Revista Ingenio
UFPS Ocaña
"Journal of Engineering Sciences"

Original Article DOI: https://doi.org/10.22463/2011642X.2370

Internet de las Cosas: una revisión de vulnerabilidades, amenazas y contramedidas

Internet of Things: a review of vulnerabilities, threats and countermeasures

Ing. Luis Fernando Gélvez Rodríguez[1], Ph.D. Luz Marina Santos Jaimes[1]

[1]*CICOM, Universidad de Pamplona, Colombia, Orcid: https://orcid.org/0000-0002-8224-0053, https://orcid.org/ 0000-0003-4499-795X, Email: {luisfgelvezr, lsantos}@unipamplona.edu.co*

Como citar: L. F. Gélvez y L. M. Santos, "Internet de las cosas: una revisión de vulnerabilidades, amenazas y contramedidas", *Revista Ingenio*, vol. 17, n°1, pp. 56-64, 2020, doi: https://doi.org/10.22463/2011642x.2370.

Fecha de recibido:14 de agosto de 2019
Fecha aprobación:12 de noviembre de 2019

RESUMEN

Palabras claves:

Amenaza, contramedida, Internet de las Cosas, seguridad, vulnerabilidad.

En la última década con el surgimiento del paradigma de Internet de las Cosas y su gran acogida y expansión en diferentes dominios de aplicación, han surgido nuevos retos que dejan ver una gran problemática en lo referente a la gestión de la seguridad de la información, los cuales representan un riesgo importante para las organizaciones y los usuarios finales que ya están implementando este paradigma en sus actividades y procesos. Frente a esta problemática se han venido desarrollando algunos estudios desde diferentes puntos de vista, abarcando varios dominios de aplicación, pero sin presentar aún una visión unificada de cómo afrontar los riesgos asociados a la implementación de tecnologías de Internet de las Cosas en las organizaciones. El presente estudio está basado en una investigación cualitativa junto con un acercamiento deductivo enfocado a recopilar las vulnerabilidades y amenazas que suelen presentarse de forma específica en entornos que implementan Internet de las Cosas, así como diferentes propuestas para gestionar la seguridad de información frente a los retos emergentes.

ABSTRACT

Keywords:

Threat, countermeasure, Internet of Things, security, vulnerability.

In the last decade with the emergence of the Internet of Things paradigm and its great reception and expansion in different application domains, new challenges have emerged that reveal a great problem in relation to information security management, which represent a significant risk for organizations and end users who are already implementing this paradigm in their activities and processes. Faced with this problem, some studies have been carried out from different points of view, covering various application domains, but without yet presenting a unified vision of how to face the risks associated with the implementation of Internet of Things technologies in organizations. The present study is based on a qualitative research along with a deductive approach focused on collecting vulnerabilities and threats that are specifically presented in environments that implement the Internet of Things are exposed, as well as different proposals to manage information security against emerging challenges.

1. Introducción

Los últimos avances tecnológicos han traído consigo el uso y adquisición de diversos dispositivos con capacidades de conexión a Internet que van desde objetos que hacen parte de nuestra vida cotidiana, como el teléfono, automóvil, electrodomésticos, entre otros, hasta áreas como la salud, la seguridad, la industria o la educación [1–3]. Esta era de la evolución de Internet, en donde la conectividad cubre a los objetos que nos rodean, es lo que se conoce como el Internet de las Cosas (IoT – Internet of Things) [4]. Este nuevo enfoque ha permitido la explotación de los dispositivos a un nivel superior, agilizando tareas y procesos, acortando distancias o incrementando el intercambio de datos y conocimiento [5]. La visión detrás de IoT es permitir que las personas y las cosas inteligentes se conecten en cualquier momento, en cualquier lugar, a cualquier cosa y a cualquier persona, a través de cualquier red y servicio [6]. De acuerdo a esta visión, las áreas de aplicación de IoT aumentarán de forma continua y dramática para cada aspecto de la vida [7], como se ha visto recientemente en la lucha contra la pandemia de COVID-19, siendo IoT útil para capturar datos en tiempo real de los pacientes infectados.

En 2011 el número de sistemas interconectados superaba la población mundial y para el 2012, unos 9 billones de dispositivos ya estaban interconectados [8-9]. El mundo alcanzará en el 2020, 50 billones de dispositivos conectados [10], y se espera que el mercado

Autor para correspondencia
Correo electrónico: luisfgelvezr@unipamplona.edu.co (Luis Fernando Gélvez Rodríguez)

de IoT para el 2025 en aplicaciones como la domótica, hábitos personales y salud permita que cada persona en el planeta tenga por lo menos 25 dispositivos IoT por persona [7-11]. El hecho de que tantos dispositivos con diferente uso o aplicación puedan conectarse a Internet, abre también muchas posibilidades para los atacantes que a diario asechan la red, con lo que se incrementan los riesgos en materia de privacidad, seguridad e integridad de la información y de los usuarios [12]. De acuerdo a [13–15] dichos problemas de seguridad pueden resumirse en 3 aspectos importantes: i)Dominios en expansión, ya que cada objeto en la vida real es mapeado como una entidad virtual, haciendo el ámbito de IoT mucho más grande que el mismo Internet; ii) Ciclo de actividad dinámico, ya que los objetos como entidades virtuales pueden estar activos o inactivos dentro de la red de forma simultánea; iii)Interacciones heterogéneas, ya que los objetos como ciber-entidades poseen atributos sociales que son particularmente importantes para las interacciones a través del espacio.

En el presente estudio, se aborda la revisión sobre la problemática de seguridad de información inherente a implementaciones de IoT, considerando como aspectos iniciales en un proceso de un análisis de riesgos de seguridad los siguientes: i)Primero, conocer cuáles son los niveles que conforman la arquitectura IoT para tener una comprensión clara de los diferentes componentes que hacen parte de dichas implementaciones, las interacciones que se dan entre sí para un mejor análisis de seguridad; ii) Una recopilación de diferentes vulnerabilidades específicas que se presentan en dispositivos y redes IoT, y las amenazas asociadas que pueden tener impacto en la seguridad de la información; iii) Revisión de contramedidas propuestas por diferentes autores para diferentes problemas de seguridad típicos de implementaciones de IoT.

2. Metodología

El artículo origina del desarrollo de una guía de gestión de riesgos de seguridad específica y unificada orientada a la aplicación de IoT en las empresas y/o instituciones; por lo tanto como punto de partida, esté artículo direcciona la siguiente pregunta, ¿Cuáles son los riesgos y medidas de seguridad presentes en la tecnología IoT?. Para dar respuesta, se realizó una revisión sistemática de trabajos en la literatura referentes a vulnerabilidades, amenazas, contramedidas, y soluciones para mitigar los problemas de seguridad derivados de escenarios puntuales que implementan IoT. Se consideraron trabajos realizados en la última década teniendo en cuenta la evolución que ha tenido IoT en este periodo de tiempo. Posteriormente se analizó y clasificó los diferentes trabajos (Figura 1).

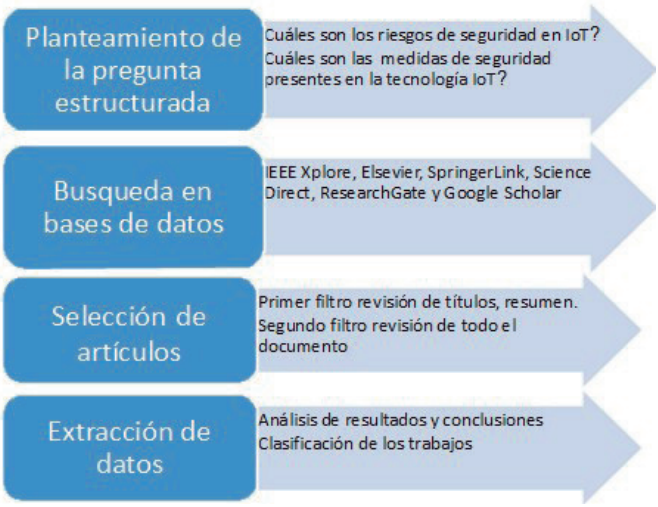

Figura 1. Pasos para el desarrollo del artículo

3. Arquitectura IoT

El estudio de las arquitecturas IoT es clave para la identificación de los activos en un proceso de análisis de riesgos de seguridad, los autores en [16-17] exponen una vista general y simplificada de las interacciones entre los diferentes elementos que intervienen en un ambiente IoT, a través de una arquitectura de cuatro capas en la cual se puede diferenciar claramente el rol que toma cada parte, (Figura 2). En la capa de percepción se encuentran los sensores y dispositivos que capturan los datos del mundo físico, en la capa de red se encuentra toda la infraestructura de comunicaciones encargada de llevar los datos desde los dispositivos IoT hasta las bases de datos, repositorios e infraestructura de procesamiento, en la capa intermedia o Middleware se reciben los datos para ser almacenados y recibir un primer procesamiento, luego la información viaja hasta la capa de aplicación donde las diferentes aplicaciones y servicios la utilizan y presentan para la toma de decisiones. En [12-18] se presenta un mayor desglose al incluir una quinta capa denominada capa de negocio, la cual recibe la información de la capa de aplicación y la entrega a interfaces de nivel superior donde se integran diversas aplicaciones y servicios que permiten la construcción de modelos de negocio, y cuyos resultados sirven de apoyo para la toma de decisiones para la gestión estratégica del negocio.

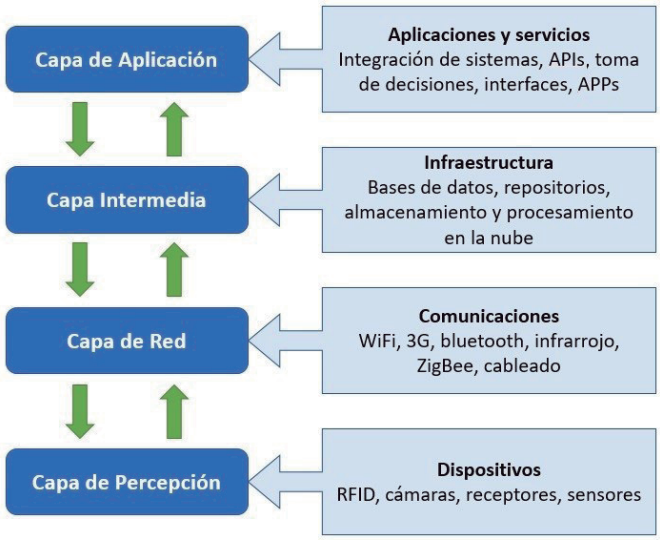

Figura 2. Arquitectura por capas de Internet de las Cosas.

La arquitectura presentada en [19] propone cuatro capas con una superposición semántica que interconecta las capas y facilita la provisión de acceso seguro a los servicios de IoT. Un factor clave para la implementación de seguridad en IoT es la arquitectura en sí misma, tal como lo planteó inicialmente [20]. En el caso de [12-16] se expone una arquitectura IoT simple conformada por una capa de percepción, capa de red y capa de aplicación, definiendo internamente tres conceptos: Dominio de unidad, dominio de ubicuidad y dominio lógico, los cuales clasifican los objetos IoT de acuerdo a su función, interacción con los demás, y presencia dentro del sistema. Finalmente, [21] propone una arquitectura basada en un esquema de protección de privacidad integrado para seguridad de extremo a extremo y la arquitectura original de OpenIoT. El esquema de protección de extremo a extremo sigue los siguientes requisitos: (i)Conexión segura entre la puerta de enlace y el servidor IoT; (ii)Persistencia segura de datos en el almacén de datos de IoT; (iii) Acceso para preservar la privacidad de los datos de IoT para el análisis de los mismos sin revelarlos a otros servidores o al usuario [22]. En estudios como el planteado en [23] se diseñó un framework de seguridad y privacidad de IoT basado en el Modelo de Referencia de Arquitectura (ARM) del proyecto IoT-A, fundamentado en los siguientes pilares: (i)Análisis e identificación de requisitos de seguridad y privacidad sobre el ciclo de vida de los objetos inteligentes; (ii) Diseño de un framework arquitectónico para inferir las necesidades de seguridad y privacidad de los objetos inteligentes durante su ciclo de vida; (iii)Creación de un modelo de control de acceso distribuido mediante la consideración de aspectos dinámicos de autorización para su implementación en ambientes IoT; (iv)Diseño de mecanismos de preservación de la privacidad y su integración en el modelo de control de acceso.

4. Vulnerabilidades y amenazas en IoT

La identificación de vulnerabilidades en una infraestructura IoT es un aspecto clave en la gestión de riesgos. El estudio realizado en [24] presenta una taxonomía sobre vulnerabilidades, vectores de ataque, impacto sobre objetivos de seguridad (integridad, confidencialidad y disponibilidad), ataques y metodologías de remediación. La taxonomía enmarca las vulnerabilidades de IoT dentro del alcance de: (i) Arquitectura por capas; (ii)Impacto en seguridad, basado en los objetivos definidos; (iii) Ataques; (iv) Métodos de remediación; (v)Capacidad de conciencia de la situación, (identificación de vulnerabilidades, detección de intrusos y descubrimiento de red). Entre las conclusiones del estudio, se resaltan factores de diseño limitados que impiden implementar los requerimientos de seguridad aplicables a IoT y las malas prácticas como apertura de puertos innecesarios, programación débil de software y mal manejo de las actualizaciones. Lo anterior, crea puntos de entrada para los atacantes al permitir la reprogramación maliciosa de los dispositivos, provocando mal funcionamiento y abuso.

El trabajo presentado en [25], hace una recopilación de vulnerabilidades y amenazas teniendo en cuenta tres servicios principales dentro de la seguridad en IoT: Autenticación, confidencialidad y control de acceso. En cuanto a la autenticación, se encontró que la mayoría de protocolos KMS (Key Management Service) no son adecuados ya que tanto el cliente y servidor se exponen a un ataque de intermediario al intercambiar llaves sobre Internet. Es difícil garantizar la privacidad debido a que muchos de los dispositivos IoT no pueden implementar técnicas de cifrado tradicionales por sus limitadas especificaciones de cómputo [26]. Respecto al control de acceso, un problema es el hecho de que los dispositivos IoT son entidades que gozan de permisos, roles y privilegios al igual que un usuario, por lo que pueden ser usados para ejecutar una intrusión en el sistema. En [27] además de los objetivos de seguridad, se enfoca en la privacidad y confianza, y define una clasificación de amenazas y ataques a nivel físico, red, software y cifrado. En cuanto a la privacidad, se identifican falencias provenientes principalmente de los requerimientos para la implementación de tecnologías IoT y las políticas de privacidad.

Recientemente, en [7] se presenta una revisión de ataques a Redes de Sensores Inalámbricos WSN

(Wireless Sensor Network). El trabajo presenta una taxonomía que primero divide los ataques entre pasivos y activos, considerando a los ataques pasivos como amenazas que no pueden ser detectadas de ninguna forma afectando principalmente la confidencialidad de los datos, mientras que los ataques activos aparte de afectar la confidencialidad, también atentan contra la integridad y disponibilidad de los datos y los servicios. Luego los autores proponen una clasificación de los ataques activos en 5 categorías de acuerdo a las capas del modelo OSI (Open Systems Interconnection), agrupando los ataques de las capas de sesión y presentación dentro de la capa de aplicación.

Diversos autores han abordado la identificación de vulnerabilidades y amenazas desde el punto de vista de la arquitectura IoT. En la capa de percepción (física), se registran ataques de tipo electrónico y cinético [28]. En otros casos, las limitaciones en el poder de procesamiento y el consumo de energía, han permitido llevar a cabo ataques DDoS (Distributed Denial of Service) [12-16]. Los problemas de cifrado en la memoria y la comunicación de dispositivos también pueden ocasionar ataques como espionaje, suplantación, o interferencia de [7]. En [29] se demuestra que muchos dispositivos IoT poseen vulnerabilidades de corrupción de memoria, lo cual permite al atacante tomar control de los dispositivos. Otras vulnerabilidades como puertos inseguros y lectura de credenciales por defecto son revisadas por [30]. En dispositivos RFID (Radio Frequency Identification) se han documentado ataques como retransmisión por etiquetas falsas, ataque de relé, repetición, clonación de etiquetas y seguimiento a personas [31-32].

Muchos de los dispositivos IoT de hogar ya han sido parte de incidentes importantes de seguridad, siendo participes en el caso de ataques de DDoS. Se describe un método para la identificación de vulnerabilidades de alto riesgo en dispositivos IoT domésticos inteligentes y presenta ejemplos reales de su aplicación en dispositivos comerciales disponibles. El método hace uso de varias herramientas de código abierto para la identificación de vulnerabilidades. En la misma línea de dispositivos IoT para uso doméstico y de adquisición al público, las vulnerabilidades se enfocan específicamente en la capa de percepción, atribuyendo mayores riesgos de seguridad a los fabricantes quienes en su afán por atender el ritmo de las necesidades del mercado, establecen tiempos de comercialización y ciclo de soporte muy cortos, llevando los dispositivos IoT a la obsolescencia. Otros trabajos como los presentados en [33–35], abordan el ámbito de soluciones IoT de hogar y usuarios finales.

En la capa de red, [36] presenta vulnerabilidades en el uso de los estándares IEEE 802.15.4 y 6LoWPAN (Low-Power Wireless Personal Area Networks) que son comunes en dispositivos IoT. Se han documentado ataques como DDoS, monitoreo, inundación, sybil, repetición, intermediario, interferencia, sumidero (DNS Sinkhole), ataques de agujero, y ataque selectivo [12-16-28]. En dispositivos que implementan LPWAN (Low Power Wide Area Network) se han encontrado ataques como repetición, volteo de bits, espionaje, reconocimiento y DoS.

En las capas Middleware/Aplicación, [16] registra ataques por acceso no autorizados, phishing, olfateo e inyección de código arbitrario. Trabajos como [1] se refieren a problemas de privacidad en la integración de datos cuando son compartidos o reutilizados por diferentes servicios y objetos en un ecosistema IoT. En el ámbito de Internet Industrial de las Cosas (IIoT), concepto introducido por primera vez en [37] y luego desarrollado por el Consorcio de Internet Industrial [38], destacan estudios como en [39] con la proposición de una herramienta de detección de vulnerabilidades en aplicaciones industriales como SCADA (Supervisory Control And Data Acquisition), donde se registraron debilidades tales como sobrecarga de búfer, paquetes incompletos, errores de formato, direcciones iniciales y finales incorrectas, código débil de software. Dentro del mismo ámbito de SCADA y PLC (Programmable Logic Controller), [28-40] atribuyen ataques como la desagregación de comandos e inyección de código malicioso al uso inseguro de protocolos UDP (User Datagram Protocol), TCP (Transmission Control Protocol), SIP (Session Initiation Protocol), DNS (Domain Name Service) y FTP (File Transfer Protocol); también ha registrado ataques como tap activo y pasivo, DDoS, falsificación, reproducción y análisis de tráfico debido al uso de repositorios y almacenamientos distribuidos vulnerables.

En el trabajo publicado por [41], se habla sobre la presencia de botnets que hacen uso de dispositivos IoT, lo cual devela dos problemas con las infraestructuras IoT: (i)El acceso a una gran cantidad de dispositivos IoT a través de Internet; (ii)La seguridad es por lo general una medida de último momento en la arquitectura de muchos dispositivos IoT. Se presenta una descripción de la anatomía de las botnets de IoT y su modo básico de operación; también discute las vulnerabilidades que se suelen presentar en los dispositivos y redes IoT y los principales incidentes de Denegación de Servicio

(DDoS) que aprovechan estos puntos débiles. Entre las principales debilidades que presentan los dispositivos IoT se encuentra la baja capacidad de memoria RAM (Read Access Memory), limitaciones en la capacidad de memoria Flash, uso de arquitectura MIPS (Microprocessor Without Interlocked Pipeline Stages) o ARM (Advanced RISC Machine), uso de binarios ELF (Executable and Linkable Format) y salida sin restricción a Internet.

Finalmente, en [14-15-42-43], los problemas de seguridad en ambientes IoT se atribuyen al factor humano, con prácticas como el uso de contraseñas débiles, manejo inadecuado de puertos, la ausencia de políticas de gestión de activos y la falta de gestión de seguridad física. A continuación, se lista las vulnerabilidades especificando la capa en la arquitectura IoT (Tabla 1)

Tabla 1. Vulnerabilidades de seguridad por capas de arquitectura IoTl.

Capa	Contramedida
Percepción	Manipulación de nodos, interferencia, bloqueo de nodos, inyección de código malicioso, destrucción del nodo, ingeniería social, privación del sueño, jamming.
Red	Análisis de tráfico, spoofing, clonación, sumidero, agujero negro, agujero gris, agujero de gusano, intermediario (MiTM), denegación de servicio (DDoS), ataque Sybil, colisión, desincronización, inundación capa de enlace, bloqueo de capa de enlace, spoofing ARP, unfairmess, inundación HELLO, clonación de nodo, dirección errónea, particionamiento de red, bucle de enrutamiento, rushing, alteración de rutas, exploit RPL, exploit 6LoWPAN, exploit MQTT, secuestro de sesión, inundación SYN
Middleware/ Aplicación	Infección de virus y gusanos, spyware, adware, troyanos, denegación de servicio (DDoS), exploit CoAP, inyección de datos falsos, reprogramación
Todas las capas	Ataque de canal lateral, ataque con sólo texto cifrado, ataque de texto sin formato conocido, ataque de texto sin formato escogido, intermediario (MiTM).

5. Contramedidas y soluciones de seguridad

Algunas soluciones de seguridad tienen un enfoque preventivo, como en [44], donde se propone un sistema de evaluación dinámico de riesgos basado en el Sistema Inmune Artificial para la detección de ataques, analizando la capa de red y aplicación.

Más tarde, [45] propone un sistema de control de acceso basado en capacidades para administrar el acceso a servicios e información; el mecanismo admite la delegación de derechos y personalización de control de acceso. El sistema le entrega a los usuarios o procesos un token que le da la capacidad de interactuar con los objetos de cierta forma, por lo que es el usuario quien debe demostrar que tiene propiedad o autoridad sobre las entidades a las cuales desea acceder.

En la investigación realizada en [46], se presenta un sistema llamado IOT SENTINEL, con la capacidad para identificar automáticamente los tipos de dispositivos que se conectan a una red IoT y aplicar reglas para restringir las comunicaciones a aquellos que sean identificados como vulnerables para minimizar el impacto o daño de un ataque que pudiese filtrarse por dichos dispositivos.

En el trabajo presentado por [47], el autor aborda la seguridad a nivel de capa de red y define una extensión IPsec (Internet Protocol Security) de 6LoWPAN mostrando la viabilidad de dicho enfoque. Se evidenció que es posible reutilizar los transceptores IEEE 802.15.4 existentes para manejar 6LoWPAN / IPsec. Los resultados del estudio mostraron que IPsec es una opción viable para implementar en redes de dispositivos IoT en términos de tamaño de los paquetes, consumo de energía, uso de memoria y tiempo de procesamiento. También se evidenció que IPsec puede escalar mejor que la seguridad implementada a nivel de capa de enlace a medida que aumenta el tamaño de los datos y la cantidad de saltos, lo que termina en un ahorro de tiempo y energía. Por otra parte, [7] propone una serie de contramedidas detalladas para contrarrestar amenazas a redes WSN conectadas a Internet, que bien pueden aplicarse a otros contextos en los que dispositivos IoT utilicen protocolos y tecnologías similares.

En el trabajo realizado por [27], los autores presentan una serie de medidas de seguridad para hacer frente a diferentes tipos de ataques que han clasificado de acuerdo a la arquitectura básica de IoT conformada por las capas de percepción, red y aplicación. Los ataques y contramedidas documentados en este trabajo no abordan un escenario específico, sino que describen los problemas y soluciones que se pueden dar

hablando en términos generales para un sistema IoT. Por el mismo camino, [24] presenta una taxonomía de contramedidas que es coherente con la clasificación de vulnerabilidades y ataques definida, distinguiendo tres clases de estrategias a saber: (i)Controles de acceso y autenticación (algoritmos y esquemas de autenticación, modelos biométricos, modelos de permisos conscientes del contexto); (ii)Garantía de software; (iii)Protocolos de seguridad. Adicional incluye un apartado denominado Capacidades de Conciencia Situacional que clasifican las técnicas disponibles para capturar información sobre las actividades maliciosas generadas en el contexto de IoT, siendo estas medidas de carácter preventivo frente a los problemas de seguridad IoT.

En el caso de [41], se encuentra un aporte significativo sobre contramedidas a incidentes que implican dispositivos IoT esclavizados para conformar grandes botnets que históricamente han tenido gran impacto a nivel mundial por sus ataques DDoS y que siguen siendo una amenaza latente. Las contramedidas propuestas en este estudio abarcan soluciones que van desde ajustes en los dispositivos IoT, pasando por configuraciones y controles a nivel de red, hasta llegar a gestiones de servicios y protocolos por parte del ISP (Internet Service Provider).

En el trabajo de [20] se presentó el diseño de un marco de seguridad consciente de los medios para facilitar la operación de aplicaciones multimedia sobre una infraestructura IoT. El marco propuesto incluye en primera instancia un método de análisis y clasificación de tráfico multimedia para manejar la heterogeneidad de diversas aplicaciones en este ámbito; luego, basado en la clasificación anterior se define una arquitectura de seguridad de tráfico enfocada en el objetivo de disponibilidad y accesibilidad de servicios denominada Arquitectura de Seguridad de Tráfico Consciente de los Medios. Dicha arquitectura se compone de cuatro aspectos esenciales: Gestión de claves, reescritura por lotes, autenticación y marca de agua.

Un sector importante de la literatura se ha enfocado en proponer y desarrollar mecanismos y técnicas de cifrado ligeras que puedan ser implementados en los dispositivos IoT con bajas prestaciones computacionales. En [48] es definido un mecanismo de autenticación basado en proximidad de dispositivos IoT. El estudio de [49] describe algunas técnicas de control de acceso, encriptación, gestión de identidad, control de acceso y mecanismos de negociación. Los autores en [26] propone el uso de cifrados simétricos y funciones hash en dispositivos IoT, soportables en arquitecturas con microcontroladores de RAM inferior a 1 KB. El trabajo de [50] por su parte define un esquema de autenticación bidireccional para IoT basado en DTLS (Datagram Transport Layer Security) utilizando RSA (Rivest, Shamir y Adleman) en redes que usan 6LoWPAN. En [51] es definido un enfoque integral de la privacidad en la trasmisión de datos de dispositivos IoT a la nube. Por último, en [52] se propone un enfoque para lograr la confidencialidad e integridad en los mensajes a través de un mapeo de código de autenticación de mensajes de valor clave a hash (HMAC- Hash-based Message Authentication Code), el cual utiliza firmas para enviar mensajes en lugar de cifrado.

A continuación, (Tabla 2) presenta una serie de contramedidas generales frente a amenazas de IoT que pueden servir de apoyo para la identificación de controles de seguridad existentes o nuevos.

Tabla 2. Contramedidas de seguridad por capas de arquitectura IoT.

Capa	Contramedida
Percepción	Inicio seguro para todos los dispositivos, autenticación de dispositivos usando funciones de baja complejidad, confidencialidad y anonimato de datos, configurar los dispositivos para limitar la comunicación únicamente a direcciones privadas y la dirección del fabricante, emparejamiento de dispositivos basado en proximidad, remover dispositivos con fallas de seguridad no mitigables, mecanismo de borrado de memoria, deshabilitar interfaz JTAG de los sensores. protección con contraseña para el cargador de arranque de las placas de sensores, mecanismo de seguridad de capa cruzada – swarm intelligence, limitar la tasa de solicitud disminuyendo la tasa de control MAC, multiplexación por división de tiempo – TDM, implementación de protocolo 6TiSCH.
Red	Comunicación segura entre dispositivos, seguridad en el enrutamiento, datos de usuario seguros en los dispositivos, medidas de seguridad con IPS y CDN, deshabilitar puertos y servicios que no estén en uso, deshabilitar la función Universal Plug and Play en routers a menos que ello sea absolutamente necesario, aislar dispositivos IoT en una propia red privada protegida usando firewall u otras técnicas de segmentación, monitorear los registros del firewall para detectar tráfico sospechoso, especialmente en los puertos 2323/TCP y 23/TCP, aislamiento de dispositivos vulnerables, filtrado de tráfico dirigido a dispositivos IoT en los puertos o protocolos en los que

	haya la vulnerabilidad, configurar zonas desmilitarizadas (DMZ) de bajo, uso de S-QMTT, uso de comunicación inalámbrica de amplio espectro (ataque de interferencia)
Middleware/ Aplicación	Seguridad de datos, Software de protección, Listas de control de acceso (ACLs), uso de mecanismos de autenticación de doble factor, Uso de criptografía PUF (funciones físicamente no clonables).
Todas las capas	Gestión de tecnología, sistema de gestión de intrusos especializados en ambientes IoT, seguridad física en las instalaciones de los ambientes IoT, gestión de confianza, seguridad del personal.

6. Resultados y discusión

Las vulnerabilidades se pueden dar a nivel de hardware o de software, a nivel de políticas o procedimientos o por causa de los mismos usuarios [53]. Las vulnerabilidades asociadas al hardware son difíciles de encontrar y mucho más difíciles de corregir, debido a la compatibilidad e interoperabilidad y también, al mismo esfuerzo que conlleva la corrección [54]. Un gran número de las amenazas encontradas en IoT son ataques y acciones ya conocidas que tienen lugar en Internet, pero con una ocurrencia particular en infraestructuras IoT por las características de los dispositivos y las aplicaciones [55].

Las soluciones de seguridad de información tradicionales representan una gran dificultad de implementación en muchos escenarios IoT principalmente debido a los siguientes factores: (i)Bajas prestaciones de cómputo de los equipos de la capa de percepción. Muchos dispositivos IoT son producidos con capacidades de procesamiento y memoria muy limitadas, lo que impide la implementación de soluciones robustas de seguridad como el cifrado de datos en memoria o en la transmisión de información hacia la red [56]; (ii)Ciclos de vida cortos. Los fabricantes producen dispositivos IoT con periodos de producción y soporte técnico cortos, lo que dificulta el acceso a actualizaciones importantes de firmware y/o sistema operativo que pudiesen mitigar vulnerabilidades; (iii) Fallas en el diseño de dispositivos. Los proveedores de soluciones IoT en su carrera por suplir las necesidades del mercado cada vez más crecientes, liberan rápidamente equipos y aplicaciones quizá con muchas funcionalidades versátiles, pero dejando como último aspecto en sus diseños y arquitecturas la seguridad; (iv)Uso de protocolos de comunicación específicos. Se han desarrollado protocolos de red y comunicación específicos que algunos dispositivos IoT usan para condiciones determinadas de operación y que, por su carácter novedoso, presentan vulnerabilidades explotables con pocas opciones de contramedidas.

7. Conclusiones

Son innegables los beneficios que trae consigo la implementación de soluciones tecnológicas basadas en IoT; sin embargo, las organizaciones y usuarios finales deben tener en cuenta seriamente los riesgos de seguridad en la información a los que se puede estar expuesto, enfocando su atención en la definición de políticas de activos que permitan mantener vigentes las tecnologías de dispositivos IoT y aplicaciones.

El diseño limitado de los dispositivos IoT impide abordar los requisitos de seguridad, permitiendo que una gran cantidad de dispositivos de IoT vulnerables residan en el espacio de Internet. Por tanto, un reto que persiste es el diseño y programación de dispositivos capaces de implementar soluciones de seguridad robustas. Un aspecto para futuros trabajos está en la definición de arquitectura o marcos que permitan lidiar con dispositivos IoT inseguros, de tal forma que se mantenga al mínimo el riesgo asociado.

8. Referencias

[1] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," Secur. Commun. Networks, vol. 7, no. 12, pp. 2728–2742, 2014.

[2] L. A. Zabala Jaramillo, "Gestión de la seguridad en el internet de las cosas," Universidad Piloto de Colombia, 2016.

[3] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," Futur. Gener. Comput. Syst., vol. 78, pp. 964–975, Jan. 2018.

[4] M. Alcaraz, "Internet de las cosas," Univ. Católica Nuestra Señora la Asunción, pp. 2–3, 2014.

[5] J. L. Hernández Ramos, "Development of a security and privacy framework for the internet of things = Desarrollo de un framework de seguridad y privacidad aplicado al internet de las cosas," TDR (Tesis Dr. en Red), Oct. 2016.

[6] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," Int. J. Comput. Appl., vol. 90, no. 11, 2014.

[7] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," IEEE Commun. Surv. Tutorials, vol. 22, no. 1, pp. 616–644, 2019.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Futur. Gener. Comput. Syst., vol. 29, no. 7, pp.

1645–1660, 2013.
[9] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digit. Commun. Networks, vol. 4, no. 2, pp. 118–137, 2018.
[10] G. Davis, "2020: Life with 50 billion connected devices," in 2018 IEEE International Conference on Consumer Electronics (ICCE), 2018, p. 1.
[11] G. L. Y. Germán, "El internet de las cosas y sus riesgos para la privacidad," Universidad Piloto de Colombia, 2017.
[12] K. Chen et al., "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," J. Hardw. Syst. Secur., vol. 2, no. 2, pp. 97–110, 2018.
[13] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer (Long. Beach. Calif)., vol. 46, no. 4, pp. 46–53, 2013.
[14] A. Tejero, "Metodolog{\'\i}a de análisis de riesgos para la mejora de la seguridad del Internet de las Cosas. Caso Smartwatch," 2017.
[15] J. A. Molina Garc\'\ia, "La importancia de la gestión de riesgos y seguridad en el internet de las cosas (IOT)," 2019.
[16] A. Khairi, M. Farooq, M. Waseem, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.
[17] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in 2012 international conference on computer science and electronics engineering, 2012, vol. 3, pp. 648–651.
[18] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in 2012 10th international conference on frontiers of information technology, 2012, pp. 257–260.
[19] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled internet of things," Wirel. Pers. Commun., vol. 61, no. 3, pp. 567–586, 2011.
[20] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," IEEE Netw., vol. 25, no. 3, pp. 35–40, 2011.
[21] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," Futur. Gener. Comput. Syst., vol. 76, pp. 540–549, Nov. 2017.
[22] N. Madaan, M. A. Ahad, and S. M. Sastry, "Data integration in IoT ecosystem: Information linkage as a privacy threat," Comput. Law Secur. Rev., vol. 34, no. 1, pp. 125–133, Feb. 2018.
[23] J. L. H. Ramos, "Desarrollo de un framework de seguridad y privacidad aplicado a internet de las cosas," Universidad de Murcia, 2016.
[24] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2702–2733, 2019.
[25] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Networks, vol. 76, pp. 146–164, Jan. 2015.
[26] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," Comput. Networks, vol. 102, pp. 83–95, Jun. 2016.
[27] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 180–187.
[28] F. Hoffman, "INDUSTRIAL INTERNET OF THINGS VULNERABILITIES AND THREATS: WHAT STAKEHOLDERS NEED TO CONSIDER.," Issues Inf. Syst., vol. 20, no. 1, 2019.
[29] K. V. English, I. Obaidat, and M. Sridhar, "Exploiting Memory Corruption Vulnerabilities in Connman for IoT Devices," in 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019, pp. 247–255.
[30] R. Antrobus, B. Green, S. Frey, and A. Rashid, "The forgotten i in iiot: a vulnerability scanner for industrial internet of things," 2019.
[31] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 709–712.
[32] G. P. Hancke, K. Markantonakis, and K. E. Mayes, "Security challenges for user-oriented RFID applications within the" Internet of things"," J. Internet Technol., vol. 11, no. 3, pp. 307–313, 2010.
[33] D. Wang, X. Zhang, T. Chen, and J. Li, "Discovering Vulnerabilities in COTS IoT Devices through Blackbox Fuzzing Web Management Interface," Secur. Commun. Networks, vol. 2019, 2019.
[34] L. Costa, J. P. Barros, and M. Tavares, "Vulner-

abilities in IoT Devices for Smart Home Environment," in Proceedings of the 5th International Conference on Information Systems Security e Privacy, ICISSP 2019., 2019, vol. 1, pp. 615–622.
[35] N. Apthorpe, D. Reisman, and N. Feamster, "A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic," arXiv Prepr. arXiv1705.06805, 2017.
[36] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," IEEE Commun. Surv. Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.
[37] P. C. Evans and M. Annunziata, "Industrial internet: Pushing the boundaries," Gen. Electr. Reports, pp. 488–508, 2012.
[38] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," Comput. Ind., vol. 101, pp. 1–12, 2018.
[39] J. Men et al., "Finding sands in the eyes: vulnerabilities discovery in IoT with EUFuzzer on human machine interface," IEEE Access, vol. 7, pp. 103751–103759, 2019.
[40] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," IEEE Internet Things J., vol. 6, no. 4, pp. 6822–6834, 2019.
[41] K. Angrishi, "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets," arXiv Prepr. arXiv1702.03681, 2017.
[42] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer (Long. Beach. Calif)., vol. 44, no. 9, pp. 51–58, 2011.
[43] I. Salas Sanz, "Seguridad en la Internet de las cosas," 2019.
[44] C. Liu, Y. Zhang, J. Zeng, L. Peng, and R. Chen, "Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology," in 2012 8th International Conference on Natural Computation, 2012, pp. 874–878.
[45] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the internet of things," Math. Comput. Model., vol. 58, no. 5–6, pp. 1189–1205, 2013.
[46] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "Iot sentinel: Automated device-type identification for security enforcement in iot," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 2177–2184.
[47] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," Secur. Commun. Networks, vol. 7, no. 12, pp. 2654–2668, 2014.
[48] C. T. Zenger, M. Pietersz, J. Zimmer, J.-F. Posielek, T. Lenze, and C. Paar, "Authenticated key establishment for low-resource devices exploiting correlated random channels," Comput. Networks, vol. 109, pp. 105–123, 2016.
[49] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad hoc networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[50] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, pp. 2710–2723, 2013.
[51] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things," Futur. Gener. Comput. Syst., vol. 56, pp. 701–718, 2016.
[52] D. Dinculean\ua and X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," Appl. Sci., vol. 9, no. 5, p. 848, 2019.
[53] J. M. Kizza, Guide to computer network security. Springer, 2013.
[54] M. Abomhara and others, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," J. Cyber Secur. Mobil., vol. 4, no. 1, pp. 65–88, 2015.
[55] Q. Jing, A. V Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wirel. Networks, vol. 20, no. 8, pp. 2481–2501, 2014.
[56] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (iot)," in 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011, pp. 1–5.