la IO se refiere al proceso que garantiza almacenar y transmitir la información dentro del entorno de la IO por el ultimo propone el acceso seguro a los datos esta característica permite que solo los usuarios autorizados puedan acceder a algunos datos determinados (Borgia, 2014).

En consecuencia, dicha investigación permite hacer un aporte con un análisis del futuro del internet de las cosas y exponer las consideraciones sobre la seguridad que involucran a estos dispositivos, tomando como guía las herramientas, documentos e información que propone OWASP para el desarrollo de sistemas de alta calidad en seguridad, se propone el análisis de lo que plantea OWASP para llevar a cabo el desarrollo de la guía. Como resultado de esta

Investigación se desea proponer: una guía de buenas prácticas en torno a la seguridad IoT para las Smart House.

1.5 Delimitaciones

1.5.1 Geográfica. Esta investigación o estudio se realizara en un contexto Internacional haciendo uso de la organización OWASP (Proyecto de seguridad de aplicaciones Web abiertas), que permite a las organizaciones que conciban, desarrollen, adquieran y mantengan aplicaciones confiables.

1.5.2 Temporal. El proyecto se realizara dentro de un periodo de 2 a 6 meses a partir de la fecha de aprobación del proyecto.

1.5.3 Conceptual. Se abordaran conceptos como: IoT (Internet de las cosas), ataques, seguridad, amenaza, Norma ISO/IEC 30141, Cobit 5.0, ISO 27001, guía, Smart House (definición y características), arquitectura, capas IoT, OWASP.

1.5.4 Operativo. Para el cumplimiento al proyecto es posible que se tengan dificultades al realizar acercamientos viviendas que sean inteligentes, estos elementos se encuentran a nivel nacional.

Capítulo 2. Marco referencial

2.1 Marco histórico

2.1.1 Origen de los sistemas de información.

Barcos (2008), afirma que los sistemas de información se originan cuando:

Los líderes, administradores y dirigentes de la antigüedad y de distintas culturas tanto europeas como americanas; incluso precolombinas, que, obviamente, no poseían los medios actuales reconocían el valor de la información y la imposibilidad de adoptar decisiones sin información confiable, comprensible y oportuna (Pag 1).

Si bien todas las organizaciones a nivel mundial tienen claro que la información es sumamente valiosa, pues esta es la que permite la toma de decisiones estratégicas con base en información almacenada y tratada a través de los diferentes sistemas de información. De lo anterior, la pontificia universidad Javeriana ratifica en el segundo encuentro Colombiano de Gestión Universitaria que “los sistemas de información son un factor estratégico en la gestión universitaria” (Javeriana, 2013), gracias a que cumplen una función en común y es hacer unir diferentes partes para lograr una meta en común y es la toma de decisiones estratégicas desde cualquier punto.

En Argentina en la universidad institucional de la UNLP (Universidad Nacional de la Plata), se propone el diseño y construcción de sistema de IoT seguros escalables, en ella se propone realizar una línea de investigación que aborde el diseño y construcción de sistemas de IoT escalables y seguros, teniendo en cuenta que un sistema IoT está conformado por personas y por dispositivos compuestos por sensores y actuadores, en el cual cada una de estas partes

Interactúan entre sí, manteniendo un cierto grado de independencia para el correcto funcionamiento del sistema. (Flores, Berón, Riesco, & Rangel Henriques, 2018)

A nivel nacional la universidad pontificia Bolivariana propone la construcción de una guía para implementar controles de seguridad al almacenar datos sensibles en la nube, en esta se plantea la protección de datos (Información) el principal componente ya que esto ha sido un reto para los especialistas de seguridad de la información y sigue intensificando con la aparición de nuevas tecnologías, como el internet de las cosas (IOT) y servicios tecnológicos albergados en la nube. En esta guía se plantea la ley 1581 de 2012, incluye aspectos relevantes tópicos sobre la protección de información sensible, en algunos casos administrada por empresas de mensajería en territorio colombiano, las cuales se encuentran reglamentadas según la ley postal colombiana (Castañeda Sandoval & Comunicación, 2018)

2.1.2 Origen del Internet. La guerra ha contribuido a desarrollar invenciones que luego resultan útiles para la humanidad, el internet es una de estas, pues en el caso de la Guerra Fría (El periodo de tensiones entre Estados Unidos y el bosque soviético), las dos superpotencias participaban en la escalada atómica. Al tiempo, la carrera espacial no podía esconder, bajo sus llamadas a la aventura, el interés estratégico de la ocupación del espacio. En toda guerra la información es vital, y precisamente el origen de Internet fue la necesidad de un sistema de comunicaciones que sobreviviera a un conflicto. (Historia de la Internet, n.d.)

2.1.3 Origen del Internet de las Cosas. La idea de poder conectar objetos y que estos fueran inteligentes fueron pronosticadas por Nikola Tesla en 1926, este científico anticipó de forma sorprendente el crecimiento y la evolución de la conectividad a nivel global y el desarrollo de dispositivos que incorporarían piezas mínimas. Más adelante Alan Turing en 1950, hace un

aporte significativo en el que se deduce que tan grande será el avance tecnológico se verá la necesidad de dotar de inteligencia y capacidades de comunicación a los dispositivos. Ashton en uno de sus artículos expone el origen del internet de las cosas de la siguiente forma:

“Si tuviésemos ordenadores que fuesen capaces de saber todo lo que pudiese saberse de cualquier cosa usando datos recolectados sin intervención humana seríamos capaces de hacer seguimiento detallado de todo, y poder reducir de forma importante los costes y malos usos.

El **Internet de las Cosas** tiene el potencial de cambiar el mundo como ya lo hizo Internet. O incluso más.” (Partner, 2011)

Kevin Ashton, es la persona que acuñó el término “internet de las cosas” (IoT), que hoy se utiliza para referirse a un mundo en el que todo –la casa, los electrodomésticos, el carro, el mobiliario urbano, las máquinas de las fábricas estarán conectadas a internet. El objetivo es arrojar información en tiempo real que permita tomar decisiones (Partner, 2011). El internet de las cosas reside en la capacidad para combinar datos con personas, procesos y objetos. Esto con el fin de mejorar la calidad de vida de las personas al implementar esta tecnología que permitirá interactuar en tiempo real con todos los dispositivos que nos rodean, además potenciaran las ciudades, edificios y redes eléctricas, con el objetivo de aumentar la seguridad la información.

2.2 Marco conceptual

2.2.1 Internet de las Cosas. El Internet de las cosas se refiere a la presencia ubicua de sensores electrónicos en dispositivos como teléfonos inteligentes, vehículos, aparatos domésticos, sistemas de seguridad para el hogar, dispositivos de atención médica y monitores de acondicionamiento físico. Estos dispositivos basados en sensores generan información detallada sobre las personas involucradas en actividades cotidianas (Peppet, 2014).

Los avances en computación móvil, redes inalámbricas, dispositivos móviles y sistemas embebidos han dado lugar al paradigma de IoT el cual consiste en una infraestructura de red global y dinámica de nodos (things) interconectados, inteligentes y auto configurables.” IoT es un habilitador del ecosistema IoE (Internet of Everything) que permite no solo que las personas se interconecten y se comuniquen, sino que ahora también lo hacen los procesos, los datos y los objetos, convirtiéndose en sus cuatro pilares. Esta interrelación permite transformar la información en acciones que crean nuevas capacidades y experiencias” (Murazzo, Medel Fernández, & Rodríguez, 2016).

2.2.2 Cloud Computing. Gartner define la computación en la nube como “un estilo de computación en el cual las capacidades escalables y elásticas habilitadas por TI se entregan como un servicio usando tecnologías de internet” (Gartner, 2018).

2.2.3 Datos abiertos. Una variante muy importante de Big Data es la estrategia Open Data. “La estrategia de Open Data, que históricamente nació en 2009 en Washington, se refiere a la posibilidad de que el ciudadano acceda a los datos del gobierno que antes solo eran analizados en el interior de las administraciones públicas” (Aguilar L. J., 2013).

2.2.4 Smart Cities. Una ciudad inteligente además de digital es sustentable, ello implica que “los sistemas inteligentes se encuentren “embebidos” dentro de la infraestructura de la ciudad automatizando la entrega de la información y la entrega de los servicios básicos. Las ciudades inteligentes ofrecen una mejor oportunidad para atender los problemas urbanos tales como el medio ambiente, el transporte y la seguridad” (Casas Pérez, 2014).

2.4.5 Modelos de despliegue. Hacen referencia al tipo de nube que se van a usar para desplegar los servicios, los cuales pueden ser PRIVADA en donde los recursos proporcionados

son exclusivamente para uso de quien los contrata, PUBLICA donde los recursos utilizados son propiedad de un gran distribuidor y la información se coloca allí con acuerdos públicos, en la nube COMUNITARIA los recursos se comparten con comunidades que por lo general buscan el mismo fin, HIBRIDA es un conjunto seleccionado de los modelos anteriores definido por necesidades o fines específicos. (Areitio, 2011).

Por otro lado, los modelos de servicio tienen que ver con el tipo de infraestructura o plataforma en donde deseamos implementar los servicios, así que podemos encontrar:

- SaaS: Software como Servicio, consiste en proveer al usuario final una sencilla plataforma para que use los servicios alojados en el proveedor.
- PaaS: Plataforma como Servicio, proporciona al consumidor recursos con capacidad para desplegar en los servicios que prestara y de las cuales tiene el control.
- IaaS: Infraestructura como Servicio, el consumidor cuenta con recursos de procesamiento, almacenamiento y puede proveer más recursos para poder configurar múltiples plataformas de servicios.

2.4.6 Cobit 5.0. Se define como un marco de buenas prácticas para el gobierno empresarial de TI (De Haes, Van Grembergen, & Debrecey, 2013). Este marco permite a través de principios básicos obtener conocimiento de la literatura relacionada con TI, en él se describen las principales direcciones y los principios fundamentales del marco.

2.4.7 ISO 30141. Norma sobre el Internet de las Cosas (IoT) – Arquitectura de Referencia, esta norma proporciona un vocabulario común para diseñar y desarrollar aplicaciones de IoT. Con esta norma se pretende reforzar la seguridad y la protección de los datos, permitiendo desplegar sistemas fiables y respetuosos tanto con la privacidad como a la hora de afrontar

ataques (“Communications standards news,” 2015). Esta norma sirve de base para desarrollar aplicaciones relacionadas con la IO, además proporciona normas y orientaciones para el desarrollo de la arquitectura de la IO (ISO/IEC, 2016).

2.4.8 ISO 27001. Esta norma cuenta con 42 requisitos que debe cumplir el SGSI (Sistema de gestión de seguridad de la información) para poder obtener la certificación. Dentro de esta norma se tiene como punto focal el requisito para la planificación, implementación, operación, monitoreo y mejora continua de un SGSI orientado al proceso (Disterer, 2013).

2.4.9 Tratamiento de Datos. Los Estados establecen garantías para la tutela y protección de los derechos de las personas frente al tratamiento automatizado de los datos, lo que no se puede suponer es una barrera a la libre circulación de los datos, ya que como expone la Directiva “El nivel de protección de los derechos y libertades de las personas, se refiere al tratamiento de dichos datos” (Herrán Ortiz, 2002).

2.4.10 IEEE 2030.5. Se ejecuta a través del Protocolo de Internet (IP) para permitir una variedad de rutas de comunicación y capas de enlace. Además, el estándar está diseñado para ser liviano, lo que reduce el costo de integración del estándar en los productos de consumo, así como para habilitar aplicaciones que puedan ser alimentadas por batería. Y, por supuesto, IEEE 2030.5 está diseñado pensando en la seguridad, incorporando lo último en tecnología y mejores prácticas de ciberseguridad (“Communications standards news,” 2015).

2.3 Marco teórico

2.3.1 Desafíos en la seguridad del IoT. Según Zhang, en un artículo publicado en la IEEE se establecen los principales retos para la seguridad de la IO son la heterogeneidad y la gran

escala de los objetos (Zhang et al., 2014), entraremos en detalle sobre cada uno de ellos para conocer los desafíos a los que estos se enfrentan.

- **Identificación de objetos.** El principal reto es garantizar la integridad de los registros utilizados en la arquitectura de asignación de nombres. Aunque el Sistema de Nombre de Dominio (DNS) proporciona servicios de traducción de nombres a los usuarios de Internet, se trata de un sistema de nombres inseguro.
- **Autenticación y autorización.** Aunque los criptosistemas de clave pública tienen ventajas para construir esquemas de autenticación o sistemas de autorización, la falta de una autoridad de certificado raíz global (global root CA) dificulta la implementación de muchos esquemas teóricamente viables.
- **Privacidad.** Este tipo de desafíos puede dividirse en dos categorías: política de recopilación de datos y anonimización de datos. la política de recopilación de datos describe la política durante la recopilación de datos en la que se aplica en tipo de datos que se pueden recopilar y el control de acceso de una “cosa” a los datos, la anonimización de los datos, garantiza el anonimato de los datos, es deseable tanto la protección criptográfica como la ocultación de las relaciones de datos.

2.3.2 Entendiendo las tres capas básicas del Internet de las Cosas. Hasta ahora hemos visto cómo el fenómeno del Internet de las Cosas ha irrumpido a nuestro alrededor, dando vida a objetos cotidianos que se interconectan gracias a Internet y constituyen fuentes inagotables de información. Para entender el Internet de las Cosas desde un punto de vista más técnico es necesario comprender las tres capas que lo hacen realidad (Partner, 2011).

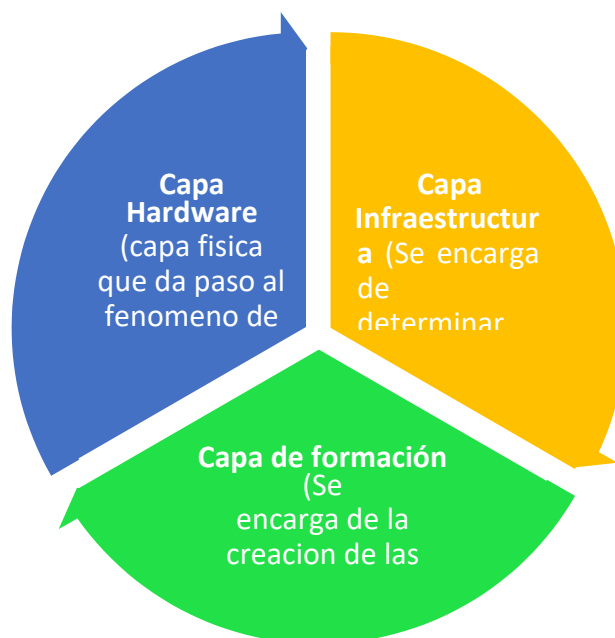


Ilustración 2: Capas del IoT

Nota. Fuente: (Partner, 2011)

2.3.3 Principales barreras al IoT. Los principales obstáculos para la adopción del Internet de las Cosas se pueden encontrar infinidad de problemas viéndolos desde varios puntos de vista, pero se los puede enmarcar en asegurar la privacidad y seguridad de las nuevas soluciones, y conseguir estándares globalmente aceptados (Press, n.d.).

Privacidad y seguridad. Hay una necesidad de tener una solución técnicamente para garantizar la privacidad y la seguridad de los clientes y de las empresas para poder tener una adopción generalizada de cualquier sistema de identificación de objetos. Mientras que en muchos casos se ha hecho la seguridad como una característica adicional, es la sensación que la aceptación pública de Internet de las Cosas ocurrirá sólo cuando las soluciones de seguridad estén en su lugar. La privacidad de la información juega un capítulo importante en las arquitecturas de IoT.

La comisión Europea y países como Estados Unidos han debatido este tema en el pasado analizando las consecuencias que la privacidad y seguridad genera en la creciente demanda de conectividad de las “cosas”. Las implicancias de no comprender la importancia en la seguridad o privacidad podría ser devastador en la arquitectura diseñada. Podrían verse afectados, por ejemplo, datos personales bancarios, de salud, etc. o información empresarial o de industrias, gobiernos, etc. El efecto o el riesgo dependen del contexto y la función que cumplen los datos generados por los sensores o dispositivos que están conectados a la red (IOT SIMPLE S.A.).

Gobernanza. Una barrera importante para la adopción generalizada de la tecnología de Internet de las Cosas es la ausencia de gobernabilidad. Sin una autoridad, similar a la que gobierna Internet, existen altas probabilidades que será imposible tener un verdaderamente global "Internet de las Cosas", también existe la necesidad de mantener la gobernabilidad como genérico como sea posible, como tener una autoridad por campo llevará sin duda a superposición, la confusión y la competencia entre las normas.

2.3.4 Elementos de Seguridad. Amazon aprovecha una arquitectura de seguridad multicapa para AWS (Amazon Web Security), en la que la seguridad se aplica en todos los niveles de tecnología (Ammar, Russello, & Crispo, 2018) se basa en los siguientes elementos:

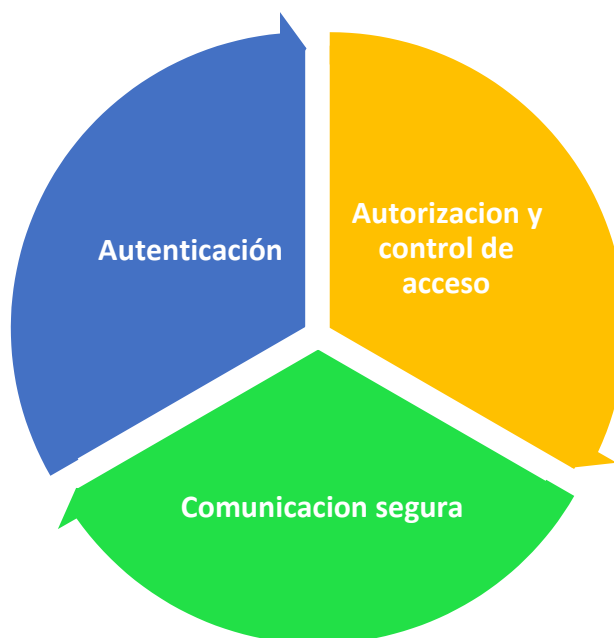


Ilustración 3. Elementos de Seguridad IoT

Nota. Fuente: (Ammar et al., 2018)

2.3.5 Análisis Sistemático del Internet de las Cosas. En Argentina, en la Universidad Nacional de la Plata, se realizó un análisis sistemático de la seguridad en internet de las cosas, en este se define que el Internet of Things (IoT, siglas en inglés) es una innovación tecnológica con gran auge en la actualidad debido a la incorporación en múltiples sectores en la sociedad como en la salud (Smart Health), en la educación (Smart Education), en el hogar (Smart Home), en el transporte (Smart Transport), en la seguridad (Smart Security), en las ciudades (Smart City), entre otros sectores. IoT permite interconectar objetos integrados físicos (Smart Object) en diferentes redes de comunicación transmitiendo y recibiendo información. Sin embargo, debido a su evolución exponencial surge la problemática de la seguridad y privacidad que afecta directamente en el desarrollo y mantenimiento de la utilización sostenible de IoT.(Perez, Bustos, Berón, & Rangel Henriques, 2018)

2.3.6 Norma ISO 30141. Esta norma se define como una infraestructura de entidades físicas, sistemas y recursos de información interconectados junto con los servicios inteligentes que pueden procesar y reaccionar a la información tanto del mundo físico como del mundo virtual, esta norma cumple con tres objetivos:

1. describir las características de los sistemas IO
2. definir los ámbitos del sistema de IO
3. describir las vistas de la arquitectura de IO

La norma aborda las características de los sistemas IO, descritas a continuación:

1. Características del sistema IoT
2. Características del servicio IoT
3. Características del componente IoT
4. Compatibilidad
5. Usabilidad
6. Robustez
7. Seguridad
8. Protección de la información personal

La característica a aplicar es la seguridad, pues el análisis y estudio de la misma permitirá identificar de qué manera se llevan a cabo los marcos de seguridad en lo que respecta a la norma internacional, esta característica presenta una serie de componente a estudiar (ISO/IEC, 2016):



Ilustración 4. Características de los sistemas IO

Nota. Fuente: (ISO/IEC, 2016)

2.3.7 OWASP

La fundación OWASP se puso en línea en diciembre de 2001, se estableció como una organización sin ánimo de lucro en los Estados Unidos, esta es una organización internacional que busca mejoras en la seguridad de las aplicaciones. Por otra parte se considera una comunidad que ofrece; herramientas, documentos, foros y capítulos de OWASP gratuitos para mejorar la seguridad (“Acerca del proyecto Open Web Application Security - OWASP,” n.d.).

Con la guía que propone OWASP, basada principalmente en la seguridad del fabricante IoT, busca básicamente plantear una serie de categorías que van enlazadas directamente con el nivel básico de los dispositivos IoT, esta al mismo tiempo expone una serie de consideraciones y recomendaciones que permitirán realizar la guía de buenas prácticas entorno a la seguridad IoT,

tomando como referencia este proyecto que busca ayudar a los fabricantes a construir productos más seguros en el internet de las cosas (“Guía de seguridad de IoT - OWASP,” n.d.).

Se enfocara en proyecto OWASP IoT (Internet de las Cosas), básicamente viene muy alineado con la fundación OWASP, solo que este compre los problemas de seguridad asociados con la internet de las cosas, para permitir a los usuarios tomar las mejores decisiones de seguridad al crear, implementar o evaluar tecnologías de IoT (“Proyecto OWASP de Internet de las Cosas - OWASP,” n.d.).

2.4 Marco legal

La Ley 1581 de 2011 reglamentada mediante el decreto 1377 de 2013, reglamenta:

“Artículo 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 2. **Ámbito de aplicación.** Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. El régimen de protección de datos personales que se establece en la presente Ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. 21 Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control, del lavado de activos y el financiamiento del terrorismo.

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales.

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008. f) A las bases de datos y archivos regulados por la Ley 79 de 1993.” (Colombia. Congreso de la República, 2012)

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

LEY ESTATUTARIA 1581 DE 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

DECRETO 1377 DE 2013. Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Capítulo 3. Diseño Metodológico

Para llevar a cabo el presente proyecto se define el tipo de investigación, las técnicas y los procedimientos que serán utilizados para responder al problema planteado. Se plantea la metodología de tipo cuantitativo bajo los elementos teóricos que encierran la teoría fundamentada.

3.1 Diseño Metodológico

El desarrollo de este proyecto se fundamentara en una metodología descriptiva de corte cuantitativo basado en la teoría fundamentada, en el cual a partir del análisis documental se podrán establecer las mejores prácticas de seguridad IoT para las Smart House, teniendo en cuenta los elementos y barreras presentes en el IoT.

Por lo tanto, esta metodología consiste en caracterizar un fenómeno o situación concreta indicando sus rasgos más peculiares o diferenciales. Con este tipo de investigación se busca especificar y categorizar cada uno de los elementos y estrategias acorde a la seguridad en dispositivos IoT. Según (Tamayo, 1999), la investigación descriptiva “comprende la descripción, registro, análisis e interpretación de la naturaleza actual, composición o procesos de los fenómenos”, Según Sampieri, la investigación cuantitativa lleva consigo un proceso; deductivo, secuencial, probatorio y analiza una realidad objetiva (Geometry & Analysis, n.d.).

Para investigar cuantitativamente hay que centrarse dentro del contexto, por lo tanto esta investigación es exploratoria, entrando en contexto con las bases de datos digitales, libros, artículos, documentos, videos, tesis, resúmenes, que permitirán la obtención de conocimientos.

3.1.1 Teoría Fundamentada

La teoría fundamentada según la obra “The Discovery of Grounded Theory” (Glase Strauss, 1967), en su libro insisten en que teoría: a) se genera y emerge del campo, b) este fundamentada en el área substantiva, y c) se desarrolle inductivamente (Trinidad Requena, Carrero Planes, & Soriano Miras, 2006).

Autores como Charman (2005), manifiestan que la teoría fundamentada se concibe como un método de análisis definido con unas directrices que apoyan la investigación en su recolección sucesiva de información o datos y desarrollos conceptuales para la construcción de teorías.

Considerando las definiciones dadas, en lo que corresponde a este proyecto hace énfasis en que la teoría fundamentada es la metodología adoptada para el desarrollo del mismo donde a partir de una recolección consecutiva de información sobre el objeto de estudio, contribuya a la identificación de elementos que permitan establecer un modelo que cumpla con las políticas de seguridad establecidas en la constitución política colombiana y todos los entes que rigen la seguridad de la información, estableciendo una guía de buenas prácticas, donde se involucren los marcos de seguridad que propone OWASP de IoT.

3.1.2 Características de quien trabaja con la teoría fundamentada

1. Capacidad de mirar de manera retrospectiva y analizar las situaciones críticamente.
2. Capacidad de reconocer la tendencia a los sesgos.
3. Capacidad de pensar de manera abstracta.
4. Capacidad de ser flexibles y abiertos a la crítica constructiva.

5. Sensibilidad a las palabras y acciones de los que responden a las preguntas.

6. Sentido de absorción y devoción al proceso del trabajo.

3.1.3 Calidad en teoría fundamentada

La calidad en métodos cualitativos se puede abordar con los siguientes criterios:

- Credibilidad: la verdad de los hallazgos a través de los ojos del investigado o entrevistado y en el contexto en que se desarrolla la investigación.
- Transferibilidad: punto hasta el que los hallazgos pueden transferirse a otros contextos.
- Confiabilidad (dependability): grado en que la investigación produciría hallazgos similares y coincidentes si se llevara a cabo como está descrito.
- Confirmabilidad: evidencia que corrobore los hallazgos, proveniente de los sujetos y el contexto de investigación.

La calidad en la TF, según Glaser y Strauss (1967) radica en la adaptabilidad (fit), el trabajo, la relevancia y la modificabilidad; en tanto que para Strauss y Corbin (1990) existen 2 conjuntos de criterios: de proceso de investigación y de fundamentación empírica de los hallazgos, se puede afirmar que la teoría fundamentada promueve la investigación (de la Espriella & Gómez Restrepo, 2018).

3.1.4 Técnicas de Recolección de la Información

Por tratarse de una investigación con enfoque cuantitativo, bajo los preceptos de la teoría fundamentada, la recolección de la información se basará en instrumentos que faciliten la identificación de los marcos de seguridad de IoT. Los procedimientos de recolección de la información (bases de datos digitales, libros, videos y artículos),

permitirán situarnos en el contexto de los problemas que enfrenta la Seguridad IoT, la técnica exploratoria, consiste en indagar la información que va relacionada al objeto de estudio, para su posterior análisis.

3.1.5 Análisis de la Información

En el caso de la presente investigación se requiere aplicar la teoría fundamentada específicamente considerando un análisis de datos, que permitirá interpretar la información para luego establecer el aporte teórico que permite: Diseñar una Guía de Buenas prácticas en torno a la seguridad de IoT para las Smart House, como un elemento para las personas que diseñan este tipo de dispositivos, aumentando los niveles de seguridad y permitiendo la protección de datos personales.

Capítulo 4. Resultados

4.1 Estudio de las capas de IoT

Para dar cumplimiento a este objetivo se hace necesario abordar una serie de actividades para llevar a cabo la ejecución del mismo.

4.1.1 Características generales del IO (Internet de Objetos)

Las principales características que presenta la IO van ligadas directamente con el diseño de aplicaciones innovadoras.

1. Características Generales de la IO

Tabla 1.

Requisitos de la IO

Requisitos	Descripción de Requisitos
Heterogéneos	Gestionar la variedad de dispositivos/tecnologías/servicios/entornos
Escalabilidad	Evitar la explosión de recursos/datos/operaciones intercambiados
Minimización de costes	Optimización de los costes de desarrollo/mantenimiento y del consumo de energía
Auto	Auto-configuración, auto-organización, auto-adaptación, auto-reacción a los acontecimientos y estímulos, auto-descubrimiento de entidades y servicios, auto-procesamiento de Big Data.
Flexibilidad	Gestión dinámica/reprogramación de los decisores o grupo de dispositivos
QoS	El cumplimiento de las garantías de calidad de servicio (por ejemplo, ancho de banda, retardo) a los servicios/aplicaciones
Entorno Seguro	Robustez a los ataques de comunicación, autenticación, confidencialidad de la transferencia de datos, integridad de datos/dispositivos, privacidad, entorno seguro y de confianza

Nota. Fuente: (Borgia, 2014)

En la tabla anterior se puede apreciar que se resumen los requisitos generales de la IO, en los que se incluye la heterogeneidad y la escalabilidad son de vital importancia en sistemas complejos y dinámicos como la IO, para tratar estas cuestiones se proponen que la solución es buscar en el sector de la arquitectura a nivel de nombre/identificación/dirección, a nivel de asignación de nombre/código de objeto que permitirán analizar lo planteado anteriormente con el fin de ofrecer dispositivos con un mayor grado de escalabilidad, por otra parte el hecho de comenzar a minimizar los objetos ayuda en gran parte a la optimización de los costes operativos (desarrollo, instalación, mantenimiento, materiales) (Borgia, 2014).

Entre las características principales de la IO, es que los objetos deben ofrecer capacidades de auto.

- Auto-grado de autonomía de configuración
- Auto-organización y auto-adaptación
- Auto-reacción a los acontecimientos y estímulos a los que se ven sometidos los objetos
- Auto procesamiento de la cantidad de datos intercambiados por terceros

Por último la IO debe garantizar:

Un entorno seguro en términos de seguridad de la comunicación/autenticación y de integridad de los datos y dispositivos, la privacidad de los usuarios y los datos personales, y la fiabilidad del medio ambiente y de las partes implicadas (Borgia, 2014).

2. Requisitos de comunicación

Existen una serie de requisitos relacionados con el tráfico generado y transmitido por dispositivos IO, sin embargo no toda la comunicación de dispositivos IO debe ser apoyada por los requisitos de comunicación, sin embargo se pueden identificar alguno de ellos en la siguiente tabla, que muestra las características necesarias de las comunicaciones M2M (Borgia, 2014).

Tabla 2.

Características de las comunicaciones

Característica	Descripción de la característica
Diferentes redes subyacentes	La abstracción de las diferentes redes subyacentes (por ejemplo, alámbricas, inalámbricas, celulares), soporte para diferentes modos de comunicación (por ejemplo, punto de acceso basado en la moda p2p (Intercambio)).
Modos de direccionamiento	El soporte de transmisiones anycast/unicast/multicast/broadcast, sustitución dinámica de la emisión con multicast/anycast para reducir la carga de la red.
Transmisión masiva de dispositivos	Manejar transmisiones simultáneas o casi simultáneas desde un gran número de dispositivos (es decir, protocolos MAC eficientes).
Alta fiabilidad	Garantía de conectividad/transmisiones fiables basadas en diferentes soluciones (por ejemplo, enlace protocolos de adaptación, esquemas de modulación/codificación, establecimiento de rutas múltiples).
Prioridad de acceso mejorada	Gestión de los niveles de prioridad de los servicios y de los servicios de comunicaciones (por ejemplo, el derecho mecanismos de preferencia).
Selección de la ruta	Optimización de las vías de comunicación en función de las diferentes políticas (por ejemplo, coste de la red, retraso, fuentes de transmisión).
Movilidad	Itinerancia y movilidad sin fisuras, gestión de la comunicación hacia los sistemas estacionarios y de dispositivos móviles de bajo costo.

Bajo consumo de energía	Incluir mecanismos para reducir el consumo de energía.
Notificación e interacción	Funciones para soportar el reconocimiento de datos, las notificaciones de fallos y el modo de interacción
Perfil de tráfico	Gestión del tráfico de datos con diferentes perfiles de tráfico (por ejemplo, transmisiones continuas, transmisiones largas períodos entre dos transmisiones de datos, pequeña cantidad de datos transmitidos, estallido de datos, bidireccionales/unidireccionales).
Tráfico dependiente del tiempo	soporte de tráfico de datos con diferentes requisitos de tiempo (por ejemplo, tráfico controlado por tiempo, tráfico tolerante al retardo, tráfico de latencia extremadamente baja).
Soporte de informes de localización	Reportar el dispositivo, localización a otros dispositivos aplicaciones de forma continua sobre demanda.
Conexiones seguras	Integridad de la comunicación

Nota. Fuente: (Borgia, 2014)

Cada una de las características planteadas anteriormente buscan dar solución a los problemas de seguridad a los que se enfrentan los dispositivos IO, siendo la comunicación una de las principales fuentes de ataque, es por esta razón que se busca que las credenciales o la configuración de las mismas sean robustas, es decir evitar que estas se vean comprometidas a ataques de red (hacking y DoS), asegurando así la integridad de las comunicaciones, es un claro ejemplo de poder garantizar la seguridad, en la siguiente imagen se pueden apreciar algunas de las soluciones para mejorar la seguridad en las comunicaciones (Borgia, 2014).



Ilustración 5. Soluciones de seguridad en las comunicaciones

Nota. Fuente: (Borgia, 2014)

4.1.2 Identificar el modelo de dispositivos IOT

Existe una cantidad de modelos para dispositivos IOT, pero en este caso se centrara en hablar del modelo en forma de diagrama en estrella, en su primer nivel se compone de cuatro elementos; comunicación, objetivo, manipulación de datos y desarrollo, cabe resaltar que cada uno de estos componentes pueden ser manipulados por los usuarios, a continuación se describen cada uno de ellos (Caivano, Cassano, Lanzilotti, & Piccinno, 2018).

- **Comunicación:** dentro de este componente aparecen tres elementos fundamentales que son; criptografía, protocolo y destino. La criptografía representa básicamente la cantidad de datos que están protegidos a los ataques por parte de usuarios no autorizados, en este componente se busca que no exista sobrecarga de transmisión para que no se hayan interrupciones en la señal y se logre la entrega de la información al destino.
- **Objetivo:** este componente es el que se encarga básicamente de clasificar el dispositivo IO según su uso y/o despliegue: personal, profesional y mixto. En el aspecto personal se tiene muy en cuenta el bajo coste del dispositivo, mientras que para el aspecto profesional se prefiere un dispositivo de mayor calidad, con precisión en el sensor, sin importar el costo del mismo, otra característica como la posibilidad de leer y editar el dispositivo, el bajo impacto en la infraestructura donde se va a utilizar son elementos que permiten evaluar el aspecto mixto.
- **Manipulación de datos:** este elemento implica la recopilación, el análisis y la visualización de datos, uno de los aspectos principales a analizar es la privacidad de los datos, la integridad de los datos (Es la garantía de la exactitud y consistencia de los datos), el segundo aspecto hace referencia a la recopilación , puede realizarse

directamente en el dispositivo o utilizando otras técnicas, la visualización esta suele estar ausente con el fin de ahorrar energía, finalmente el último aspecto hace referencia a la transformación de datos, representa como los datos son transformados por el dispositivo.

- **Desarrollo:** este cubre tres aspectos principales dependiendo que quien pueda programar el dispositivo. Los desarrolladores profesionales, el experto en dominio y los usuarios finales. Los desarrolladores profesionales son los que están familiarizados con la programación y se encargan de leer, entender, manipular y modificar el código, los usuarios expertos en dominios son expertos familiarizados con la mayor parte del mundo de la tecnología y por último los usuarios finales no están familiarizados con el ordenador o con la tecnología.

4.1.3 Recopilar la información relacionada con las capas IoT

Una vez se ha hecho una recolección de las características generales del IO y se ha identificado el modelo de dispositivo IoT, se abordan a continuación cada una de las capas relacionadas con el IoT.

Capa de Percepción (CP): Realiza la identificación de objetos. Recopila datos a través de sus sensores. La seguridad se ve afectada debido a los sensores empleados en esta capa de percepción que son, generalmente, de diferentes tecnologías, por ejemplo los sensores RFID (Perez et al., 2018).

Capa de Red: Transmite datos obtenidos de la capa de percepción a través de Internet, red móvil o cualquier otro tipo de red de comunicación confiable (Perez et al., 2018).

Capa de Nivel Medio: Es la encargada de garantizar el mismo tipo de servicio entre los objetos físicos conectados. Los problemas de seguridad se producen en el canal de comunicación (Perez et al., 2018).

Capa de Aplicación: Es la encargada de las aplicaciones de IoT provenientes de los más diversos tipos de industrias, como por ejemplo, Smart Hospital, Smart City, Smart transportation, entre otros (Perez et al., 2018).

A continuación se detallaran cada una de las capas de IoT, tomando como base la ilustración 6, donde se pueden evidenciar los bordes y los protocolos que se utilizan por cada capa en una infraestructura IoT:

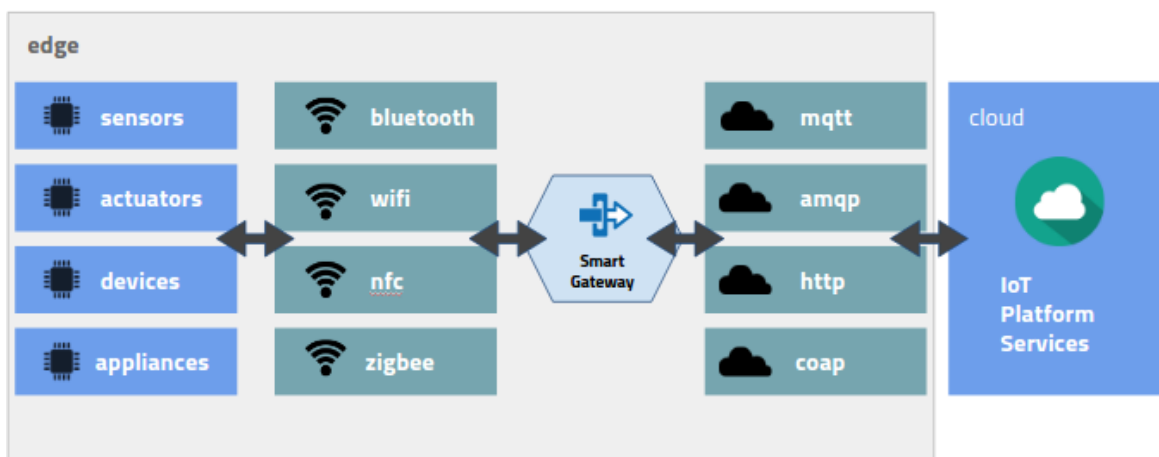


Ilustración 6. Bordes y Protocolos en una infraestructura IoT

Nota. Fuente: (Ammar et al., 2018)

La ilustración 6, muestra el lado del borde y el lado de la nube. En el lado del borde, las cosas podrían ser sensores, actuadores, dispositivos y una cosa crucial llamada pasarela. Esta puerta de enlace tiene la responsabilidad de establecer comunicaciones entre las cosas y los servicios en la nube y también organizar las acciones entre las cosas, seguidamente se definirán cada una de las capas y la infraestructura que la relaciona.

CAPA DE PERCEPCIÓN

Sensores.

Todo lo que vive en el borde son cosas, una de las más comunes se llama sensores. Los sensores leen e informan sobre el estado real de los productos conectados, las máquinas y los entornos locales. Son los ojos y oídos del sistema, que controlan elementos ambientales como la temperatura, la luz y la humedad. La innovación de sensores en curso, un área que a menudo se pasa por alto en la tecnología IoT, será fundamental para desarrollar y mejorar las soluciones (Ammar et al., 2018).

Si bien podemos pensar en los sensores solo como objetos físicos, cualquier cosa que pueda leerse, desde archivos hasta datos específicos del producto, puede y debe considerarse una entrada de sensor. Por ejemplo, una pieza de equipo industrial puede tener cientos de puntos de datos únicos para ese producto, y cada uno de ellos podría considerarse un sensor. Ejemplos de sensores incluyen:

- Sensores de temperatura
- Sensores de luz
- Sensores de humedad
- Receptores GPS
- Diagnóstico a bordo del vehículo.

Actuadores.

Hay otra cosa de borde común que se llaman actuadores. Por lo general, afectan el estado electromecánico o lógico de un producto o entorno. Son las manos y los pies del sistema. Los

actuadores pueden incluir una luz que se puede encender y apagar, o una válvula que se puede abrir y cerrar. Comúnmente los actuadores ofrecen un conjunto de API para su interacción.

Los comandos del sistema que se envían a las aplicaciones integradas, como el reinicio remoto, las actualizaciones de configuración y la distribución de firmware, también deben considerarse activación porque, al cambiar su software, el sistema está cambiando la realidad física de un producto (Ammar et al., 2018). Ejemplos de actuadores incluyen:

- Luces
- Válvulas
- Motores
- Comandos (acciones “suaves”, distribución de archivos, actualizaciones de firmware)

CAPA DE RED

Protocolos de red.

Dado que los sensores, los actuadores y los dispositivos están viviendo en el límite, deben comunicarse entre sí y también con Smart Gateway. Este tipo de comunicación se basa en protocolos de campo (Ammar et al., 2018), los protocolos más comunes son:

- Bluetooth de bajo consumo de energía (BLE): el nuevo Bluetooth de bajo consumo de energía (BLE), o Bluetooth Smart, como se lo denomina ahora, es un protocolo importante para las aplicaciones de IoT. Es importante destacar que, aunque ofrece un alcance similar al de Bluetooth, se ha diseñado para ofrecer un consumo de energía significativamente reducido.

- Zigbee: Al igual que Bluetooth, tiene una gran base de operaciones instalada, aunque quizás sea más tradicional en entornos industriales. ZigBee PRO y ZigBee Remote Control (RF4CE), entre otros perfiles disponibles de ZigBee, se basan en el protocolo IEEE802.15.4, que es una tecnología de red inalámbrica estándar de la industria que opera a aplicaciones de focalización de 2,4 GHz que requieren intercambios de datos relativamente poco frecuente a baja información. tarifas en un área restringida y dentro de un rango de 100 m, como en una casa o edificio.
- Wifi: este tipo de conectividad suele ser una opción obvia para muchos desarrolladores, especialmente dada la omnipresencia de WiFi en el entorno doméstico dentro de las LAN. Requiere poca explicación adicional, excepto para establecer lo obvio de que claramente existe una amplia infraestructura existente, además de ofrecer una transferencia de datos rápida y la capacidad de manejar grandes cantidades de datos.
- NFC: Near Field Communication (NFC) es una tecnología que permite interacciones bidireccionales simples y seguras entre dispositivos electrónicos, y especialmente aplicable para teléfonos inteligentes, permitiendo a los consumidores realizar transacciones de pago sin contacto, acceder a contenido digital y conectar dispositivos electrónicos. Esencialmente, amplía la capacidad de la tecnología de tarjetas sin contacto y permite que los dispositivos compartan información a una distancia de menos de 4 cm.

CAPA DE NIVEL MEDIO Y DE APLICACIONES

Protocolos en la nube.

La mayoría de las soluciones de IoT (“The IoT Architecture at the Edge - IoT Central,” n.d.), incluso aquellas que viven casi por completo en el borde, necesitan integrarse con servicios

en la nube u otra solución de IoT basada en la nube. Dado que es un requisito, debemos comunicarnos utilizando un protocolo de nube como se indica a continuación (Ammar et al., 2018):

- MQTT: El transporte de telemetría de la cola de mensajes (MQTT) fue introducido por IBM en 1999 y estandarizado por OASIS en 2013. Está diseñado para proporcionar conectividad integrada entre aplicaciones y middlewares en un lado y redes y comunicaciones en el otro. Sigue una arquitectura de publicación / suscripción, donde el sistema consta de tres componentes principales: editores, suscriptores y un intermediario.
- AMQP: El protocolo avanzado de Message Queue Server (AMQP) es un protocolo diseñado para la industria financiera. Se ejecuta sobre TCP y proporciona una arquitectura de publicación / suscripción que es similar a la de MQTT. La diferencia es que el intermediario se divide en dos componentes principales: intercambio y colas. El intercambio es responsable de recibir los mensajes del editor y distribuirlos en colas según los roles y condiciones predefinidos. Básicamente, las colas representan los temas y los suscriptores de los suscriptores que obtendrán los datos sensoriales siempre que estén disponibles en la cola.
- CoAP: El Protocolo de aplicación restringido (CoAP) es otro protocolo de capa de sesión diseñado por el grupo de trabajo de Entorno RESTful Restringido (Core) de IETF para proporcionar una interfaz RESTful (HTTP) ligera. Representational State Transfer (REST) es la interfaz estándar entre el cliente HTTP y los servidores. Sin embargo, para aplicaciones livianas como IoT, REST podría generar una sobrecarga y un consumo de energía significativos. CoAP está diseñado para permitir que los sensores de baja potencia utilicen los servicios RESTful mientras cumplen con sus limitaciones de

energía. Se construye sobre UDP, en lugar de TCP comúnmente utilizado en HTTP y tiene un mecanismo ligero para proporcionar confiabilidad. La arquitectura de CoAP se divide en dos subcapas principales: mensajería y solicitud / respuesta. La subcapa de mensajería es responsable de la confiabilidad y la duplicación de mensajes, mientras que la subcapa de solicitud / respuesta es responsable de la comunicación. Al igual que en HTTP, CoAP utiliza los mensajes GET, PUT, PUSH, DELETE para recuperar, crear, actualizar y eliminar, respectivamente.

- HTTP: este es el protocolo estándar para servicios web y aún se utilizará en soluciones de IoT, la sobrecarga de este protocolo es bien conocida pero continuaremos usando este protocolo en algunos casos cuando la latencia y el ancho de banda no sean problemas. También debemos considerar HTTP / 2, otros protocolos como Google Protobuf e incluso CoAP que se basan en HTTP. El estilo arquitectónico más popular llamado RESTful se usa ampliamente en aplicaciones móviles y web y debe considerarse en IoT Solutions.

La recopilación de la información relacionada con cada una de las capas del IoT, permite hacer un enfoque de cómo va a estar estructurado el dispositivo IoT, teniendo en cuenta que la capa de red es la más importante de ellas, puesto que está en conjunto con la capa de percepción permiten la transmisión de datos.

4.1.4 Analizar los protocolos utilizados en IoT

El análisis de los protocolos utilizados en IoT, son de vital importancia a la hora del diseño, desarrollo, creación e implementación de los mismos, pues como se mencionaba anteriormente se considera que la capa de red es la más importante dentro de las capas IoT,

identificar el protocolo que se desea utilizar en el diseño del dispositivo permitirán ofrecer dispositivos con más seguros y confiables de acuerdo a las características de los mismos.

Comenzaremos analizando el Protocolo IP, dentro de este protocolo se tienen los Protocolos para la Internet de las cosas, definidos a continuación:

Protocolo de Internet (IP).

El uso de la tecnología de IP es fundamental para la IoT. El IP permite la interoperabilidad de los sistemas. Es posible que esta característica no parezca importante hoy, pero a medida que la IoT evolucione, la interoperabilidad de los sistemas se convertirá en una competencia importante para generar ingresos. Ethernet/Wi-Fi y 6LoWPAN dependen en gran medida de IPv4 e IPv6 (“Protocolos para la Internet de las cosas | Arrow.com,” n.d.).

Protocolos IP utilizados en la IoT.

Definitivamente, es posible crear un sistema de IoT con las tecnologías Web existentes, aunque no sean tan eficaces como los protocolos más nuevos. HTTP(S) y Websockets son estándares comunes, junto con XML o JavaScript Object Notation (JSON) para la carga útil. Cuando se utiliza un explorador Web estándar (cliente HTTP), JSON proporciona una capa de abstracción para que los desarrolladores Web creen una aplicación Web con estado de conexión dúplex constante a un servidor Web (servidor HTTP) mediante la mantención de dos conexiones HTTP abiertas (“Protocolos para la Internet de las cosas | Arrow.com,” n.d.), a continuación se describen cada uno de ellos:

HTTP.

HTTP es la base del modelo cliente-servidor usado para la Web. El método más seguro de implementar el HTTP en su dispositivo de IoT es incluir solo un cliente, no un servidor. En otras palabras, es más seguro si el dispositivo de IoT puede iniciar conexiones a un servidor Web, pero no es capaz de recibir solicitudes de conexión. Después de todo, no queremos permitir que máquinas externas tengan acceso a la red local donde se encuentran instalados los dispositivos de IoT.

WebSocket.

WebSocket es un protocolo que proporciona comunicación dúplex completa a través de una conexión TCP única por la cual se pueden enviar mensajes entre el cliente y el servidor. Forma parte de la especificación HTML 5. El estándar WebSocket simplifica gran parte de la complejidad que circunda la comunicación Web bidireccional y la administración de la conexión. Usar Websockets junto con HTTP es una solución apropiada para los dispositivos de IoT si los dispositivos pueden soportar las cargas de HTTP.

XMPP.

XMPP (Protocolo extensible de mensajería y presencia) es un excelente ejemplo de una tecnología Web existente que encuentra un uso nuevo en el espacio de IoT. El XMPP tiene sus raíces en la mensajería instantánea y la información de presencia, y se ha ampliado a llamadas de voz y video, colaboración, middleware ligero, redifusión de contenido y enrutamiento generalizado de datos XML. Es un aspirante a administración a escala masiva de electrodomésticos de consumo, como lavadoras, secadoras, refrigeradores, etc. Las ventajas del XMPP son su direccionamiento, seguridad y escalabilidad. Esto lo hace ideal para aplicaciones de IoT orientada a los consumidores.

HTTP, Websocket y XMPP son solo ejemplos de tecnologías que se han tenido que poner a trabajar para la IoT. Otros grupos también están trabajando intensamente a fin de desarrollar soluciones para los nuevos desafíos que la IoT nos presenta.

El Protocolo de Internet (IP) es un portador; puede encapsular tantos protocolos para la IoT como lo hace hoy para la Web. Muchos especialistas de la industria exigen una estandarización de protocolos. Sin embargo, si existe una cantidad tan grande de protocolos para la Web, ¿por qué no habría la misma cantidad de protocolos para la IoT? La diferencia es que los protocolos de IoT aún son muy nuevos y deben demostrar su confiabilidad. Es importante resaltar que cuando Internet se transformó en realidad, la versión 4 del IP fue lo que lo hizo posible. Ahora, se está implementando masivamente la versión 6 del IP. El posicionamiento de cada uno de los protocolos de IoT requiere un cuestionamiento similar. Salvo el protocolo HTTP, todos estos protocolos están posicionados como protocolos de IoT de publicación-suscripción en tiempo real, compatibles con millones de dispositivos. Según cómo defina "tiempo real" (segundos, milisegundos o microsegundos) y "cosas" (nodo WSN, dispositivo multimedia, dispositivo usable personal, escáner médico, control de motor, etc.), la selección del protocolo para su producto es fundamental ("Protocolos para la Internet de las cosas | Arrow.com," n.d.).

Sin embargo, el diseño de los sistemas de datos de IoT se encuentra más allá del diseño de hardware y de software. Se hace necesario separar los datos de la aplicación, de manera que se puedan hacer cosas nuevas con ellos, cosas inimaginables. Para el desarrollador de sistemas integrados normal, pensar específicamente en los datos que genera el sistema requiere una nueva mentalidad. Estos datos son valiosos.

La tecnología de hardware, la tecnología de software, la infraestructura y la computación en nube de los sistemas integrados se están probando e implementando activamente,

promoviendo la emergente Internet de las cosas. Para tener un éxito real y alcanzar los 50 mil millones de dispositivos que se implementarán para el año 2020, se hace necesario contar con los mismos estándares abiertos y desarrollo que apoyaron la creación de la Internet de las personas (también conocida como la Web).

4.2 Proyecto OWASP de IoT

Una vez se han estudiado las capas del IoT, continuaremos con la recolección de la información en lo que corresponde al proyecto OWASP de IoT, se describirá el mismo, se representara el Top 10 IoT, que es básicamente una serie de características propuesta por el proyecto OWASP de IoT en su versión más reciente (2018), con el fin de que los desarrolladores de dispositivos logren mejorar la seguridad de los mismos, además se abordaran los marcos que propone OWASP, que serán de gran utilidad en el diseño de la guía de buenas prácticas en torno a la seguridad IoT para las Smart House.

4.2.1 Recolectar la información relacionada con el proyecto OWASP de IoT

Existen un sin número de vulnerabilidades en los dispositivos IoT, que afectan directamente a las personas y empresas en lo que se relaciona con la privacidad de la información, organizaciones ajenas a los fabricantes se están dedicando a reducir los riesgos.

Una de estas organizaciones es el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP “Open Web Application Security”), reconocido por la documentación relacionada a la seguridad de aplicaciones web y la lista de Top 10 de vulnerabilidades (González, 2017).

El proyecto OWASP Internet of Things se inició en 2014, como una forma de ayudar a los desarrolladores a tomar mejores decisiones con respecto a la creación y el uso de los

sistemas de IoT. Esta continúa con la versión 2018 de OWASP IoT Top 10, que muestra a los desarrolladores las diez cosas que se deben evitar al diseñar, crear, desarrollar, implementar y administrar en sistemas IoT. Este proyecto busco darle solución a la mayor parte de riesgos y vulnerabilidad a la que se están expuestos los dispositivos IoT, por esta razón propone una guía única que aborde los problemas de mayor prioridad para los fabricantes, empresas y consumidores (“Proyecto OWASP de Internet de las Cosas - OWASP,” n.d.).

A continuación se muestra el Top 10 del IoT que ayuda a los desarrolladores y diseñadores de dispositivos a tener en cuenta las vulnerabilidades a las que se exponen los dispositivos IoT.

1. Contraseñas débiles, adivinables o con códigos duros
2. Servicios de red inseguros
3. Interfaces inseguras del ecosistema
4. Falta de un mecanismo seguro de actualización
5. Uso de componentes inseguros u obsoletos
6. Insuficiente protección de la privacidad
7. Transferencia y almacenamiento de datos inseguros
8. Falta de gestión de dispositivos
9. Configuración predeterminada insegura
10. Falta de endurecimiento físico

Ilustración 7: Top 10 del IoT

Nota. Fuente: (*The OWASP Internet of Things, n.d.*)

El futuro del IoT del Top 10 de OWASP IoT, incluye una serie de actividades y temas que permitirán al desarrollar planificar los procesos que darán mejoras significativas al proyecto

en el futuro (“Proyecto OWASP de Internet de las Cosas - OWASP,” n.d.), algunos de los temas son:

- Continuar mejorando la lista en una cadencia de dos años, incorporando los comentarios de la comunidad y de contribuyentes de proyectos adicionales para garantizar que nos mantengamos al día con los problemas que enfrenta la industria.
- Asignación de los elementos de la lista a otros proyectos OWASP, como el ASVS, y quizás también a otros proyectos fuera de OWASP.
- Expandiendo el proyecto a otros aspectos de IoT, incluyendo seguridad incorporada, ICS / SCADA, etc.
- Agregar casos de uso y abuso, con múltiples ejemplos, para solidificar cada concepto discutido.
- Teniendo en cuenta la incorporación de arquitecturas de referencia, no solo podemos decirle a las personas qué deben evitar, sino también cómo hacer lo que necesitan hacer de forma segura.

4.2.2 Identificar los marcos establecidos por el proyecto OWASP de IoT

El proyecto OWASP de IoT, dispone a los desarrolladores una guía de seguridad, de forma de “Borrador” en la que se exponen las vulnerabilidades más críticas de la IoT, a continuación se exponen los marcos que estos utilizan:

Interfaz Web Insegura

- Busca evaluar la interfaz web, el mecanismo de bloqueo para mostrar las vulnerabilidades que estos presentan.
- Busca evaluar el uso de HTTPS, para proteger la información transmitida.

Autenticación/Autorización Insuficiente

- Busca evaluar las contraseñas y el mecanismo de recuperación de contraseñas seguras.
- Busca darle solución a la opción de forzar la caducidad de la contraseña después de un período específico.

Servicios de Red Inseguros

- Busca darle solución a los servicios que no responden de manera deficiente a los ataques.
- Busca darle solución a los puertos de prueba.

Falta de Cifrado de Transporte

- Busca evaluar la comunicación y las prácticas de cifrado que se usan en los protocolos.
- Busca darle solución a los firewalls.

Problemas de Privacidad

- Busca determinar los datos personales, para determinar si estos se encuentran protegidos adecuadamente.
- Busca garantizar a los usuarios finales que puedan elegir los datos personales para el correcto funcionamiento del dispositivo.

Interfaz de Nube Insegura

- Busca evaluar las interfaces en la nube para detectar las vulnerabilidades de seguridad (interfaces API, interfaces web basadas en la nube)
- Busca evaluar las contraseñas para proteger la seguridad de los usuarios.

Interfaz Móvil Insegura

- Busca evaluar la interfaz móvil (contraseñas, logueo, bloqueo, cifrado), para mejorar la seguridad en cada una de ellas.
- Busca evaluar la información personal recopilada.

Configurabilidad de Seguridad Insuficiente

- Busca darle solución a las opciones que se presentan en la creación de una contraseña.
- Busca evaluar las alertas y notificaciones, para darle solución a estos eventos de seguridad.

Software/Firmware Inseguro

- Busca evaluar el dispositivo para asegurarse que cuenta con todas las actualizaciones y archivos cifrados.
- Busca evaluar el dispositivo para asegurarse que utilizan archivos firmados y poder validarlos antes de la instalación.

Mala Seguridad Física

- Busca evaluar el dispositivo, para asegurarse de que utilicen la cantidad de puertos físicos necesarios, y al mismo tiempo determinar si permite la desactivación de puertos físicos no utilizados como USB.
- Busca evaluar el dispositivo para determinar si incluye la capacidad de limitar las capacidades administrativas solo a una interfaz local.

Ilustración 8. Marcos de Seguridad establecido por el proyecto OWASP IoT

Nota. Fuente: (“Guía de seguridad de IoT - OWASP,” n.d.), Autora del proyecto.

El estudio de los marcos permiten mitigar un poco los problemas de seguridad, teniendo en cuenta que contar con objetos de uso cotidiano conectados a Internet, implica grandes problemas para la privacidad y la protección de la información, a esto se le suma la indiferencia de muchos fabricantes, y aunque muchos quieran mejorar y trabajar para asegurar sus dispositivos, no lo logran pues la tecnología avanza a pasos agigantados. A diario aparecen nuevas técnicas de hacking más sofisticadas y cada vez es mayor el número de ciberataques exitosos. Para reducir un poco todos estos problemas, organizaciones de regulación y de seguridad se han tomado el trabajo de crear normas de estandarización del IoT, abarcando aspectos de seguridad, como lo hace la organización OWASP. Es de gran importancia hacer una revisión de la lista de vulnerabilidades más críticas junto a sus respectivas recomendaciones de mitigación, que propone esta organización y que le permiten al fabricante ir reduciendo los riesgos en la privacidad y la protección de la información (González, 2017).

OWASP cuenta con un equipo de profesionales voluntarios de la industria de la seguridad, con experiencia que abarca múltiples áreas de especialización, que incluyen: fabricantes, consultoría, probadores de seguridad, desarrolladores y muchos más, estos profesionales realizaron el proyecto en las siguientes fases:

- Formación del equipo: Recolectar personal que estén dispuestos a contribuir a la actualización de 2018 (IoT Top 10).
- Revisión del proyecto: Análisis del proyecto 2014 para determinar las actualizaciones que se le deben hacer al nuevo proyecto.
- Recopilación de datos: Revisión de vulnerabilidades, enfocados principalmente en el mayor impacto y daño que tuvieron.

- Sister Project Review: Revisión de proyectos de seguridad de IoT, para garantizar el contenido que se va a lanzar.
- Comentarios: Se lanza un borrador a la comunidad para su revisión, esto con el fin de retroalimentar el proyecto.
- Lanzamiento: Se hace pública la lista.

4.3 Guía de buenas prácticas para los desarrolladores de sistemas IoT SmartHouse basados en el proyecto OWASP de IoT

ESTRUCTURA DE LA GUIA

- Pruebas: Teniendo en cuenta la Tabla de Consideraciones de Seguridad de IoT, propuesta por el proyecto OWASP IoT.
- Controles: Una vez los hallazgos hayan sido detectados se aplican los controles de acuerdo a la Tabla de Consideraciones de Seguridad IoT-Controles propuesta por el proyecto OWASP IoT.
- Consideraciones de seguridad del marco de IoT de acuerdo a OWASP IoT.
- Recomendaciones del autor.

Objetivo de la guía

El objetivo de esta guía fundamentada en el proyecto OWASP de IoT, es determinar el grado de vulnerabilidad de los dispositivos IoT con el fin de mejorar la seguridad de los mismos, a través de la aplicación de controles que vienen en el proyecto OWASP de IoT.

Alcance de la guía

El alcance de la guía va orientado directamente a sistema IOT para Smart House.

Limitaciones

Esta guía se propone como un "borrador", pues estamos hablando de un tema que está tomando fuerza y no se cuenta a ciencia cierta con una metodología robusta que me permita alcanzar un grado de madurez en cuanto a la seguridad en los sistemas IOT. Según Balmaseda (2018) se deben hacer uso de metodologías de evaluación de la seguridad y gestión del riesgo, combinadas con el uso de guías de buenas prácticas como MAGERIT, COBIT o ISO 27005 que aportarían nuevas visiones de los escenarios de riesgo, así como de sus posibles remediaciones, permitiéndonos aumentar el conocimiento sobre esta tecnología y sus posibles implementaciones seguras.

Pruebas.

Para poder realizar las pruebas se hace necesario hacer un inventario de Software y Hardware con el fin de identificar los elementos o dispositivos con los cuales se cuenta y con los que se está trabajando en el sistema que se está desarrollando o se ha desarrollado, como autora del proyecto se propone que los dispositivos sean evaluados de forma independiente, de igual manera también se recomienda que se evalúen como un todo, es decir luego del proceso de instalación realizar las pruebas en conjunto. Es muy importante resaltar que para el desarrollo de esta guía se utilizó un prototipo de domótica, este tenía bajo niveles de seguridad lo que permite hacer la evaluación teniendo en cuenta la Tabla 3. Consideraciones de Seguridad IoT.

Prueba aplicada a dispositivo IoT (Aleatoriamente)

Las siguientes pruebas basadas en el proyecto OWASP son una guía de gran importancia que permite medir la madurez en cuanto a la seguridad de esos sistemas desarrollados por las

organizaciones. El proyecto OWASP IoT trabaja con 10 categorías, cada categoría está compuesta por una serie de consideraciones a tener en cuenta. Para el proyecto de grado se trabajó de tal manera que se pudiera medir el grado de cumplimiento para cada categoría en donde habrá dos opciones de cumplimiento que son los siguientes:

1=Cumple

0=No cumple

Tabla 3.

Consideración de seguridad de IoT

CATEGORÍA	CONSIDERACIÓN DE SEGURIDAD DE IOT	CUMPLIMIENTO	TOTAL
I1: Interfaz web insegura	Evalúe cualquier interfaz web para determinar si se permiten contraseñas débiles	1	6
	Evaluar el mecanismo de bloqueo de cuenta	1	
	Evalúe la interfaz web para las vulnerabilidades de XSS, SQLi y CSRF y otras vulnerabilidades de aplicaciones web	1	
	Evaluar el uso de HTTPS para proteger la información transmitida	1	
	Evaluar la capacidad de cambiar el nombre de usuario y la contraseña	1	
	Determine si los firewalls de aplicaciones web se utilizan para proteger interfaces web	1	
I2: Autenticación / Autorización Insuficiente	Evalúe la solución para el uso de contraseñas seguras donde se necesita autenticación	0	3
	Evalúe la solución para entornos de múltiples usuarios y asegúrese de que incluya funcionalidad para la separación de roles	0	
	Evalúe la solución para la implementación de autenticación de dos factores cuando sea posible	0	
	Evaluar mecanismos de recuperación de contraseña	0	

	Evalúe la solución para la opción de requerir contraseñas seguras	1	
	Evalúe la solución para la opción de forzar la caducidad de la contraseña después de un período específico	1	
	Evalúe la solución para la opción de cambiar el nombre de usuario y la contraseña predeterminados	1	
I3: Servicios de red inseguros	Evalúe la solución para asegurarse de que los servicios de red no respondan de manera deficiente a los ataques de desbordamiento de búfer, falsificación o denegación de servicio	1	2
	Evalúe la solución para asegurarse de que los puertos de prueba no estén presentes	1	
I4: Falta de cifrado de transporte	Evalúe la solución para determinar el uso de la comunicación cifrada entre dispositivos y entre dispositivos e Internet.	1	3
	Evalúe la solución para determinar si se utilizan prácticas de cifrado aceptadas y si se evitan los protocolos propietarios	1	
	Evalúe la solución para determinar si hay disponible una opción de firewall disponible	1	
I5: Problemas de privacidad	Evaluar la solución para determinar la cantidad de información personal recopilada	1	4
	Evalúe la solución para determinar si los datos personales recopilados están protegidos adecuadamente mediante el cifrado en reposo y en tránsito	1	
	Evalúe la solución para determinar si Asegurar la anulación de datos o anonimización	1	
	Evalúe la solución para garantizar que los usuarios finales puedan elegir los datos recopilados más allá de lo que se necesita para el correcto funcionamiento del dispositivo.	1	
I6: Interfaz de nube insegura	Evalúe las interfaces en la nube para detectar vulnerabilidades de seguridad (por ejemplo, interfaces API y interfaces web basadas en la nube)	1	9
	Evalúe la interfaz web basada en la nube para asegurarse de que no permite contraseñas débiles	1	

	Evalúe la interfaz web basada en la nube para asegurarse de que incluya un mecanismo de bloqueo de cuenta	1	
	Evalúe la interfaz web basada en la nube para determinar si se utiliza la autenticación de dos factores	1	
	Evalúe cualquier interfaz de nube para las vulnerabilidades de XSS, SQLi y CSRF y otras vulnerabilidades	1	
	Evalúe todas las interfaces en la nube para garantizar que se utiliza el cifrado de transporte	1	
	Evalúe las interfaces de la nube para determinar si la opción de requerir contraseñas seguras está disponible	1	
	Evalúe las interfaces de la nube para determinar si la opción de forzar la caducidad de la contraseña después de un período específico está disponible	1	
	Evalúe las interfaces de la nube para determinar si la opción para cambiar el nombre de usuario y la contraseña predeterminados están disponibles	1	
I7: Interfaz móvil insegura	Evalúe la interfaz móvil para asegurarse de que no permite contraseñas débiles	1	3
	Evalúe la interfaz móvil para asegurarse de que incluye un mecanismo de bloqueo de cuenta	0	
	Evalúe la interfaz móvil para determinar si implementa autenticación de dos factores (p. Ej., La identificación táctil de Apple)	0	
	Evalúe la interfaz móvil para determinar si utiliza cifrado de transporte	0	
	Evalúe la interfaz móvil para determinar si la opción de requerir contraseñas seguras está disponible	0	
	Evalúe la interfaz móvil para determinar si está disponible la opción de forzar la caducidad de la contraseña después de un período específico	0	
	Evalúe la interfaz móvil para determinar si la opción para cambiar el nombre de usuario y la contraseña predeterminados están disponibles	1	

	Evaluar la interfaz móvil para determinar la cantidad de información personal recopilada	1	
I8: Configurabilidad de seguridad insuficiente	Evalúe la solución para determinar si las opciones de seguridad de contraseña (por ejemplo, habilitar contraseñas de 20 caracteres o habilitar la autenticación de dos factores) están disponibles	1	4
	Evalúe la solución para determinar si las opciones de cifrado (por ejemplo, Habilitar AES-256 donde AES-128 es la configuración predeterminada) están disponibles	1	
	Evalúe la solución para determinar si el registro de eventos de seguridad está disponible	1	
	Evalúe la solución para determinar si las alertas y notificaciones al usuario sobre eventos de seguridad están disponibles	1	
I9: Software / Firmware Inseguro	Evalúe el dispositivo para asegurarse de que incluya la capacidad de actualización y se pueda actualizar rápidamente cuando se descubren vulnerabilidades	1	3
	Evalúe el dispositivo para asegurarse de que utiliza archivos de actualización cifrados y de que los archivos se transmiten utilizando el cifrado	1	
	Evalúe el dispositivo para asegurarse de que utiliza archivos firmados y luego valida ese archivo antes de la instalación	1	
I10: Mala Seguridad Física	Evalúe el dispositivo para asegurarse de que utiliza un número mínimo de puertos físicos externos (por ejemplo, puertos USB) en el dispositivo	1	4
	Evalúe el dispositivo para determinar si se puede acceder a él a través de métodos no intencionados, como a través de un puerto USB innecesario	1	
	Evalúe el dispositivo para determinar si permite la desactivación de puertos físicos no utilizados, como USB	1	
	Evalúe el dispositivo para determinar si incluye la capacidad de limitar las capacidades administrativas solo a una interfaz local	1	

Nota. Fuente: (“IoT Security Guidance - OWASP,” n.d.)

Teniendo en cuenta los resultados arrojados en la Tabla 3. Consideraciones de Seguridad IoT, en el que se está evaluando un sistema IoT SmartHouse solo para dar entender como trabajar con las pruebas, una vez se evaluaron las consideraciones, se obtuvo un puntaje total para cada categoría, dicho resultado se puede evidenciar en la Ilustración 9. Evaluación de Sistema IoT Smart House.

Tabla 4.

Evaluación de sistemas IoT Smart House

Categorías	Producto de total
I1: Interfaz web insegura	6
I10: Mala Seguridad Física	4
I2: Autenticación / Autorización Insuficiente	3
I3: Servicios de red inseguros	2
I4: Falta de cifrado de transporte	3
I5: Problemas de privacidad	4
I6: Interfaz de nube insegura	9
I7: Interfaz móvil insegura	3
I8: Configurabilidad de seguridad insuficiente	4
I9: Software / Firmware Inseguro	3

Nota. Fuente: Elaboración propia

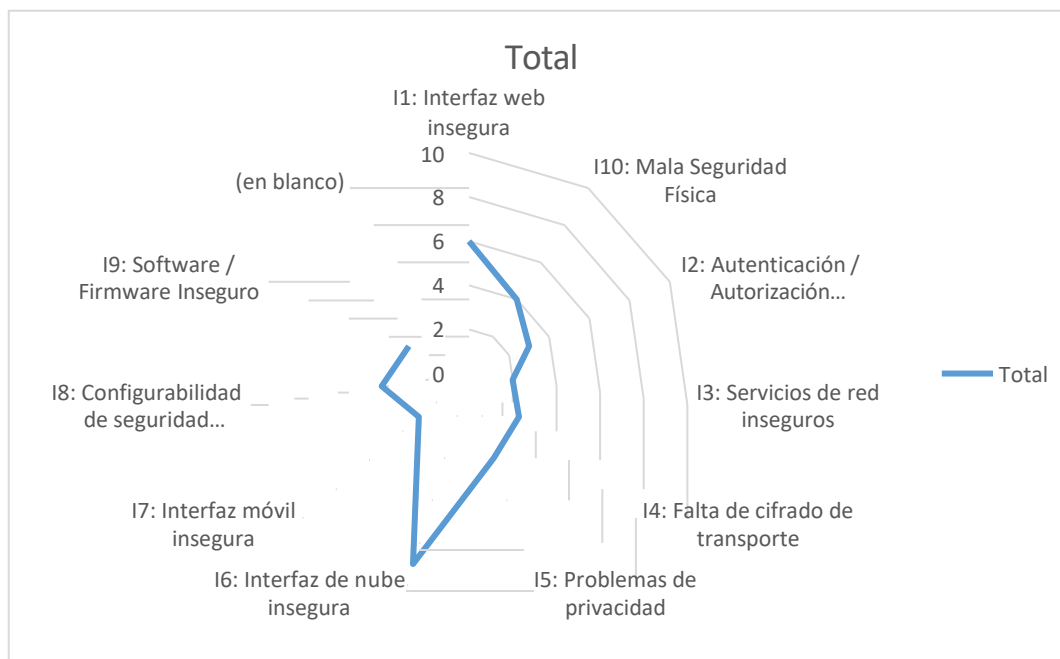



Ilustración 9. Evaluación de sistemas IoT Smart House

Nota. Fuente: Elaboración propia

La tabla 4, permite evidenciar el nivel de cumplimiento de las categoría dentro de la evaluación hecha, donde la categoría I6: Interfaz de Nube Insegura obtuvo un valor nueve (9), lo que permite determinar que se está dando cumplimiento con todas las consideraciones que se exponen para esa categoría, mientras que para la categoría I7: Interfaz Móvil Insegura en el ejemplo fue la que menor cumplimiento obtuvo en cuanto a las consideraciones, lo que conlleva a implementar una serie de controles para la vulnerabilidad detectadas, esta evaluación se hace con el fin de que la que tenga menor grado de cumplimiento sea a la que se le apliquen los controles con mayor prioridad, como se presenta en la Tabla 5. Controles a Aplicar.

Tabla 5.*Controles a Aplicar*

<i>DISPOSITIVO A EVALUAR</i>	<i>DESCRIPCIÓN</i>	<i>EVALUACIÓN DEL DISPOSITIVO</i>	<i>CONTROLES A APLICAR</i>
<p><i>Proyecto Domotica</i></p> 	<p>Este proyecto está enfocado al ahorro de energía y no tiene seguridad alguna. El aplicativo móvil se conecta automáticamente sin exigir contraseña, por lo que se presentan falencias al igual que en la interfaz web.</p>	<p>I3: Servicios de Red Inseguros</p> <p>I2: Autenticación / Autorización Insuficiente</p> <p>I7: Interfaz Móvil Insegura</p>	<ul style="list-style-type: none"> • Realizar pruebas de contraseña de cuenta. • Permitir la Caducidad de la contraseña • Asegurar que las aplicaciones requieran contraseñas donde sea necesario la autenticación. • Implementar mecanismos de recuperación de contraseña seguros. • Asegurar que la aplicación utilice el cifrado de transporte. • Permitir la caducidad de la contraseña. • Asegurar que la interfaz móvil solo recopile la cantidad de información mínima.

Nota. Fuente: Elaboración Propia.

Controles para la Prueba Realizada

Controles y recomendaciones para todas las consideraciones. Para este caso los controles expuestos en la tabla 6. Consideraciones de Seguridad IoT se encuentran resaltados en color

naranja, lo que le indica al fabricante que estos controles deben ser implementados por los desarrolladores de sistemas IoT, con el objetivo de brindar productos seguros en donde las amenazas y vulnerabilidad se encuentren en el nivel más mínimo posible.

Tabla 6.

Consideraciones de Seguridad IoT – Controles

Categoría	Consideración de Seguridad de IoT	Recomendaciones
II: Interfaz web insegura	Asegúrese de que toda la codificación de la interfaz web esté escrita para evitar el uso de contraseñas débiles	Al crear una interfaz web, considere implementar lecciones aprendidas de la seguridad de la aplicación web. Utilice un marco que utilice controles de seguridad para garantizar que las vulnerabilidades se mitigan en el código. Asegúrese de planear eventuales actualizaciones o arreglos de seguridad para el marco también. Si usa complementos opcionales para el marco, asegúrese de revisarlos por seguridad.
	Asegúrese de que toda la codificación de la interfaz web esté escrita para incluir un mecanismo de bloqueo de cuenta	Implemente y proteja la interfaz web de la misma forma que lo haría con cualquier aplicación web. Utilice protocolos de transporte encriptados si es posible, asegurándose de

		validar los certificados. Limite el acceso de cualquier manera posible. Suponga que los usuarios no cambiarán la configuración, así que implemente de forma segura con credenciales sólidas ya establecidas.
	Asegúrese de que toda la codificación de la interfaz web se haya probado para las vulnerabilidades de XSS, SQLi y CSRF	
	Asegúrese de que cualquier interfaz web tenga la capacidad de usar HTTPS para proteger la información transmitida	
	Asegúrese de que toda la codificación de la interfaz web esté escrita para permitir al propietario cambiar el nombre de usuario y la contraseña	
	Considere el uso de firewalls de aplicaciones web para proteger cualquier interfaz web	
I2: Autenticación / Autorización Insuficiente	Asegúrese de que las aplicaciones estén escritas para requerir contraseñas seguras donde se necesita autenticación	Una preocupación cuando se usan contraseñas para la autenticación es la seguridad de la contraseña “segura” hace difícil o incluso improbable que uno adivine la contraseña a través de medios manuales o
	Asegúrese de que la aplicación tenga en cuenta los entornos multiusuario e incluya funcionalidad para la separación de roles	
	Implementar la autenticación de dos factores cuando sea posible	

	<p>Asegurar que los mecanismos de recuperación de contraseña estén escritos para funcionar de manera segura</p>	<p>automáticos. Las siguientes características definen una contraseña segura:</p>
	<p>Asegúrese de que las aplicaciones estén escritas para incluir la opción de requerir contraseñas seguras</p>	<p>Longitud de la contraseña.</p>
	<p>Asegúrese de que las aplicaciones estén escritas para incluir la opción de forzar la caducidad de la contraseña después de un período específico</p>	<p>Mínima longitud de las contraseñas se debe cumplir con la aplicación. Las contraseñas de menos de 8 caracteres se consideran débiles (NIST SP800-63B) la</p>
	<p>Asegúrese de que las aplicaciones estén escritas para incluir la opción de cambiar el nombre de usuario y la contraseña predeterminados</p>	<p>longitud máxima de la contraseña no debe establecerse demasiado baja, ya que evitara que los usuarios creen frases de contraseña. La longitud máxima típica es de 128 caracteres.</p> <p>Al seleccionar la longitud máxima de la contraseña, debe tenerse en cuenta la limitación del algoritmo de hash que se usara para las contraseñas de hash, porque algunas de ellas tienen una longitud máxima de contraseña.</p> <p>No trunque las contraseñas. Asegúrese de que todos los caracteres que escriba el</p>

		<p>usuario estén realmente incluidos en la contraseña.</p> <p>Permitir el uso de todos los caracteres, incluidos los espacios en blanco Unicode.</p> <p>No debe haber reglas de composición de contraseña que limite el tipo de carácter permitido.</p> <p>Asegure la rotación de credenciales cuando se pierde una contraseña o en el momento de la identificación de compromiso.</p> <p>Incluya un medidor de seguridad de contraseña para ayudar a los usuarios a crear una contraseña más compleja y bloquear contraseñas comunes y previamente violadas.</p>
--	--	---

<p>I3: Servicios de red inseguros</p>	<p>Asegúrese de que las aplicaciones que utilizan servicios de red no respondan de manera deficiente a los ataques de desbordamiento de búfer, confusión o denegación de servicio</p>	<p>Intente utilizar pilas e interfaces de red probadas y comprobadas que manejen las excepciones con elegancia. Asegúrese de que las interfaces de prueba o mantenimiento estén deshabilitadas o protegidas adecuadamente. Evite exponer protocolos no autenticados (como TFTP) o canales no cifrados (como telnet) si es posible. Considere la superficie de ataque que presentan los servicios de red del dispositivo. Desactive los servicios innecesarios e implemente medidas para proteger los servicios</p>
	<p>Asegúrese de que los puertos de prueba de las aplicaciones estén fuera de servicio antes de ir a producción</p>	<p>requeridos, detectar actividades maliciosas y reaccionar a un ataque con medidas como bloqueos o reglas de firewall temporales.</p>

<p>I4: Falta de cifrado de transporte</p>	<p>Asegúrese de que todas las aplicaciones estén escritas para hacer uso de la comunicación cifrada entre dispositivos y entre dispositivos e Internet.</p> <p>Utilice las prácticas de encriptación recomendadas y aceptadas y evite los protocolos propietarios.</p> <p>Considere hacer una opción de firewall disponible para la aplicación</p>	<p>Utilice protocolos cifrados siempre que sea posible para proteger todos los datos en tránsito. Cuando no sea posible el cifrado de protocolo, considere la posibilidad de cifrar los datos antes de la transferencia.</p>
<p>I5: Problemas de privacidad</p>	<p>Asegúrese de que solo se recopile la cantidad mínima de información personal de los consumidores</p>	<p>Los datos pueden presentar problemas de privacidad involuntarios cuando se agregan. Como regla general, recopilar la mínima cantidad de datos posible. Consulte con científicos de datos, equipos legales y de cumplimiento para determinar el riesgo de recolección y</p>

		almacenamiento de datos. Considere las implicaciones del consentimiento y el hecho de que los dispositivos de IoT pueden no presentar una interfaz para recopilar el consentimiento y pueden recopilar pasivamente datos sobre personas distintas de los propietarios y operadores. IoT puede recopilar información sobre personas que no pueden dar su consentimiento (como menores de edad) y la recopilación de datos debe modificarse en consecuencia.
	Asegúrese de que todos los datos personales recopilados estén protegidos adecuadamente mediante el cifrado en reposo y en tránsito	Riesgo de privacidad de OWASP, (“OWASP Top 10 Privacy Risks Project - OWASP,” n.d.).
	Asegurar que los datos sean anónimos o anónimos	
	Asegurar que los usuarios finales tengan una opción para los datos recopilados más allá de lo que se necesita para el correcto funcionamiento del dispositivo	

I6: Interfaz de nube insegura	Asegúrese de que todas las interfaces en la nube se revisen para detectar vulnerabilidades de seguridad (por ejemplo, interfaces API y interfaces web basadas en la nube)	La seguridad en la nube presenta consideraciones de seguridad únicas, así como contramedidas. Asegúrese de consultar a su proveedor de la nube sobre las opciones para los mecanismos de seguridad. Los 10 riesgos de seguridad de la nube de OWASP (“Category:OWASP Cloud - 10 Project - OWASP,” n.d.).
	Asegúrese de que cualquier codificación de interfaz web basada en la nube esté escrita para no permitir contraseñas débiles	
	Asegúrese de que toda la codificación de la interfaz web basada en la nube esté escrita para incluir un mecanismo de bloqueo de cuenta	
	Implementar la autenticación de dos factores para interfaces web basadas en la nube	
	Asegúrese de que toda la codificación de la interfaz de la nube se haya probado para las vulnerabilidades de XSS, SQLi y CSRF	
	Asegúrese de que todas las interfaces de nube utilicen el cifrado de transporte	

	Asegúrese de que las interfaces de nube estén escritas para incluir la opción de requerir contraseñas seguras	
	Asegúrese de que las interfaces de nube estén escritas para incluir la opción de forzar la caducidad de la contraseña después de un período específico	
	Asegúrese de que las interfaces de nube estén escritas para incluir la opción de cambiar el nombre de usuario y la contraseña predeterminados	
I7: Interfaz móvil insegura	Asegúrese de que la codificación de cualquier aplicación móvil esté escrita para no permitir contraseñas débiles	Las interfaces móviles a los ecosistemas de IoT requieren seguridad específica. Proyecto móvil OWASP (“OWASP Mobile Security Project - OWASP,” n.d.).
	Asegúrese de que la codificación de cualquier aplicación móvil esté escrita para incluir un mecanismo de bloqueo de cuenta	
	Implemente la autenticación de dos factores para aplicaciones móviles (por ejemplo, ID de Touch de Apple)	
	Asegúrese de que cualquier aplicación móvil utilice el cifrado de transporte	
	Asegúrese de que las interfaces móviles estén escritas para incluir la opción de requerir contraseñas seguras	

	<p>Asegúrese de que las interfaces móviles estén escritas para incluir la opción de forzar la caducidad de la contraseña después de un período específico</p>	
	<p>Asegúrese de que las interfaces móviles estén escritas para incluir la opción de cambiar el nombre de usuario y la contraseña predeterminados</p>	
	<p>Asegúrese de que las interfaces móviles solo recopilen la cantidad mínima de información personal necesaria</p>	
<p>I8: Configurabilidad de seguridad insuficiente</p>	<p>Asegúrese de que las aplicaciones estén escritas para incluir opciones de seguridad de contraseña (por ejemplo, habilitar contraseñas de 20 caracteres o habilitar la autenticación de dos factores)</p>	<p>La seguridad puede ser una propuesta de valor. El diseño debe tener en cuenta una escala móvil de los requisitos de seguridad. Diseñe proyectos con valores predeterminados seguros y permita a los consumidores seleccionar opciones para habilitar o deshabilitar. El diseño de IoT debe ser compatible con la seguridad, ya que las suites de cifrado aumentan y las nuevas tecnologías de seguridad se vuelven ampliamente disponibles. El diseño de IoT debe poder adoptar estas nuevas tecnologías.</p>

	<p>Asegúrese de que las aplicaciones estén escritas para incluir opciones de cifrado (p. Ej., Habilitar AES-256 donde AES-128 es la configuración predeterminada)</p>	<p>Recuerde el ciclo de vida de seguridad de proteger, detectar y reaccionar. Diseñar sistemas para permitir la detección de actividad maliciosa, así como capacidades de autodefensa y un plan de reacción en caso de que se detecte un compromiso. Diseñe todas las etapas del ciclo de vida para que sea evolutiva, de modo que se puedan agregar mejoras a un sistema o dispositivo futuras versiones, actualizaciones o parches.</p>
	<p>Asegúrese de que todas las aplicaciones estén escritas para producir registros para eventos de seguridad</p>	
	<p>Asegúrese de que todas las aplicaciones estén escritas para producir alertas y notificaciones al usuario para eventos de seguridad</p>	
<p>I9: Software / Firmware Inseguro</p>	<p>Asegúrese de que todas las aplicaciones estén escritas para incluir la capacidad de actualización y se puedan actualizar rápidamente cuando se descubren vulnerabilidades</p>	<p>Muchas implementaciones de IoT son ya sea brownfield (es decir, se aplican sobre la infraestructura existente) y / o tienen un ciclo de implementación extremadamente largo. Para mantener la seguridad de los dispositivos a lo largo del</p>

		<p>tiempo, es fundamental planificar los parches y las actualizaciones.</p>
	<p>Asegúrese de que todas las aplicaciones estén escritas para procesar archivos de actualización cifrados y que los archivos se transmitan utilizando el cifrado</p>	<p>La confidencialidad, la integridad y la disponibilidad (CIA) son las principales preocupaciones al proporcionar archivos binarios y actualizaciones a los dispositivos perimetrales. Cifre las actualizaciones antes de la distribución, proporcionando claves de descifrado junto con las instrucciones de descarga a los dispositivos autorizados. Las actualizaciones deben tener firmas criptográficas que utilicen criptografía de clave pública que puedan ser verificadas por los dispositivos. Una firma criptográfica permite la distribución de actualizaciones a través de canales que no son de confianza, como la red de entrega de contenido (CDN), punto a punto o máquina a máquina (M2M).</p>

	<p>Asegúrese de que todas las aplicaciones estén escritas para procesar archivos firmados y luego validar ese archivo antes de la instalación</p>	<p>Los dispositivos siempre deben validar los certificados criptográficos y descartar las actualizaciones que no se hayan entregado o firmado correctamente. Si se utilizan actualizaciones no cifradas, asegúrese de que se proporcione un hash criptográfico de la actualización a través de un canal cifrado para que el dispositivo pueda detectar la manipulación.</p>
		<p>Proporcionar un mecanismo para emitir, actualizar y revocar claves criptográficas también. La administración de claves y el ciclo de vida deben tomarse en consideración antes de la implementación. Esto incluye el SSL trust store, o root trust, en un dispositivo, que puede tener que modificarse durante la vida útil del dispositivo.</p>
<p>I10: Mala Seguridad Física</p>	<p>Asegúrese de que las aplicaciones estén escritas para utilizar un número mínimo de puertos físicos externos (por ejemplo, puertos USB) en el dispositivo</p>	<p>Planee que los dispositivos de borde de IoT caigan en manos maliciosas. Utilice cualquier protección de</p>

		seguridad física disponible. Deshabilite las interfaces de prueba o depuración, utilice los Módulos de seguridad de hardware (HSM), los coprocesadores criptográficos y los Módulos de plataforma confiable (TPM) siempre que sea posible.
	Asegúrese de que no se pueda acceder a todas las aplicaciones a través de métodos no intencionados, como a través de un puerto USB innecesario	Considere las implicaciones de un dispositivo comprometido. No comparta credenciales, aplicaciones o claves criptográficas en múltiples dispositivos para limitar el alcance del daño debido a un compromiso físico.
	Asegúrese de que todas las aplicaciones estén escritas para permitir la desactivación de puertos físicos no utilizados, como USB	Planifique la transferencia de propiedad de dispositivos y asegúrese de que los datos no sean transferibles junto con la propiedad.
	Considere escribir aplicaciones para limitar las capacidades administrativas solo a una interfaz local	
Categoría	Consideración de Seguridad de IoT	Recomendaciones
II: Interfaz web insegura	Asegúrese de que toda la codificación de la interfaz web esté escrita para evitar el uso de contraseñas débiles	Al crear una interfaz web, considere implementar lecciones aprendidas de la

		<p>seguridad de la aplicación web. Utilice un marco que utilice controles de seguridad para garantizar que las vulnerabilidades se mitigan en el código. Asegúrese de planear eventuales actualizaciones o arreglos de seguridad para el marco también. Si usa complementos opcionales para el marco, asegúrese de revisarlos por seguridad (“OWASP Periodic Table of Vulnerabilities - OWASP,” n.d.).</p>
	<p>Asegúrese de que toda la codificación de la interfaz web esté escrita para incluir un mecanismo de bloqueo de cuenta</p>	<p>Implemente y proteja la interfaz web de la misma forma que lo haría con cualquier aplicación web. Utilice protocolos de transporte encriptados si es posible, asegurándose de validar los certificados. Limite el acceso de cualquier manera posible. Suponga que los usuarios no cambiarán la configuración, así que implemente de forma segura</p>

		con credenciales sólidas ya establecidas.
	Asegúrese de que toda la codificación de la interfaz web se haya probado para las vulnerabilidades de XSS, SQLi y CSRF	
	Asegúrese de que cualquier interfaz web tenga la capacidad de usar HTTPS para proteger la información transmitida	
	Asegúrese de que toda la codificación de la interfaz web esté escrita para permitir al propietario cambiar el nombre de usuario y la contraseña	
	Considere el uso de firewalls de aplicaciones web para proteger cualquier interfaz web	
I2: Autenticación / Autorización Insuficiente	Asegúrese de que las aplicaciones estén escritas para requerir contraseñas seguras donde se necesita autenticación	Consulte la hoja de referencia de autenticación de OWASP
	Asegúrese de que la aplicación tenga en cuenta los entornos multiusuario e incluya funcionalidad para la separación de roles	
	Implementar la autenticación de dos factores cuando sea posible	
	Asegurar que los mecanismos de recuperación de contraseña estén escritos para funcionar de manera segura	
	Asegúrese de que las aplicaciones estén escritas para incluir la opción de requerir contraseñas seguras	
	Asegúrese de que las aplicaciones estén escritas para incluir la opción de forzar la	

	caducidad de la contraseña después de un período específico	
	Asegúrese de que las aplicaciones estén escritas para incluir la opción de cambiar el nombre de usuario y la contraseña predeterminados	
I3: Servicios de red inseguros	Asegúrese de que las aplicaciones que utilizan servicios de red no respondan de manera deficiente a los ataques de desbordamiento de búfer, confusión o denegación de servicio	Intente utilizar pilas e interfaces de red probadas y comprobadas que manejen las excepciones con elegancia. Asegúrese de que las interfaces de prueba o mantenimiento estén deshabilitadas o protegidas adecuadamente. Evite exponer protocolos no autenticados (como TFTP) o canales no cifrados (como telnet) si es posible. Considere la superficie de ataque que presentan los servicios de red del dispositivo. Desactive los servicios innecesarios e implemente medidas para proteger los servicios requeridos, detectar actividades maliciosas y reaccionar a un ataque con medidas como bloqueos o reglas de firewall temporales.

	Asegúrese de que los puertos de prueba de las aplicaciones estén fuera de servicio antes de ir a producción	
I4: Falta de cifrado de transporte	Asegúrese de que todas las aplicaciones estén escritas para hacer uso de la comunicación cifrada entre dispositivos y entre dispositivos e Internet.	Utilice protocolos cifrados siempre que sea posible para proteger todos los datos en tránsito. Cuando no sea posible el cifrado de protocolo, considere la posibilidad de cifrar los datos antes de la transferencia.
	Utilice las prácticas de encriptación recomendadas y aceptadas y evite los protocolos propietarios.	
	Considere hacer una opción de firewall disponible para la aplicación	
I5: Problemas de privacidad	Asegúrese de que solo se recopile la cantidad mínima de información personal de los consumidores	Los datos pueden presentar problemas de privacidad involuntarios cuando se agregan. Como regla general, recopilar la mínima cantidad de datos posible. Consulte con científicos de datos, equipos legales y de cumplimiento para determinar el riesgo de recolección y almacenamiento de datos. Considere las implicaciones del consentimiento y el hecho de

		que los dispositivos de IoT pueden no presentar una interfaz para recopilar el consentimiento y pueden recopilar pasivamente datos sobre personas distintas de los propietarios y operadores. IoT puede recopilar información sobre personas que no pueden dar su consentimiento (como menores de edad) y la recopilación de datos debe modificarse en consecuencia.
	Asegúrese de que todos los datos personales recopilados estén protegidos adecuadamente mediante el cifrado en reposo y en tránsito	Consulte también los 10 principales riesgos de privacidad de OWASP (“OWASP Top 10 Privacy Risks Project - OWASP,” n.d.).
	Asegurar que los datos sean anónimos o anónimos	
	Asegurar que los usuarios finales tengan una opción para los datos recopilados más allá de lo que se necesita para el correcto funcionamiento del dispositivo	
I6: Interfaz de nube insegura	Asegúrese de que todas las interfaces en la nube se revisen para detectar vulnerabilidades de seguridad (por ejemplo, interfaces API y interfaces web basadas en la nube)	La seguridad en la nube presenta consideraciones de seguridad únicas, así como contramedidas. Asegúrese de consultar a su proveedor de la

		nube sobre las opciones para los mecanismos de seguridad. Consulte los documentos de los 10 riesgos de seguridad de la nube de OWASP (“Category:OWASP Cloud - 10 Project - OWASP,” n.d.)
	Asegúrese de que cualquier codificación de interfaz web basada en la nube esté escrita para no permitir contraseñas débiles	
	Asegúrese de que toda la codificación de la interfaz web basada en la nube esté escrita para incluir un mecanismo de bloqueo de cuenta	
	Implementar la autenticación de dos factores para interfaces web basadas en la nube	
	Asegúrese de que toda la codificación de la interfaz de la nube se haya probado para las vulnerabilidades de XSS, SQLi y CSRF	
	Asegúrese de que todas las interfaces de nube utilicen el cifrado de transporte	
	Asegúrese de que las interfaces de nube estén escritas para incluir la opción de requerir contraseñas seguras	
	Asegúrese de que las interfaces de nube estén escritas para incluir la opción de forzar la caducidad de la contraseña después de un período específico	
	Asegúrese de que las interfaces de nube estén escritas para incluir la opción de cambiar el	

	nombre de usuario y la contraseña predeterminados	
I7: Interfaz móvil insegura	Asegúrese de que la codificación de cualquier aplicación móvil esté escrita para no permitir contraseñas débiles	Las interfaces móviles a los ecosistemas de IoT requieren seguridad específica. Proyecto móvil OWASP (“OWASP Mobile Security Project - OWASP,” n.d.)
	Asegúrese de que la codificación de cualquier aplicación móvil esté escrita para incluir un mecanismo de bloqueo de cuenta	
	Implemente la autenticación de dos factores para aplicaciones móviles (por ejemplo, ID de Touch de Apple)	
	Asegúrese de que cualquier aplicación móvil utilice el cifrado de transporte	
	Asegúrese de que las interfaces móviles estén escritas para incluir la opción de requerir contraseñas seguras	
	Asegúrese de que las interfaces móviles estén escritas para incluir la opción de forzar la caducidad de la contraseña después de un período específico	
	Asegúrese de que las interfaces móviles estén escritas para incluir la opción de cambiar el nombre de usuario y la contraseña predeterminados	
	Asegúrese de que las interfaces móviles solo recopilen la cantidad mínima de información personal necesaria	

<p>I8: Configurabilidad de seguridad insuficiente</p>	<p>Asegúrese de que las aplicaciones estén escritas para incluir opciones de seguridad de contraseña (por ejemplo, habilitar contraseñas de 20 caracteres o habilitar la autenticación de dos factores)</p>	<p>La seguridad puede ser una propuesta de valor. El diseño debe tener en cuenta una escala móvil de los requisitos de seguridad. Diseñe proyectos con valores predeterminados seguros y permita a los consumidores seleccionar opciones para habilitar o deshabilitar. El diseño de IoT debe ser compatible con la seguridad, ya que las suites de cifrado aumentan y las nuevas tecnologías de seguridad se vuelven ampliamente disponibles. El diseño de IoT debe poder adoptar estas nuevas tecnologías.</p>
	<p>Asegúrese de que las aplicaciones estén escritas para incluir opciones de cifrado (p. Ej., Habilitar AES-256 donde AES-128 es la configuración predeterminada)</p>	<p>Recuerde el ciclo de vida de seguridad de proteger, detectar y reaccionar. Diseñar sistemas para permitir la detección de actividad maliciosa, así como capacidades de autodefensa y un plan de reacción en caso de que se detecte un compromiso. Diseñe todas las etapas del ciclo de vida para que sea evolutiva, de modo</p>

		que se puedan agregar mejoras a un sistema o dispositivo futuras versiones, actualizaciones o parches.
	Asegúrese de que todas las aplicaciones estén escritas para producir registros para eventos de seguridad	
	Asegúrese de que todas las aplicaciones estén escritas para producir alertas y notificaciones al usuario para eventos de seguridad	
I9: Software / Firmware Inseguro	Asegúrese de que todas las aplicaciones estén escritas para incluir la capacidad de actualización y se puedan actualizar rápidamente cuando se descubren vulnerabilidades	Muchas implementaciones de IoT son ya sea brownfield (es decir, se aplican sobre la infraestructura existente) y / o tienen un ciclo de implementación extremadamente largo. Para mantener la seguridad de los dispositivos a lo largo del tiempo, es fundamental planificar los parches y las actualizaciones.
	Asegúrese de que todas las aplicaciones estén escritas para procesar archivos de actualización cifrados y que los archivos se transmitan utilizando el cifrado	La confidencialidad, la integridad y la disponibilidad (CIA) son las principales preocupaciones al proporcionar archivos binarios y actualizaciones a los dispositivos perimetrales. Cifre las actualizaciones antes de la

		<p>distribución, proporcionando claves de descifrado junto con las instrucciones de descarga a los dispositivos autorizados. Las actualizaciones deben tener firmas criptográficas que utilicen criptografía de clave pública que puedan ser verificadas por los dispositivos. Una firma criptográfica permite la distribución de actualizaciones a través de canales que no son de confianza, como la red de entrega de contenido (CDN), punto a punto o máquina a máquina (M2M).</p>
	<p>Asegúrese de que todas las aplicaciones estén escritas para procesar archivos firmados y luego validar ese archivo antes de la instalación</p>	<p>Los dispositivos siempre deben validar los certificados criptográficos y descartar las actualizaciones que no se hayan entregado o firmado correctamente. Si se utilizan actualizaciones no cifradas, asegúrese de que se proporciona un hash criptográfico de la actualización a través de un canal cifrado para que el</p>

		dispositivo pueda detectar la manipulación.
		Proporcionar un mecanismo para emitir, actualizar y revocar claves criptográficas también. La administración de claves y el ciclo de vida deben tomarse en consideración antes de la implementación. Esto incluye el SSL trust store, o root trust, en un dispositivo, que puede tener que modificarse durante la vida útil del dispositivo.
I10: Mala Seguridad Física	Asegúrese de que las aplicaciones estén escritas para utilizar un número mínimo de puertos físicos externos (por ejemplo, puertos USB) en el dispositivo	Planee que los dispositivos de borde de IoT caigan en manos maliciosas. Utilice cualquier protección de seguridad física disponible. Deshabilite las interfaces de prueba o depuración, utilice los Módulos de seguridad de hardware (HSM), los coprocesadores criptográficos y los Módulos de plataforma confiable (TPM) siempre que sea posible.
	Asegúrese de que no se pueda acceder a todas las aplicaciones a través de métodos no	Considere las implicaciones de un dispositivo

	intencionados, como a través de un puerto USB innecesario	comprometido. No comparta credenciales, aplicaciones o claves criptográficas en múltiples dispositivos para limitar el alcance del daño debido a un compromiso físico.
	Asegúrese de que todas las aplicaciones estén escritas para permitir la desactivación de puertos físicos no utilizados, como USB	Planifique la transferencia de propiedad de dispositivos y asegúrese de que los datos no sean transferibles junto con la propiedad.
	Considere escribir aplicaciones para limitar las capacidades administrativas solo a una interfaz local	

Nota. Fuente: Elaboración propia

Luego de la evaluación y aplicación de la prueba a un sistema IoT Smart House, se recomienda a los fabricantes que una vez se lleven a cabo los controles propuestos por el proyecto OWASP IoT, es importante que los desarrolladores de estos sistemas complementen sus buenas prácticas bajo las consideraciones de seguridad del marco de IoT.

Consideraciones de seguridad del marco de IoT

Las siguientes consideraciones fueron tomadas del proyecto OWASP de IoT, como herramienta a los lectores para las posibles soluciones a las vulnerabilidades encontradas.

El diseño de una solución segura de IoT depende de una serie de consideraciones de seguridad. Una de las consideraciones más importantes es el uso de un marco de IoT seguro para crear su ecosistema. El uso de un marco seguro garantiza que los desarrolladores no pasen por

alto las consideraciones de seguridad y permite un rápido desarrollo de aplicaciones. Lo ideal es que un marco contenga componentes de seguridad integrados en el marco de manera tal que proporcione seguridad por defecto que los desarrolladores no tengan que pensar. Esto libera a los desarrolladores y arquitectos para centrarse en las características y capacidades sin cargar sus esfuerzos de desarrollo con consideraciones de seguridad (o errores) (“Evaluación del Marco de IoT - OWASP,” n.d.).

El propósito de este documento (“Evaluación del Marco de IoT - OWASP,” n.d.), es describir un conjunto de criterios de evaluación independientes del proveedor que los desarrolladores y arquitectos pueden usar para medir las fortalezas de seguridad relativas de los marcos de desarrollo de IoT. Esto debería servir como un punto de referencia útil, así como un ímpetu para que los proveedores produzcan marcos de desarrollo de IoT más robustos para abordar los numerosos problemas de seguridad que, por lo tanto, tienen IoT.

Los criterios de evaluación se dividen en cuatro secciones distintas. Estas secciones son representativas de los arquetipos típicos del sistema de IoT. Cada sección tiene preocupaciones específicas relacionadas con la seguridad que se describen en los criterios de evaluación del marco para esa sección. Estas secciones son:

- Borde
- Puerta
- Plataforma en la nube
- Móvil

Definiciones

El código de borde que se ejecuta en los dispositivos reales de IoT. A menudo, los componentes de los bordes tienen recursos limitados u operan en entornos aislados. Un dispositivo de puerta de enlace se usa a menudo para agregar y puentear comunicaciones desde dispositivos de borde. El borde, o pasarela, a menudo se comunicará con algún tipo de componente de la nube, a menudo un servicio web. Este componente podría implementarse en un centro de datos de la empresa o en un entorno de computación en la nube pública. El componente de la nube a menudo admite interfaces de usuario complejas, capacidades de análisis y proporciona acceso a los back-end de agregación de datos. Finalmente, muchos ecosistemas de IoT consisten en componentes de aplicaciones móviles que permiten a los usuarios interactuar con el ecosistema a través de teléfonos inteligentes o tabletas (“Evaluación del Marco de IoT - OWASP,” n.d.).

Borde.

El borde es el dispositivo físico real que conforma el ecosistema de IoT. Tenga en cuenta que en muchas implementaciones, el borde es heterogéneo, lo que significa que está compuesto por cualquier número de dispositivos con diferente hardware, sistemas operativos, redes y capacidades y recursos de comunicaciones. Un marco ideal proporcionará componentes multiplataforma para que el código perimetral se pueda implementar en cualquier lugar, desde un entorno completo, a un sistema operativo integrado, a un sistema operativo móvil, a una computadora de escritorio en toda regla, y así sucesivamente (“Evaluación del Marco de IoT - OWASP,” n.d.).

Consideraciones marco para el componente Borde (sensores)

Cifrado de comunicaciones.

Las comunicaciones cifradas deben ocurrir de extremo a extremo siempre que sea posible. Tenga en cuenta que algunas comunicaciones pueden pasar a través de una barrera, como una puerta de enlace o un equilibrador de carga, que puede afectar al cifrado de extremo a extremo. El cifrado permite que los puntos finales validen la identidad (por ejemplo, a través de certificados x509 y raíces de confianza) para garantizar que las comunicaciones no puedan ser interceptadas o redirigidas.

Cifrado de almacenamiento.

Los datos confidenciales en el borde están sujetos a robo o exposición a menos que se almacenen con las consideraciones de seguridad adecuadas. Los marcos deberían ofrecer algún tipo de almacenamiento local seguro para los datos que lo protegen de aplicaciones malintencionadas locales, sistemas operativos comprometidos o propietarios / operadores malintencionados. Los datos confidenciales pueden incluir lectura de sensores, ajustes de configuración, credenciales de autenticación o claves criptográficas.

Registro fuerte.

El marco debe ofrecer un registro robusto, incluido el registro de eventos de seguridad. Los eventos de registro deben ser personalizables e informar eventos confidenciales en un formato utilizable para usuarios finales, administradores y operadores. Los registros a menudo proporcionan evidencia forense de abuso, por lo que la integración con formatos de registro comunes (como los registros de eventos de Windows o el syslog de Unix), permite la integración en sistemas de monitoreo más robustos.

Actualizaciones automáticas y / o informes de versión.

Mantener el software actualizado y permitir parches y actualizaciones es fundamental para un marco seguro. El marco debe identificar claramente la versión en ejecución y permitir parches y actualizaciones de software. Un proceso de actualización automática libera a los usuarios de tener que actualizar los sistemas manualmente, lo que aumenta la posibilidad de que los sistemas se mantengan actualizados.

Verificación de actualización.

Las actualizaciones deben enviarse a través de un canal seguro y verificarse después de la descarga para garantizar que las actualizaciones sean legítimas. La firma (y comprobación) binaria y los hash de actualización entregados a través de un canal encriptado y verificado garantizan que las actualizaciones maliciosas no estén instaladas en un dispositivo. Tenga en cuenta que el acceso físico puede permitir que un atacante "cargue de lado" un binario para colocarlo directamente en un dispositivo, por lo que las actualizaciones deben verificarse antes de la instalación en lugar de simplemente verificar una descarga.

Capacidades de identificación criptográfica.

Los ecosistemas de IoT están compuestos principalmente de sistemas autónomos que son extremadamente capaces de realizar operaciones criptográficas complejas. Los marcos deben admitir capacidades criptográficas para verificar componentes confiables (como pasarela, nube o dispositivos móviles) e incluir la administración criptográfica del ciclo de vida. Esto significa respaldar la emisión y reemisión de material criptográfico, la caducidad de los certificados criptográficos, un mecanismo de revisión de revocación y revocación y un sistema de firma de material clave. Esta capacidad permite una autenticación criptográfica fuerte, lo cual es

particularmente importante con la autenticación de máquina a máquina (M2M) y el cifrado de comunicaciones.

Sin contraseñas por defecto.

El marco debe admitir credenciales personalizadas que pueden ser creadas, configuradas y restablecidas por el operador. El marco debe evitar las credenciales predeterminadas o compartidas en todo el ecosistema. Las credenciales incluyen componentes de autenticación local, así como componentes de autenticación a la nube, pasarela, dispositivos móviles u otros dispositivos del ecosistema.

Autenticación local fuerte.

El marco debe proporcionar una fuerte autenticación de los operadores al borde. Cuando sea posible, esto debe incluir contraseñas complejas y autenticación multifactor. El mecanismo de autenticación debe informar o registrar los intentos de autenticación fallidos y proporcionar un retraso exponencial o un mecanismo de bloqueo para evitar ataques de fuerza bruta.

Funciones de seguridad fuera de línea.

El marco debe asumir que el componente de borde puede perder conectividad y recurrir a características de seguridad local en ausencia de recursos de red. Estas características de seguridad fuera de línea deben ser tan robustas como las características en línea para evitar que los atacantes interrumpen las comunicaciones y degraden las contramedidas de seguridad.

Almacén de confianza de raíz configurable.

Las raíces criptográficas de la confianza son críticas para el uso de certificados para la validación de identidad. Estas tiendas deben ser configurables para agregar nuevos certificados y

vencer o eliminar certificados revocados para mantener la seguridad compatible hacia adelante. El marco debe hacer cumplir los controles sobre la capacidad de manipular la raíz de confianza. Dispositivo y autenticación del propietario.

El marco debe reconocer que en un ecosistema de IoT el dispositivo puede necesitar autenticarse como identidad propia o de intermediario de un propietario u operador. El modelo de identidad del marco debe reconocer las necesidades únicas de acceso y autenticación tanto para el componente autónomo como para los usuarios humanos.

Consideraciones de propiedad transitiva.

Los dispositivos de IoT a menudo se venden o la propiedad se transfiere. El marco debe permitir que el dispositivo sea borrado, reiniciado o que tenga datos compartimentados o destruidos para proteger la información del propietario. Ya sea que el dispositivo sea una pieza fija en una ubicación física cuyo propietario pueda cambiar, o que sea físicamente transferible a un propietario potencialmente hostil o competitivo, el marco debe tener en cuenta la naturaleza transitiva del dispositivo y permitir la protección de la información en consecuencia.

Capacidades defensivas.

El marco debe proporcionar mecanismos para detectar actividades maliciosas y anómalas o integrarse fácilmente en productos de protección de malware o detección de anomalías en el lado del dispositivo. En la medida de lo posible, el marco debe soportar un componente de borde de autodefensa.

Verificación de complementos o extensiones, informes y actualizaciones.

Las adiciones y extensiones de los componentes perimetrales deben validarse antes de la instalación por parte del marco. El marco debe admitir las capacidades de generación de informes y actualizaciones para las extensiones de la misma manera que para el núcleo.

Asegurar las capacidades M2M.

El marco debe ser compatible con la confianza, autorización, verificación y autenticación de máquina a máquina. En la medida de lo posible, este soporte debe extenderse a las capacidades fuera de línea para evitar un punto único de falla en una plataforma o pasarela. El marco podría ser compatible con la confianza transitiva, de modo que un propietario podría certificar una serie de dispositivos que luego podrían autenticarse y confiar basándose en el propietario, independientemente del dispositivo o plataforma en el ecosistema. La plataforma o la pasarela también pueden conferir confianza transitiva para las comunicaciones M2M.

Interfaz web segura.

Los marcos que proporcionan una interfaz para componentes de borde deben utilizar una interfaz que aborde el Top 10 de OWASP como mínimo. En la medida de lo posible, las interfaces web deben construirse con marcos de desarrollo de aplicaciones web que garanticen contramedidas de seguridad contra vulnerabilidades comunes, como la omisión de autenticación, los scripts entre sitios y la falsificación de solicitudes entre sitios. Las interfaces web deben presentarse a través de TLS (HTTPS) y no deben usar certificados autofirmados o no válidos. En la medida de lo posible, el marco debe limitar el acceso a la interfaz web para evitar el uso o abuso no autorizado.

Utilizar pilas y protocolos de red establecidos y probados.

Los marcos deberían utilizar pilas y protocolos de red bien soportados para evitar vulnerabilidades de seguridad comunes en pilas y protocolos más nuevos, no probados o exóticos. Los marcos deberían limitar el número de protocolos al mínimo posible y deberían proporcionar protocolos o pilas en un estado de desactivado por defecto para limitar la superficie de ataque.

Utilice los componentes de terceros más recientes y actualizados.

Los marcos deben usar componentes de terceros actualizados, así como la capacidad de informar sobre las versiones y actualizar estos componentes a medida que se actualicen o estén disponibles actualizaciones de seguridad. El marco debe garantizar que las actualizaciones se distribuyan a través de un canal seguro y se verifiquen antes de la instalación.

Capacidad para utilizar dispositivos de hardware.

El marco debe admitir el uso de cualquier función de seguridad de hardware disponible, como los Módulos de seguridad de hardware (HSM), los Módulos de plataforma de confianza (TPM) y los coprocesadores criptográficos. El marco puede no requerir estos componentes, pero debe utilizarlos si están disponibles.

Soporte de autenticación multifactor.

El marco debe admitir la autenticación de múltiples factores para el dispositivo y / o cualquier operador, si es posible.

Soporta autenticación y funcionalidad temporal y espacial.

Los dispositivos de IoT pueden moverse y el marco debería tener la capacidad de ajustar los permisos en función del espacio y el tiempo. El marco debe admitir los permisos de

ubicación utilizando cualquier número de sensores en un dispositivo de borde y también debe admitir un modelo de permisos que pueda cambiar según las reglas de tiempo.

Hace un seguimiento y contiene datos de fuentes potencialmente contaminadas (inseguras).

Es posible que se requiera que los dispositivos de IoT procesen datos de canales que no se pueden proteger. El marco debe permitir algún tipo de etiquetado o saneamiento de datos para rastrear y contener datos de fuentes no confiables.

Las características (interfaces) están deshabilitadas por defecto.

El marco debe esforzarse por deshabilitar tantos servicios y funciones como sea posible de manera predeterminada, permitiendo a los desarrolladores y la configuración de implementación habilitar las funciones según sea necesario para minimizar la superficie de ataque. El marco debe permitir informes de configuración y, posiblemente, cambios de configuración remota para responder a cambios en el ecosistema.

Escrito en un lenguaje de programación de tipo seguro o sujeto a escrutinio.

Los componentes del marco para dispositivos perimetrales deben escribirse en lenguajes de programación que posean contramedidas de seguridad y demuestren un historial de seguridad sólida. Los componentes de la infraestructura del marco escritos en lenguajes propensos a problemas de seguridad, como C, deben examinarse rigurosamente para garantizar que no existan vulnerabilidades a nivel de código, como los desbordamientos de búfer.

No emplea secretos en el código.

Los componentes del borde del marco deben ser diseñados de manera tal que reconozcan la probabilidad de ingeniería inversa y compromiso físico y empleen contramedidas defensivas para proteger cualquier secreto en el componente.

Control de dispositivos y capacidades de gestión.

El marco debe habilitar el monitoreo de la plataforma del dispositivo, y posiblemente las capacidades de administración, para permitir la detección de debilidades de seguridad o vulnerabilidades en otros componentes en el borde.

Puerta.

La puerta de enlace a menudo admitirá dispositivos de borde débil, o permitirá que los dispositivos de borde conecten redes a componentes de la nube. Las puertas de enlace pueden servir como agregación de comunicaciones y controlar los cuellos de botella y pueden permitir una interfaz sencilla entre una red local insegura pero confiable, y una conexión segura a la Internet pública no confiable. Muchas veces, las puertas de enlace admiten protocolos de rango limitado o propietarios de dispositivos de borde y, en muchos ecosistemas, la puerta de enlace y el borde pueden ser sinónimos, con sensores que se comunican con el borde que hace que esas comunicaciones entren en contacto con el ecosistema de IoT. Una pasarela puede, o puede, no tener ningún tipo de interfaz de usuario, lo que puede presentar ventajas y limitaciones para el dispositivo. Normalmente, las puertas de enlace tienen una mayor disponibilidad de recursos que los dispositivos de borde y ejecutan pilas de sistemas operativos completos.

Consideraciones marco para el componente Gateway Comunicaciones cifradas multidireccionales.

La puerta de enlace debe hacer cumplir las comunicaciones seguras para no degradar la seguridad de los mensajes en cualquier dirección siempre que sea posible. A veces, una puerta de enlace puenteará los canales de comunicación seguros y no seguros, en cuyo caso se debe prestar atención a la interceptación de datos, la manipulación y la inyección en puntos finales inseguros. La puerta de enlace debe proporcionar capacidades para segmentar y aislar las comunicaciones cuando sea posible también.

Fuerte autenticación de componentes (borde, plataforma, usuario)

Los componentes Edge deben proporcionar mecanismos de autenticación tan sólidos como cualquier otro componente en el marco. Cuando sea posible, la puerta de enlace debe autenticarse de forma multidireccional para garantizar comunicaciones confiables en el borde y en la nube. Las capacidades criptográficas en la autenticación de pasarela deben ser un componente sólido de la solución de marco.

Almacenamiento.

La puerta de enlace puede servir como un punto único de falla (o ataque) en el ecosistema y debe almacenar solo la cantidad mínima de información, en un formato encriptado si es posible.

Denegación de servicio y reproducción de mitigación de ataques.

La puerta de enlace debe ser capaz de detectar y resistir ataques desde el borde, incluida la suplantación de identidad, la reproducción y las comunicaciones excesivas. El marco debe admitir la capacidad de la puerta de enlace para registrar, alertar y responder a la actividad maliciosa o anómala detectada por los componentes de borde.

Registro y alerta.

La puerta de enlace tendrá acceso a un volumen de tráfico y debería poder iniciar sesión y alertar según el registro de eventos. El marco podría incluir la integración con servicios de registro estándar o sistemas de detección de intrusos. El marco incluso podría admitir métodos alternativos para alertar en la puerta de enlace (como SMS).

Detección de anomalías y capacidades de reporte.

El marco debe permitir a la pasarela observar, establecer una línea de base y monitorear el tráfico de comunicaciones y el comportamiento de los componentes. La puerta de enlace será especialmente adecuada para monitorear el tráfico hacia y desde la nube y debe admitir la detección de anomalías o integrarse fácilmente con los sistemas de detección de anomalías e intrusos. Un marco de puerta de enlace sólido podría incluso admitir capacidades de prevención de intrusiones para excluir a actores sospechosos del ecosistema.

Utilice los componentes de terceros más recientes y actualizados.

Los marcos deben usar componentes de terceros actualizados, así como la capacidad de informar sobre las versiones y actualizar estos componentes a medida que se actualicen o estén disponibles actualizaciones de seguridad. El marco debe garantizar que las actualizaciones se distribuyan a través de un canal seguro y se verifiquen antes de la instalación.

Actualizaciones automáticas y / o informes de versión.

Mantener el software actualizado y permitir parches y actualizaciones es fundamental para un marco seguro. El marco debe identificar claramente la versión en ejecución y permitir parches y actualizaciones de software. Un proceso de actualización automática libera a los

usuarios de tener que actualizar los sistemas manualmente, lo que aumenta la posibilidad de que los sistemas se mantengan actualizados.

Nube.

El componente de nube de un ecosistema de IoT se refiere a la porción central de agregación y gestión de datos del ecosistema. El componente de la nube generalmente consistirá de una capa de almacenamiento de datos (como una base de datos), análisis e informes, administración del ecosistema, una interfaz web y otros componentes como correo electrónico, copias de seguridad, etc. El componente de la nube puede o no estar Alojado en infraestructura de nube pública. El acceso al componente de la nube suele estar restringido, especialmente a la infraestructura de soporte. El componente de la nube conlleva un riesgo significativo porque es el punto central de agregación para la mayoría de los datos en el ecosistema y, a menudo, incluye un componente de comando y control (C2) que permite la manipulación de otros componentes, incluida la entrega y distribución de actualizaciones y extensiones.

Consideraciones marco para el componente de la nube Comunicaciones cifradas.

El componente de la nube debe admitir las comunicaciones cifradas, incluidos los certificados de seguridad, para identificarse con otros componentes del ecosistema. El marco debe admitir certificados criptográficos para identificar otros componentes también, para la verificación de identidad bidireccional.

Interfaz web segura.

La interfaz web en la nube debe construirse utilizando una tecnología que convierta soluciones para vulnerabilidades de aplicaciones web comunes en el código (como un marco de desarrollo de aplicaciones web seguras). La aplicación debe mitigar el Top 10 de OWASP como mínimo.

Autenticación.

El componente de la nube debe permitir la autenticación compleja, incluida la autenticación multifactor. La interfaz debe incluir también funciones de mitigación de enumeración de fuerza bruta y anti-cuenta. La interfaz no debe enviarse con las credenciales predeterminadas y debe permitir a los usuarios configurar fácilmente, y restablecer con seguridad, la información de la cuenta.

Credenciales de autenticación segura.

Las credenciales de autenticación, en cualquier forma (contraseñas, identificadores de dispositivos, etc.), deben incluirse adecuadamente en forma de sal y hash, cifradas, antes del almacenamiento (https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet). Los mecanismos de almacenamiento deben ser uniformemente sólidos y deben extenderse más allá de las contraseñas para abordar las credenciales de autenticación de la máquina en cualquier forma.

Almacenamiento encriptado.

El componente de nube de un ecosistema de IoT es a menudo el sistema de registro y agregación de toda la implementación. Siempre que sea posible, el marco debe admitir el cifrado de datos en reposo, incluso en la capa de persistencia, así como en cualquier mecanismo de exportación o copia de seguridad.

Capacidad para utilizar comunicaciones cifradas a la capa de almacenamiento.

Las comunicaciones entre la interfaz de la nube y la capa de agregación de datos y la capa de persistencia de datos deben utilizar un canal de comunicaciones cifrado. El marco debe utilizar comunicaciones encriptadas de forma predeterminada para evitar que los datos se expongan en tránsito.

Capacidad de clasificación de datos y segregación.

El componente de la nube recopilará una variedad de datos variables de otros componentes en el ecosistema. Algunos datos pueden ser altamente sensibles y otros datos pueden ser benignos. El marco debe proporcionar las capacidades para clasificar los datos y protegerlos según la clasificación. Los controles de la interfaz deben limitar el acceso y la exposición de datos confidenciales según la clasificación.

Informes y alertas de eventos de seguridad.

El componente de la nube a menudo tiene la mayor visibilidad de la función del ecosistema y los controles de seguridad son críticos en esta capa. El componente de la nube debe tener capacidades sólidas de monitoreo de eventos de seguridad, informes y alertas. El marco debe permitir que el componente de la nube detecte y reaccione ante actividades maliciosas. El componente de la nube debe poder segregar a los malos actores, limitar el acceso a las partes malintencionadas e integrarse fácilmente con los sistemas de detección y prevención de intrusos y registro de terceros.

Actualizaciones automáticas y verificación de actualizaciones.

El marco debe reconocer la necesidad de actualizaciones y respaldar las actualizaciones fáciles y la verificación de actualización del componente de la nube. El marco debe tener una interfaz fácil para las versiones de informes y las actualizaciones disponibles. Idealmente, el marco debería admitir actualizaciones automáticas del componente de la nube. La alerta automática de actualizaciones fuera de banda (por ejemplo, a través de SMS o correo electrónico) es deseable para la actualización automática de componentes.

Utilice los componentes de terceros más recientes y actualizados.

Los marcos deben usar componentes de terceros actualizados, así como la capacidad de informar sobre las versiones y actualizar estos componentes a medida que se actualicen o estén disponibles actualizaciones de seguridad. El marco debe garantizar que las actualizaciones se distribuyan a través de un canal seguro y se verifiquen antes de la instalación.

Verificación de complementos o extensiones, informes y actualizaciones.

El componente de la nube a menudo tendrá mejoras y opciones de personalización en forma de extensiones y complementos. El marco debe permitir actualizaciones modulares y monitoreo de estos componentes. Lo ideal sería que el marco se distribuyera con un conjunto mínimo de características habilitadas de forma predeterminada para limitar la superficie de ataque. Una interfaz de contabilidad fácil para extensiones y complementos debe estar disponible para los administradores. La alerta automática de actualizaciones fuera de banda (por ejemplo, a través de SMS o correo electrónico) es deseable para la actualización automática de componentes.

Segregación y aislamiento de la interfaz según la utilidad (dispositivo, interfaz de administración, interfaz de usuario, etc.).

El componente de nube de un ecosistema de IoT a menudo se comunicará con varios otros componentes del ecosistema. La utilidad necesaria para comunicarse con un dispositivo integrado será necesariamente muy diferente de la utilidad proporcionada a un usuario humano de una interfaz web. El marco debe permitir la segregación y protección de los canales de comunicaciones para reducir la superficie de ataque y hacer cumplir el principio de privilegio mínimo. Los atacantes pueden tratar de explotar las vulnerabilidades disponibles para las interfaces que no son humanas, como las API de dispositivos. En la medida de lo posible, el marco debe limitar el acceso según el rol y el uso. Los certificados criptográficos utilizados para el acceso específico pueden ser útiles para este objetivo. Como mínimo, el marco debe proporcionar interfaces especialmente diseñadas para el uso previsto.

Cortafuegos de nivel de aplicación y capacidades defensivas (bloqueo de IP, regulación, administración de cuentas, etc.).

El componente de la nube debe tener la capacidad de bloquear ciertos actores, controlar la actividad maliciosa y responder a las amenazas. Esto debe incluir la capacidad del marco para realizar restablecimientos masivos de credenciales, desaprobaciones y otras capacidades de respuesta a desastres e infracciones.

Asegurar la segregación del ecosistema en el caso de soluciones multi-tenant.

En el caso de que el marco admita una base de clientes diversa en un solo ecosistema, el marco debe proporcionar una segregación adecuada y protección de datos. Esto podría incluir capas de almacenamiento de datos dedicadas por cliente o etiquetado de datos para garantizar la segregación y el control de acceso.

Consideraciones de seguridad de la pila (sin interfaz de usuario web para ejecutar código arbitrario).

Al reconocer la complejidad y la multitud de configuraciones de seguridad de componentes, el marco debe admitir soluciones de seguridad de pila completa en el componente de la nube. Esto incluye contramedidas de seguridad e integraciones en todas las capas del componente de la nube, incluida la posible integración con contramedidas de seguridad específicas del proveedor de la nube, como el aislamiento o la detección de intrusos. El componente de la nube debe incluir la gestión segura de la configuración y la integración con otras actualizaciones automáticas del sistema.

Capacidad de auditoria.

En muchos ecosistemas es fundamental hacer un seguimiento de las comunicaciones para garantizar su entrega y el calendario adecuados. Los marcos deberían proporcionar mecanismos para garantizar la entrega de mensajes dirigidos a componentes específicos de borde. Esta característica permitirá la confianza en la auditoría y la resolución de problemas y se puede utilizar para respaldar las garantías de entrega de instrucciones o datos confidenciales de seguridad. Esta auditoría debe ser bidireccional para permitir el seguimiento de los mensajes hasta el borde y la recepción de mensajes desde el borde.

Móvil.

Las interfaces móviles en las implementaciones de IoT varían en capacidades e integración. Algunas aplicaciones móviles simplemente proporcionan informes limitados de datos desde dispositivos perimetrales específicos, otras permiten la manipulación de componentes perimetrales, y otras proporcionan un análisis de vista completo y capacidades de

administración de la nube. Se debe prestar especial atención a los componentes móviles en los ecosistemas de IoT, ya que normalmente se implementan más allá de los límites de la administración de dispositivos, pueden otorgar acceso privilegiado para alterar, adulterar o exponer información confidencial, pueden tener la capacidad de activar dispositivos de borde, son portátiles y Puede caer fácilmente en manos maliciosas.

Consideraciones marco para el componente móvil

Asegurar que el componente móvil impone requisitos de autenticación iguales o superiores a otros componentes

La limitada interfaz y las capacidades de almacenamiento de las aplicaciones móviles a menudo fomentan un mecanismo de autenticación simplista. Al reconocer que los atacantes encontrarán y se dirigirán al componente más débil del ecosistema, el marco debe garantizar que los mecanismos de autenticación móvil no degraden los requisitos de autenticación.

Consideraciones de seguridad de almacenamiento local.

El marco debe tener en cuenta la a veces limitada seguridad de almacenamiento en dispositivos móviles. La amenaza de robo o pérdida también significa que el almacenamiento local podría caer en manos maliciosas. El marco debe limitar estrictamente la cantidad de datos almacenados en el dispositivo y los datos deben cifrarse cuando sea posible.

Capacidades para deshabilitar o revocar componentes móviles en caso de robo o pérdida

El marco debe admitir la capacidad de desaproveccionar componentes móviles de forma rápida y sencilla para admitir la respuesta en caso de robo o pérdida de dispositivos móviles.

Fuerte pista de auditoría de interacciones móviles.

Debido a que el dispositivo móvil puede caer en manos maliciosas, es fundamental mantener un seguimiento de auditoría de seguridad de las interacciones de las aplicaciones móviles con el ecosistema. El marco debe admitir el registro robusto y las credenciales apropiadas para rastrear las interacciones de los componentes móviles para admitir el análisis forense y, en algunos casos, se descubrió que los dispositivos móviles se utilizaron de manera malintencionada después del hecho.

La aplicación móvil debe realizar la verificación criptográfica y la validación de otros componentes.

Cuando sea posible, el marco móvil debe admitir la verificación criptográfica y la validación de los otros componentes durante las interacciones. La correcta verificación y autenticación de los certificados siempre debe llevarse a cabo.

Canales de comunicaciones encriptados.

Los dispositivos móviles son particularmente propensos a ser utilizados en redes hostiles y las comunicaciones cifradas deben ser el marco predeterminado. La aplicación móvil debe funcionar bajo la presunción de un observador hostil que intentará inspeccionar, interceptar, interrumpir, reproducir y manipular el tráfico.

Autenticación multifactor.

Los dispositivos móviles tienen capacidades ampliadas para realizar múltiples factores de autenticación. Los sensores y la biometría deben ser respaldados por el marco para la verificación de seguridad extendida en la plataforma móvil.

Capacidad para utilizar componentes móviles para mejorar la autenticación y alertar sobre otros componentes.

Cuando sea posible, el componente móvil debe integrarse en la autenticación y alertar sobre eventos en otros componentes. Los componentes de borde, puerta de enlace o en la nube pueden alertar sobre el marco móvil, o el marco móvil puede permitir la autenticación multifactor o mejorar la autenticación a otros componentes.

Recomendaciones del Autor

Si el desarrollador desea evaluar un sistema real de IoT, se proponen las siguientes fases:

- Fase 1: Diagnóstico Inicial: En esta fase se debe hacer un reconocimiento del sistemas, es decir saber que se tiene y con que se cuenta, al mismo tiempo realizar un inventario de Hardware y Software (Fichas Técnicas).
- Fase 2: Aplicar Pruebas: Teniendo en cuenta la Tabla de Consideraciones de Seguridad de IoT, propuesta por el proyecto OWASP IoT. Una vez se cumpla con la Fase 1, se realiza la evaluación pertinente.
- Fase 3: Aplicar Controles: Una vez los hallazgos hayan sido detectados se aplican los controles de acuerdo a la Tabla de Consideraciones de Seguridad IoT- Controles propuesta por el Proyecto OWASP IoT.

Conclusiones

Se logró documentar toda la información relacionada con las capas de IoT; Capa de Percepción, de Red, de Nivel Medio, de Aplicación, junto con este estudio se recolectó la información relacionada con los protocolos de Internet, esto con el fin de identificar algunos elementos que serán de gran utilidad en el diseño de la guía de buenas prácticas, mediante el levantamiento, recopilación y organización de toda la información perteneciente al IoT.

Se indagó sobre el proyecto OWASP de IoT, y se tomó como base para el diseño de la guía, teniendo en cuenta los marcos que presenta el OWASP Top 10 IoT, en el que se exponen 10 marcos para realizar las respectivas recomendaciones que deben tener los creadores, diseñadores, desarrolladores y analistas de dispositivos IoT.

Se diseñó una guía de fácil entendimiento, con el fin de que los desarrolladores de sistemas IoT puedan seguir los marcos necesarios, para las mejoras en la seguridad y la vulnerabilidad de sistemas IoT. En esta guía se plantea un ejemplo como prueba para que el desarrollador logre entender mejor el funcionamiento de la misma, esta evalúa el nivel de cumplimiento de las categorías que propone OWASP, para determinar los controles que se deben implementar para las vulnerabilidades detectadas.

Recomendaciones

Se recomienda el estudio de los marcos de seguridad que propone OWASP de IoT antes de comenzar con el diseño, la creación y el desarrollo de sistemas IoT, esto con el fin de que se puedan identificar los problemas de seguridad establecidos principalmente en la red, una de las categorías que se proponen en la guía basadas en el proyecto OWASP es; Interfaz Web Insegura. Es de gran importancia enfocarse en esta categoría ya que los dispositivos utilizados en las Smart House establecen comunicación directa con la red por tanto se ven expuestos frecuentemente a este tipo de vulnerabilidades.

Bibliografía

- (2013). The essence of future smart houses: From embedding ICT to adapting to sustainability principles. *Renewable and Sustainable Energy Reviews*, 24, 593–607. <http://doi.org/10.1016/j.rser.2013.02.032>
- (2013). The essence of future smart houses: From embedding ICT to adapting to
Acerca del proyecto Open Web Application Security - OWASP. (n.d.). Retrieved July 17, 2019, from https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project
- Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8–27. <http://doi.org/10.1016/j.jisa.2017.11.002>
- Borgia, E. (2014). The internet of things vision: Key features, applications and open issues.
- Caivano, D., Cassano, F., Lanzilotti, R., & Piccinno, A. (2018). Towards an IoT model for the assessment of smart devices, 1–3. <http://doi.org/10.1145/3206505.3206587>
- Castañeda Sandoval, C. A., & Comunicación, M. en T. de la I. y la. (2018). Construcción de una guía para implementar controles de seguridad al almacenar datos sensibles en Cloud de empresas de mensajería de Colombia. *Instname: Universidad Pontificia Bolivariana*.
- Category:OWASP Cloud - 10 Project - OWASP. (n.d.). Retrieved July 19, 2019, from https://www.owasp.org/index.php/Category:OWASP_Cloud_-_10_Project
- Chandra, M. L. R., Kumar, B. V., & Sureshbabu, B. (2018). IoT enabled home with smart security. *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS 2017*, 1193–1197. <http://doi.org/10.1109/ICECDS.2017.8389630>
- Communications standards news. (2015). *IEEE Communications Magazine*, 53(9), 5–7. <http://doi.org/10.1109/MCOM.2015.7263365>
- Communications standards news. (2015). *IEEE Communications Magazine*, 53(9), 5–7. <http://doi.org/10.1109/MCOM.2015.7263365>
- Computer Communications*, 54, 1–31. <http://doi.org/10.1016/j.comcom.2014.09.008>
- De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities.
- De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, 27(1), 307–324.

<http://doi.org/10.2308/isis-50422>

de la Espriella, R., & Gómez Restrepo, C. (2018). Teoría fundamentada. *Revista Colombiana de Psiquiatría*. <http://doi.org/10.1016/j.rcp.2018.08.002>

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management.

Evaluación del Marco de IoT - OWASP. (n.d.). Retrieved July 19, 2019, from https://www.owasp.org/index.php/IoT_Framework_Assessment

Evans, D. (2011). *Internet de las cosas*. San José, CA: Cisco Internet Business Solutions Group (IBSG).

Flores, S. U., Berón, M., Riesco, D. E., & Rangel Henriques, P. (2018). Diseño y construcción de sistemas de IoT seguros y escalables. Retrieved from <http://sedici.unlp.edu.ar/handle/10915/67915>

Flores, S. U., Berón, M., Riesco, D. E., & Rangel Henriques, P. (2018). Diseño y construcción de sistemas de IoT seguros y escalables. Retrieved from <http://sedici.unlp.edu.ar/handle/10915/67915>
Future Generation Computer Systems.

Geometry, R., & Analysis, G. (n.d.). *Metodologia de la Investigacion I*.

GhaffarianHoseini, A., Dahlan, N. D., Berardi, U., GhaffarianHoseini, A., & Makaremi, N.

GhaffarianHoseini, A., Dahlan, N. D., Berardi, U., GhaffarianHoseini, A., & Makaremi, N.

González, Y. (2017). El Internet De Las Cosas Y Sus Riesgos Para La Privacidad, 1–10.

Guía de seguridad de IoT - OWASP. (n.d.). Retrieved July 17, 2019, from https://www.owasp.org/index.php/IoT_Security_Guidance

Herrán Ortíz, A. I. (2002). *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*. Dykinson. Retrieved from <https://books.google.es/books?hl=es&lr=&id=CCVT48egc5MC&oi=fnd&pg=PA133&dq=t+ratamiento+de+datos+personales&ots=qUTKKh4SAp&sig=NxMVYo-CAOjzLWV-2iZL-OuqEAw#v=onepage&q&f=false>

Historia de la Internet. (n.d.). Retrieved from www.internet2.edu

Internet de las cosas - una visión general | Temas de ScienceDirect. (n.d.). Retrieved April 20, 2019, from <https://www.sciencedirect.com/topics/computer-science/internet-of-things>

IoT Security Guidance - OWASP. (n.d.). Retrieved July 18, 2019, from https://www.owasp.org/index.php/IoT_Security_Guidance

IoT-una encuesta sobre os marcos de la de seguridad de la io. (s.f.).

- ISO/IEC. (2016). Information technology – Internet of Things Reference Architecture (IoT RA), 20160910. Retrieved from https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf
- La historia de la internet de las cosas | ELESPECTADOR.COM. (n.d.). Retrieved April 20, 2019, from <https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678>
- Marco de seguridad de la io para infraestructuras cibernticas inteligentes. (s.f.).
- OWASP Mobile Security Project - OWASP. (n.d.). Retrieved July 19, 2019, from https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- OWASP Periodic Table of Vulnerabilities - OWASP. (n.d.). Retrieved July 19, 2019, from https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities#Generic_Application_Frameworks
- OWASP Top 10 Privacy Risks Project - OWASP. (n.d.). Retrieved July 19, 2019, from https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
- Partner, M. (2011). • *The «things» in the Internet of Things • How intelligent are objects today?*
- Perez, N. B., Bustos, M. A., Berón, M., & Rangel Henriques, P. (2018). Análisis sistemático de la seguridad en internet of things. Retrieved from <http://sedici.unlp.edu.ar/handle/10915/68387>
- Press, E. (n.d.). “Ciudades Inteligentes”: la tecnología al servicio del ciudadano. Retrieved from <https://www.europapress.es/chance/tendencias/noticia-ciudades-inteligentes-tecnologia-servicio-ciudadano-20110601130049.html>
- Protocolos para la Internet de las cosas | Arrow.com. (n.d.). Retrieved July 18, 2019, from <https://www.arrow.com/es-mx/research-and-events/articles/protocols-for-the-internet-of-things>
- Proyecto OWASP de Internet de las Cosas - OWASP. (n.d.). Retrieved July 18, 2019, from https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- Quesada, S., & Pulido, A. L. (n.d.). *Smart City:Hacia un nuevo paradigma*. Retrieved from <http://aulagreencities.coamalaga.es/wp-content/uploads/2014/05/35.-Smart-City.-Hacia-un-nuevo-paradigma-en-el-modelo-de-ciudad.pdf>
- Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access*. Security: Ongoing Challenges and Research Opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications* (pp. 230–234). IEEE. <http://doi.org/10.1109/SOCA.2014.58>

- Security: Ongoing Challenges and Research Opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications* (pp. 230–234). IEEE. <http://doi.org/10.1109/SOCA.2014.58>
- SEGURIDAD Y PRIVACIDAD PARA LA IO BASADA EN LA NUBE. (s.f.). Seguridad y privacidad para la io basada en la nube. (s.f.). sustainability principles. *Renewable and Sustainable Energy Reviews*, 24, 593–607. <http://doi.org/10.1016/j.rser.2013.02.032>
- Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *The Internet of Things In a Connected World of Smart Objects Executive Summary*. Retrieved from www.accenture.es
The Internet of Things In a Connected World of Smart Objects Executive Summary. Retrieved from www.accenture.es
- The IoT Architecture at the Edge - IoT Central. (n.d.). Retrieved July 17, 2019, from <https://www.iotcentral.io/blog/the-iot-architecture-at-the-edge>
- The OWASP Internet of Things*. (n.d.). Retrieved from <https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf>
- Trinidad Requena, A., Carrero Planes, V., & Soriano Miras, R. M. (2006). *Teoría fundamentada "grounded theory" : la construcción de la teoría a través del análisis interpretacional*. Centro de Investigaciones Sociológicas. Retrieved from <https://books.google.es/books?hl=es&lr=&id=yxtGMuCSDe4C&oi=fnd&pg=PA1&dq=+teoria+fundamentada&ots=3O1jO9X0oN&sig=OSHeuqRHlcE2cknhdoT8fhT-8a0#v=onepage&q&f=false>
- VOSviewer - Visualizing scientific landscapes. (n.d.). Retrieved July 22, 2019, from <https://www.vosviewer.com/>
- Xu, Q., Ren, P., Song, H., & Du, Q. (2016). Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access*.
- Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S. (2014). IoT
- Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. (1 de 2017). Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Communications Magazine*, 55(1), 26-33.
- Zhou, j., cao, z., dong, x., & vasilakos, a. (1 de 2017). Security and privacy for cloud-based iot: challenges. *Ieee communications magazine*, 55(1), 26-33.

Apéndice

Apéndice 1. Analisis Bibliometrico

Se realiza un análisis bibliométrico, este análisis se hace con el fin de hacer una búsqueda bibliográfica, tomando como punto central el objeto de estudio. Teniendo en cuenta que estos análisis son de primordial relevancia en el marco de la evaluación de los contenidos científicos y que al mismo tiempo son de gran utilidad al permitir una aproximación detallada del objeto de estudio “Buenas prácticas en torno a la seguridad del internet de las cosas para las Smart House”, así como la información que se obtiene con el fin de ampliar el área de conocimiento.

El material analizado fueron los artículos originales publicados en la Base de Datos de la Universidad Francisco de Paula Santander Ocaña en el periodo 2012 a 2018. De este material se registró el número de artículos/volumen-año-categoría, clasificadas como artículos de revistas científicas, libros y otros, los indicadores calculados fueron el tipo de documento, idioma, años de publicación. De esta búsqueda se encontraron 300 documentados publicados en estas bases de datos digitales, donde la forma de búsqueda fue basada en Internet de las cosas para poder obtener el análisis realizado.

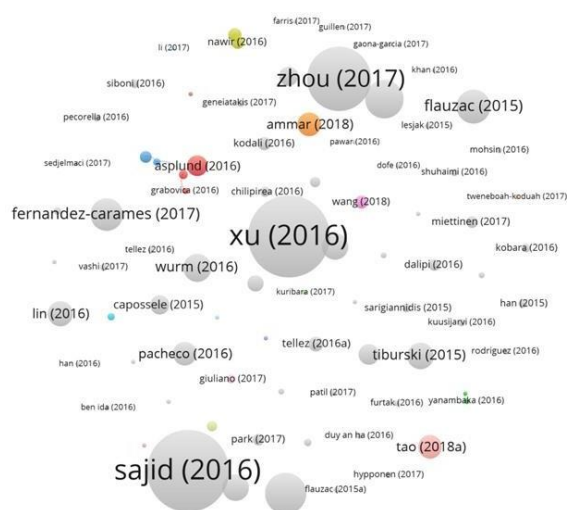


Ilustración 10: Analisis Bibliometrico

Nota. Fuente: (“VOSviewer - Visualizing scientific landscapes,” n.d.)