Hamut'ay
Revista cuatrimestral de divulgación científica
UNIVERSIDAD ALAS PERUANAS
http://revistas.uap.edu.pe/ojs/index.php/HAMUT
ISSN: 2313-7878
Vol. 7 (3). Setiembre-Diciembre. Hamut'ay 2020. Lima-Perú

Seguridad IoT: Principales amenazas en una taxonomía de activos

Security IoT: Top Threats in an Asset Taxonomy

Cartuche-Calva, Joffre J.[1]
https://orcid.org/0000-0002-1633-2291

Hernández-Rojas, Dixys L.[2]
https://orcid.org/0000-0002-2116-6531

Morocho-Román, Rodrigo F.[3]
https://orcid.org/0000-0003-0194-5033
Universidad Técnica de Machala, Ecuador

Radicelli-García, Ciro D.[4]
http://orcid.org/0000-0001-9188-0514
Universidad Nacional de Chimborazo, Ecuador

Recibido:05-09-2020
Aceptado: 20-12-2020

Cita Recomendada
Cartuche-Calva, J. J., Hernández-Rojas, D. L., Morocho-Román, R. F. & Radicelli-García, C. D., (2020). Seguridad IoT: Principales amenazas en una taxonomía de activos. Hamut´ay, 7 (1), 51-59
http://dx.doi.org/10.21503/hamu.v7i3.2192

Resumen

El Internet de las Cosas (IoT) es una extensión de internet al integrar redes móviles, internet, redes sociales y cosas inteligentes para proporcionar mejores servicios o aplicaciones a los usuarios, uno de los mayores retos que tiene IoT son los problemas de seguridad relacionados con las amenazas, ataques, vulnerabilidades, etc. En este artículo, se proporciona una taxonomía de sus activos mediante la agrupación de los diferentes elementos que conforman un ecosistema IoT, para determinar qué elementos podrían estar afectados en la adquisición, el intercambio y el procesamiento de información ante las posibles amenazas existentes. La metodología utilizada consta de cuatro pasos, comenzando con la definición del alcance y juicios de expertos en el área de IoT, la investigación de escritorio, el análisis y desarrollo, redacción y validación del informe, llegando a obtener una clasificación y análisis de las principales amenazas según la categorización de los diferentes tipos de amenazas existentes y el nivel de impacto de riesgo que estas generan identificando qué amenazas pueden mitigarse y el riesgo que puedan tener en cada entorno IoT. Como resultado se aporta con una taxonomía de seguridad que podrá ser usada para evaluar el nivel de impacto de riesgo de toda una arquitectura IoT.

Palabras clave: IoT, seguridad, amenazas, vulnerabilidades, taxonomía.

1. Ingeniero en Sistemas Informáticos y Magíster en Ingeniería del Software. Candidato a doctor en TIC-Redes Móviles en la UDC, España. Líneas de investigación ingeniería de software, gestión de proyecto y seguridad IoT. docente titular e investigador de la UTMACH. jcartuche@utmachala.edu.ec.
2. Ingeniero electrónico y Máster en Electrónica. PhD en TIC-Redes Móviles por la UDC- España. Líneas de investigación en IoT, Realidad aumentada, Blockchain y Seguridad IoT. Profesor titular e investigador de la UTMACH. dhernandez@utmachala.edu.ec
3. Ingeniero de Sistemas, con maestrías en Seguridad Informática Aplicada y en Docencia y Gerencia en Educación Superior; profesor universitario en el área de Redes de Computadoras e instructor certificado para el programa Netacad de Cisco. rmorocho@utmachala.edu.ec
4. Ingeniero en Sistemas Informáticos, con maestría en Tecnologías, Sistemas y Redes de Comunicaciones. PhD en Telecomunicación Líneas de investigación Televisión Digital Terrestre, telecomunicaciones, TIC y educación. cradicelli@unanch.edu.ec

Abstract

The Internet of Things (IoT) is an extension of the internet by integrating mobile networks, internet, social networks and smart things to provide better services or applications to users, one of the biggest challenges that IoT has are security problems related to threats, attacks, vulnerabilities, etc. In this article, a taxonomy of your assets is provided by grouping the different elements that make up an IoT ecosystem, to determine which elements could be affected in the acquisition, exchange and processing of information in the face of possible existing threats. The methodology used consists of four steps, beginning with the definition of the scope and judgments of experts in the area of IoT, desktop research, analysis and development, writing and validation of the report, reaching a classification and analysis of the main threats according to the categorization of the different types of existing threats and the level of risk impact that these generate, identifying which threats can be mitigated and the risk they may have in each IoT environment. As a result, it is provided with a security taxonomy that can be used to evaluate the level of risk impact of an entire IoT architecture.

Key words: IoT, security, threats, vulnerabilities, taxonomy

Introducción

Uno de los primeros conceptos del Internet de las cosas se atribuye a Kevin Ashton, en el año 2009, el cual hace referencia a la conexión de todo tipo de dispositivos a Internet, para el intercambio de información entre estos dispositivos, pudiendo incluso, en determinados casos, actuar de modo automático ante la detección de ciertos eventos (Carmona & Antonio, 2019). La agencia de la Unión Europea para la ciberseguridad (ENISA, 2017), define a IoT como "un ecosistema ciberfísico de sensores y actuadores interconectados, que permiten la toma de decisiones inteligentes". Sin embargo, se coincide con Russell & Duren (2018) al plantear que las tecnologías para IoT aún están en desarrollo, muchas de ellas aun no son estándares y se deben superar muchas dificultades. Uno de los obstáculos más importantes en IoT es la seguridad que afectan la garantía de los datos entre las aplicaciones y los dispositivos IoT. La seguridad en sistemas basados en IoT implica no sólo proteger datos, claves criptográficas y credenciales. Es por esto, que estos sistemas son propensos a una amplia variedad de amenazas y desafíos en cuanto a la seguridad (Perez et al., 2018).

La seguridad debe abordarse durante todo el ciclo de vida de IoT desde el diseño inicial hasta los servicios en ejecución (Shancang Li, Da Li, 2017). Las tres principales áreas de desafíos de la seguridad en IoT son la confidencialidad, "preservar la divulgación no autorizada de la información, en las operaciones internas y los componentes del dispositivo IoT", (Uribe, Felix, 2019), el objetivo es garantizar la seguridad de la transmisión de los datos en las comunicaciones, la integridad en la protección de los datos durante la transmisión, para lo cual deben existir medidas en vigor que hagan posible la verificación de que un mensaje transmitido por un equipo es legítimo de la red (Arteche Zabalo, 2018) y la disponibilidad, la que hace referencia a la "característica de la información de encontrarse siempre a disposición del solicitante que debe acceder a ella, sea persona, proceso o sistema (Augusto, 2017), el objetivo es garantizar el acceso y uso de los datos en cualquier condición adversa.

En la actualidad todos los dominios de aplicación IoT muestran una creciente preocupación de las amenazas de seguridad, ataques y vulnerabilidades. Para Romero, (2017) una amenaza es como cualquier elemento o acción capaz de atentar y aprovechar una vulnerabilidad para comprometer la seguridad de un sistema de información o ecosistemas IoT. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente que se comprometa o no la seguridad (Carrión & Rodrigo, 2017).

Método

Con este estudio lo que se pretende aportar a la comunidad científica es un análisis bibliográfico acerca de las principales amenazas para IoT, vista desde una clasificación de la arquitectura y elementos de IoT, denominada taxonomía de activos, para lo cual se ha utilizado los métodos históricos lógicos para la clasificación y la identificación de las principales amenazas, para el impacto de riesgo se aplicaron los métodos inductivos. La metodología de investigación que se aplicó se muestra en la Figura 1.

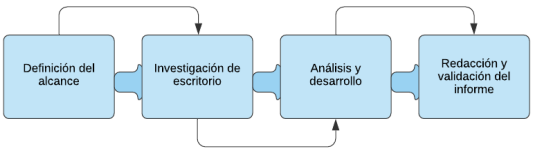

Figura 1. Metodología de estudio.
Fuente: Elaboración propia (2020)

Se inicia la metodología de estudio con la definición del alcance y juicios de expertos en el área de IoT a fin de recopilar sus aportes y conocimientos, luego, la investigación documental para identificar publicaciones e información existente sobre los principales activos y amenazas para el desarrollo de las medidas de seguridad. En el análisis y desarrollo se crearon las taxonomías de activos y amenazas identificando los escenarios de ataque y por último la redacción y validación del informe para sintetizar todos los hallazgos de la investigación.

Taxonomía de activos IoT.

Un ecosistema IoT puede entenderse como el conjunto de infraestructura hardware y software que se encuentra instalado, junto con sus actores sociales en un contexto en particular (Balcazar Hoyos & Lemos Elvira, 2019). Las tecnologías y aplicaciones específicas, en este entorno necesitan de estándares, arquitecturas, modelos de seguridad, etc. Existen varias arquitecturas de IoT definidas, por instituciones, comunidad científica (artículos, libros, congreso, etc.), algunas de ellas convertidas en estándares y las cuales están basadas en SOA (Avila et al., 2017), orientada a API (Tan et al., 2016), estandarizada oneM2M (Muhammad, 2019), referencia de Internet Industrial (Yli-Ojanperä , 2019) y referencia WSO2 (Breivold, 2017).

Para la clasificación propuesta en activos, se tomó la arquitectura basada en dominios mostrada en la figura 2, la cual tiene tres dominios o capas principales: dominio de sensores, dominio de red y dominio de aplicaciones. Dentro del ecosistema IoT y pasando por los diferentes dominios antes descritos, tenemos un conjunto de elementos físicos y lógicos, que junto a diferentes servicios y aplicaciones hacen funcionar al IoT actual. Todos ellos pueden ser clasificados a través de una taxonomía de activos, la cual estará agrupada por diferentes componentes.

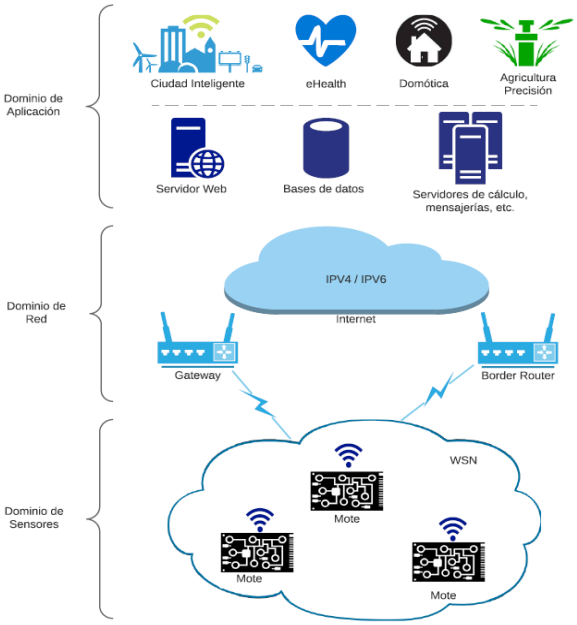

Figura 2: Arquitectura Basados en Dominios.
Fuente: Basada en (Campoverde et al., 2015)

La figura 3 muestra una clasificación general propuesta por los principales componentes lógicos (infraestructura, plataforma & back-end, decisiones de datos, servicios y aplicaciones, información) y físicos (Dispositivos IoT, otros dispositivos IoT, comunicaciones).

Figura 3: Modelo de referencia de componentes lógicos y físicos. Fuente: Elaboración propia (2020)

En la tabla 1 y 2 se proporciona una descripción general de los grupos de activos clave, y se debe mencionar que esta taxonomía es indicativo y no exhaustivo, es decir, los elementos se mencionan de manera general y no por marca o tipo, el mismo criterio se aplica a las redes y a los protocolos y para una mejor descripción se han separado en la taxonomía propuesta los elementos lógicos de los físicos.

Tabla 1: Taxonomía de activos de componentes lógicos

Tipo Activos	Activos	Descripción
Infraestructura	Router	Componentes de red que se encarga de seleccionar la ruta en el envío de paquetes de datos entre las diferentes redes del ecosistema IoT, actúan como la barrera entre internet y la red local (Segura Gavilán, 2019).
	Gateways	Nodos de red que permiten interactuar con otro segmento de red utiliza diferentes protocolos, funciona como puerta de salida de los diferentes paquetes. Es un enlace entre la WSN o WSAN y la comunicación por internet (Cloud Computing), el Gateway IOT puede acceder directamente a un recurso de la Cloud Computing o comunicarse directamente con una WSN (Villacres & David, 2016).
	Fuente alimentación	Medios de conexión para el suministro de energía eléctrica a un dispositivo IoT. Puede ser cableada o una batería integrada.
	Activos de seguridad	Comprende equipos informáticos enfocados específicamente a la seguridad de los dispositivos, redes e información de IoT. Entre estos están firewalls, firewalls de aplicaciones web WAF (Cano Alvaro, 2018), CASB (Bertolín, 2016) para proteger la nube, IDS (Coyla Jarita, 2019), IPS (Macias Victor Julio, 2020) y sistemas de autenticación / autorización (Mondragón & Guillén, 2019).
Plataforma & backend	Servicios basados en la web	Servicios dentro de la World Wide Web, proporcionan una interfaz basada en web para usuarios web o para aplicaciones conectadas a la web. Esto significa que las tecnologías web se pueden utilizar en IoT para comunicaciones de persona a máquina H2M(Ruan et al., 2019) y para comunicaciones de maquina a máquina M2M (Otero, 2018).
	Infraestructura de la cloud y servicios	En IoT, el backend de la nube se puede utilizar los servicios(Duarte & Ramírez, 2019) para agregar y procesar datos de dispositivos dispersos, y también proporciona capacidades informáticas, almacenamiento, aplicaciones y servicios.
	Procesamiento de datos	Son algoritmos y servicios para procesar los datos recopilados y transformarlos en una estructura definida para su uso posterior, utilizando tecnologías de big data (Hernández-Leal et al., 2017) para descubrir patrones en conjuntos de datos muy grandes.
Decisiones de datos	Procesamiento y computación de datos	Servicios para facilitar el procesamiento, recopilados de los datos para obtener información útil, que se puede utilizar para aplicar reglas, lógica, toma de decisiones y automatizar procesos.
Servicios & aplicaciones	Analisis y visualización de datos	La información resultante se puede analizar y visualizar para identificar nuevos patrones y mejorar la eficiencia operativa.
	Gestión de dispositivos y redes	Actualizaciones de software del sistema operativo, el firmware y las aplicaciones, abarca el seguimiento y monitoreo de los dispositivos y redes, recolectando y almacenando registros que luego pueden usarse para diagnósticos.
	Uso de dispositivos	Comprender el estado actual, patrones de uso y rendimiento.
Información	Reposo	Información almacenada en una base de datos en el backend de la nube o en los propios dispositivos.
	Transito	Información enviada o intercambiada a través de la red entre dos o más elementos de IoT.
	Uso	Información utilizada por una aplicación, servicio o elemento de IoT.

Fuente: Elaboración propia (2020)

Tabla 2: Taxonomía de activos de componentes físicos

Tipo Activo	Activos	Descripción
Dispositivos IoT	Hardware	Componentes físicos a partir de los cuales se pueden construir los dispositivos de IoT, incluyen microcontroladores, microprocesadores, los puertos físicos del dispositivo y la placa base (Ziegler, 2019).
	Software	Comprende el sistema operativo del dispositivo IoT, firmware, programas y aplicaciones instalados y en ejecución, el software se desarrolla a través de un proceso (Ramos et al., 2017).
	Sensores	Dispositivos cuya finalidad es detectar y/o medir eventos en su entorno y enviar la información a otra electrónica para su procesamiento, existen dos tipos de sensores inductivos y capacitivos (Reyes-Flores, 2019).
	Actuadores	Dispositivos de salida de los dispositivos IoT, que ejecutan decisiones basadas en información procesada previamente (Hernández-Rojas et al., 2018b).
Otros Dispositivos IoT	Interfaces de conexión con los dispositivos IoT	Dispositivos cuyo propósito sirven como interfaz o como agregado entre otros dispositivos de un ecosistema IoT. Además, los dispositivos utilizados por los usuarios para interactuar e interactuar con dispositivos IoT. Varios ejemplos aparecen en (Berrú-Ayala et al., 2020).
	Dispositivos para administrar objetos	Dispositivos diseñados para administrar otros dispositivos IoT y redes.
	Sistemas embebidos	Dispositivos conformados por un sistema electrónico, de tamaño muy reducido, construidos con materiales muy resistentes que soportan factores de calor, frio, humedad, etc. (Barrera Obando Anlly, 2018), la unidad de procesamiento permite procesar datos por sí mismos. Contienen sensores, actuadores, y puede conectarse a la red directamente en la nube y tienen capacidad de ejecutar software.
	Redes	Sistema de comunicación que conecta computadores y otros equipos informáticos entre sí, con la finalidad

		de compartir información (Zambrano et al., 2017), existen diferentes topologías de redes como LAN, PAN, WAN, entre otras.
Comunicaciones	Protocolos	Conjunto de reglas para realizar la comunicación entre dos o más dispositivos de IoT a través de un canal determinado. Existen dos tipos de protocolos de comunicación inalámbricos o alámbricos. Ejemplos de protocolos de comunicación de IoT son ZigBee, MQTT, CoAP, BLE. En (Hernández-Rojas et al., 2018a) se puede profundizar más sobre protocolos IoT.

Fuente: Elaboración propia (2020)

Seguridad IoT.

Se entiende por amenaza a la presencia de factores que pueden aprovechar las vulnerabilidades que se presentan, ya sea un sistema de información, personas o procesos (Chalá Ibarra Edwar, 2020). Para la implementación en los sistemas IoT se deben considerar los siguientes factores de seguridad: las amenazas (Palacios, 2019), vulnerabilidades (Cárdenas & Ropero , 2020), ataques y compromisos (Monzón, 2019) que puedan ocurrir en su normal funcionamiento, luego de tener clasificado la taxonomía de inventario de activos IoT procedemos a identificar las principales amenazas y su nivel de impacto en los activos de IoT descritos en el epígrafe anterior.

Las principales amenazas en una taxonomía de activos, pueden ser clasificadas según su categoría, tipo, nivel de impacto y posibles activos IoT afectados. Entre las categorías de incidencias hemos analizado las siguientes: ataques o abusos, intersección o secuestro, caídas, daños, fallos o averías, desastres y ataques físicos. Entre las amenazas de seguridad fueron seleccionadas los malware, secuencia de exploit, ataques dirigidos, DDoS, falsificación de identidad (dispositivos y usuarios), ataques de privacidad, modificación de la información, man in the midle, secuestros de protocolos, pérdidas de servicio entre otros. En la tabla 3, se muestra más amenazas, con su respectiva descripción y clasificadas por categorías y tipos.

Categoría	Amenaza	Descripción	Nivel de impacto	Tipos de activos afectados
Ataques / Abusos	Malware	"Malicious software", es cualquier tipo de programa o código malicioso, malintencionado cuyo objetivo es infiltrarse en un dispositivo sin el consentimiento del usuario (González Díez, 2020). Son los más utilizados por los hackers para el robo de información.	Alto	– Dispositivos IoT. – Otros dispositivos IoT. – Plataforma & backend.
	Kits de explotación	Son servicios basados en la web diseñados para aprovechar las vulnerabilidades en los navegadores web mediante la descarga de archivos. (Taylor et al., 2016). La función principal es encontrar errores o puntos vulnerables y acceder a un sistema IoT, para provocar un comportamiento no intencionado.	Alto	– Dispositivos IoT. – Otros dispositivos IoT. – Infraestructura.
	Ataques dirigidos	Diseñados para ejecutarse en un periodo de tiempo prolongado y llevados a cabo en numerosas fases con el objetivo de permanecer ocultos y obtener la mayor cantidad de información / datos confidenciales. El ataque dirigido requiere un modelo de destino para generar una etiqueta de destino específica (Li et al., 2020).	Media	– Infraestructura. – Plataforma & backend. – Información.
	Denegación de servicio distribuido DDoS	Varios sistemas atacan un objetivo común para saturarlo y dejar inoperativo el servicio o recurso provocando el fallo de la conectividad. Estos ataques se realizan a través de botnets, que habitualmente están compuestas por	Alto	– Dispositivos IoT. – Otros dispositivos IoT. – Infraestructura. – Plataforma & backend.

		están compuestas por ordenadores que han sido infectados y son controlados a distancia por los atacantes (Bautista Rosell, 2020).		
	Falsificación de dispositivos maliciosos	Cuando un dispositivo falso se hace pasar por un original en un sistema IoT, estos dispositivos tienen backdoors o puertas traseras que pueden utilizarse para atacar otros sistemas de TIC.	Media	– Dispositivos IoT. – Otros dispositivos IoT. – Infraestructura.
	Ataques a la privacidad	Estas amenazas afectan a la privacidad del usuario, elementos	Media	– Dispositivos IoT. – Otros dispositivos IoT.
		de la red, personas no autorizado.		– Plataforma & backend. – Información.
Ataques / Abusos	Modificación de la información	Consiste en la manipulación de la información para generar caos y obtener beneficios.	Madia	– Dispositivos IoT. – Otros dispositivos IoT. – Plataforma & backend. – Información.
Eavesdropping Intercepción / secuestro	Man in the Middle	El atacante intercepta en secreto la conexión entre dos partes comunicantes y, por tanto, en secreto retransmite o incluso puede alterar los datos que se transfieren entre las dos partes (Patni, 2017).	Alta	– Información. – Comunicaciones – Dispositivos IoT. – Decisiones de datos.
	Secuestro del protocolo de comunicación IoT	Se apropia de una sesión de comunicación existentes entre dos usuarios o elementos de la red y tiene acceso a la información, contraseñas, y forzar desconexión o negación del servicio.	Media	– Información. – Comunicaciones – Dispositivos IoT. – Decisiones de datos
	Intercepción de la información	Recepción no autorizada de procesos de comunicación privada(llamadas telefónicas, mensajería, mails)	Media	– Información. – Comunicaciones – Dispositivos IoT.
	Reconocimiento de red	Escaneo de información en la infraestructura de la red con sus dispositivos conectados, protocolos utilizados, puertos abiertos y servicios.	Media	– Información. – Comunicaciones – Dispositivos IoT. – Infraestructura.
	ecuestro de sesión	El atacante asume la identidad del cliente legítimo y obtiene una conexión de red no autorizada como si fuera un cliente legítimo(Letsoalo & Ojo, 2018). Con el objetivo de obtener modificar o eliminar datos transmitidos.	Media	– Información. – Comunicaciones – Dispositivos IoT.
	Obtención de información	Obtención pasiva de la información sobre la red : dispositivos conectados y protocolos empleados.	Media	– Información. – Comunicaciones. – Dispositivos IoT.
	Reproducción de mensajes	Utiliza una transmisión de datos valida de manera mal intencionada enviando repetidamente o retrasándolos los mensajes, con el propósito de dejar inoperativo el equipo.	Medio	– Información. – Comunicaciones. – Dispositivos IoT.
Caídas	Caída de red	Interrupción o fallo en el funcionamiento de la infraestructura de la red, puede ser ocasionada de manera intencionada o no intencional.	Alta	– Información. – Comunicaciones.
	Fallos de dispositivos	Fallos o avería en los dispositivos de hardware	Medio	– Dispositivos IoT.
	Fallos de sistemas	Fallos de los servicios o aplicaciones software	Medio	– Dispositivos IoT. – Otros dispositivos IoT. – Plataforma & backend.

	Perdida de servicio de soporte	Perdida del soporte necesarios para el funcionamiento adecuado de la información	Alta	– Todos los activos.
Daño / perdida (Activos TI)	Filtrado de datos / información confidencial	Cuando los datos confidenciales son revelados de manera intencional a terceros sin autorización del usuario, la amenaza varía según el tipo de dato que se filtre.	Medio	– Dispositivos IoT. – Plataforma & backend. – Información.
Fallos / averías	Vulnerabilidad de software	Se debe a la utilización de contraseñas débiles, por defecto, errores de software, malas configuraciones lo que es un riego para la red.	Alta	– Dispositivos IoT. – Otros dispositivos IoT. – Plataforma & backend. – Infraestructura. – Servicios y Aplicaciones.
	Fallos de tercero	Configuraciones no adecuadas en uno de los elementos activos de la red.	Medio	– Dispositivos IoT. – Otros dispositivos IoT. – Plataforma & backend. – Infraestructura. – Servicios y Aplicaciones.
Desastre	Desastre natural	Problemas que están fuera de la voluntad humana como inundaciones, vientos, etc. Pero pueden ocasionar un daño físico en los dispositivos.	Alta	– Dispositivos IoT. – Otros dispositivos IoT. – Plataforma & backend. – Infraestructura.
	Desastre ambiental	Desastres en el despliegue de los entornos de equipos de IoT, ocasionando su inoperatividad.	Media	– Otros dispositivos IoT. – Plataforma & backend. – Infraestructura.
Ataques físicos	Modificación de dispositivo	Manipulación de dispositivos mediante la errónea comunicación que puedan tener los puertos abiertos	Media	– Comunicaciones – Dispositivos IoT.
	Destrucción del dispositivo / sabotaje	Perdida de dispositivos sea por robos, ataques y vandalismo.	Media	– Dispositivos IoT. – Otros dispositivos IoT. – Plataforma & backend. – Infraestructura.

Fuente: Elaboración propia (2020)

Conclusiones

La metodología empleada para la revisión bibliográfica de conceptos, términos, taxonomías e investigaciones propuestos por la comunidad científica, permitieron hacer una clasificación de los elementos del ecosistema IoT a través de una taxonomía de activos.

Como resultado del estudio realizado se define además una taxonomía de seguridad IoT según la categorización de los diferentes tipos de amenazas existentes y el nivel de impacto de riesgo que estas generan sobre los diferentes activos de IoT, en la adquisición, el intercambio y el procesamiento de información.

Los métodos inductivos aplicados permitieron identificar aquellas amenazas que pueden mitigarse o evaluar el riesgo que estas puedan tener en cada entorno IoT.

Agradecimiento

La elaboración de este trabajo forma parte de un proyecto de investigación institucional, desarrollado dentro del grupo de investigación AutoMathTIC y financiado por la Dirección de Investigación de la UTMACH (Universidad Técnica de Machala) según Resolución 359/2020.

Referencias bibliográficas

Arteche Zabalo, E. (2018). La ciberseguridad como norma. Estudio del estado del arte en estándares y certificación en materia de seguridad cibernética aplicada a industria 4.0 e IoT, Universidad de Paos Vasco. https://addi.ehu.es/bitstream/handle/10810/32240/TFG_Zabalo%20Arteche.pdf?

Ávila, K., Sanmartín, P., Jabba, D., & Jimeno, M. (2017). Applications Based on Service-Oriented Architecture (SOA) in the Field of Home Healthcare. Sensors, 17(8),

1703. https://doi.org/10.3390/s17081703
Balcázar Hoyos, D. F., & Lemos Elvira, J. J. (2019). Modelo para la construcción de ecosistemas sociales de objetos inteligentes IoT.
http://repositorio.unicauca.edu.co:8080/xmlui/handle/123456789/1776
Barrera Obando, A. (2018). Estudio de parámetros y características para el desarrollo de aplicaciones de internet de las cosas (IoT) en sistemas embebidos. Universidad de San Buenaventura. http://biblioteca.usbbog.edu.co:8080/Biblioteca/BDigital/168052.pdf
Bautista Rosell, J. (2020). Ataques DDoS con IoT, Análisis y Prevención de Riesgos. https://e-archivo.uc3m.es/handle/10016/29630
Berrú Ayala, J., Hernandez Rojas, D., Morocho Díaz, P., Novillo Vicuña, J., Mazon Olivo, B., & Pan, A. (2020). SCADA System Based on IoT for Intelligent Control of Banana Crop Irrigation. En M. Botto-Tobar, M. Zambrano Vizuete, P. Torres Carrión, S. Montes León, G., Pizarro Vásquez, & B. Durakovic (Eds.), Applied Technologies (pp. 243-256). Springer International Publishing. https://doi.org/10.1007/978-3-030-42517-3_19
Bertolín, J. A. (2016). Implantación de la tecnología de seguridad CASB para el acceso a ecosistemas cloud en IoE. Eurofach electronica: Actualidad y tecnología de la industria electrónica, 449, 44-48.
Breivold, H. P. (2017). A Survey and Analysis of Reference Architectures for the Internet-of-things. ICSEA 2017, 143.
Campoverde, Ariel., Hernández, Dixys., & Mazón, B. (2015). Cloud computing con herramientas open-source para Internet de las cosas. Maskana, 6, 173-182.
Cano, A. (2018). Implementación y medida del rendimiento de un firewall para aplicaciones web (WAF) en un balanceador de carga.
https://idus.us.es/handle/11441/85834
Cárdenas-Quintero, D., Ropero-Silva, E., Puerto-López, K., Sanchez-Mojica, K., Castro Casadiego, S., & Ramirez Mateus, J. (2020). Vulnerabilidad en la seguridad del internet de las cosas. Mundo FESC, 10(19), 162-179.
Carmona, M., & Antonio, P. (2019). Seguridad en los ecosistemas IoT. http://openaccess.uoc.edu/webapps/o2/handle/10609/96607
Carrión, A., & Rodrigo, M. (2017). Plan de seguridad informática basado en estándares Iso-Iec 27001 para proteger la información y activos del GAD cantonal de Pastaza. http://localhost:8080/xmlui/handle/123456789/6508
Chalá Ibarra, E. (2020). Propuesta de un modelo de seguridad para la prevención de pérdida de información sensible dirigido a la asamblea nacional Universidad Internacional SEK.
https://repositorio.uisek.edu.ec/bitstream/123456789/3997/1/Edwar%20Rodolfo%20Chal%c3%a1%20Ibarra.pdf
Coyla Jarita, Y. (2019). Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión - Filial Juliaca. (Tesis de licenciatura) Universidad Peruana Unión.
http://repositorio.upeu.edu.pe/handle/UPEU/2002
ENISA. (2017). Baseline security recommendations for IoT in the context of critical information infrastructures. Publications Office.
https://data.europa.eu/doi/10.2824/03228
Gómez Duarte, M. A., & Galindo Ramírez, X. (2019). Seguridad en la nube, evolución indispensable en el siglo XXI. https://doi.org/10.14483/2322939X.15535
González Díez, M. (2020). Internet de las cosas. Privacidad y seguridad. http://openaccess.uoc.edu/webapps/o2/handle/10609/116427
Google Books Link. (s. f.). Recuperado de
https://books.google.es/books?id=G2Q4DgAAQBAJ
Hernández Leal, E. J., Duque Méndez, N. D., & Moreno Cadavid, J. (2017). Big Data: Una exploración de investigaciones, tecnologías y casos de aplicación. Tecnológicas, 20(39), 17-24. https://doi.org/10.22430/22565337.685
Hernández-Rojas, D. L., Fernández Caramés, T. M., Fraga Lamas, P., & Escudero, C. J. (2018b). A Plug-and-Play Human-Centered Virtual TEDS Architecture for the Web of Things. Sensors, 18(7), 2052. https://doi.org/10.3390/s18072052
Patni, P., Iyer, K., Sarode, R., Mali, A., & Nimkar, A. (2017). Man-in-the-middle attack in HTTP/2. 2017 International Conference on Intelligent Computing and Control (I2C2), 1-6. https://doi.org/10.1109/I2C2.2017.8321787

Letsoalo, E., & Ojo, S. (2018). A Model to Mitigate Session Hijacking Attacks in Wireless Networks. 2018 IST-Africa Week Conference (IST-Africa).
Li, M., Deng, C., Li, T., Yan, J., Gao, X., & Huang, H. (2020). Towards Transferable Targeted Attack. 641-649. https://doi.org/10.1109/CVPR42600.2020.00072
Macías, V. (2020). Diseño de sistema prototipo para análisis de intrusiones con técnicas de machine learning. Universidad Piloto de Colombia, 55. http://35.227.45.16/bitstream/handle/20.500.12277/8213/Trabajo%20de%20Grado%20Victor_Macias_20200703.pdf
Mondragón, M. V. P., & Guillén, E. P. (2019). Servicios de autenticación y autorización orientados a internet de las cosas. Telemática, 17(2), 42-51.
Monzón, G., Todt, C. M., Bolatti, D., Gramajo, S. D., & Scappini, R. J. R. (2019). Modelo de seguridad IoT. XXV Congreso Argentino de Ciencias de la Computación (CACIC) (Universidad Nacional de Río Cuarto, Córdoba). http://sedici.unlp.edu.ar/handle/10915/91363
Muhammad, A., Afzal, B., Imran, B., Tanwir, A., Akbar, A. H., & Shah, G. (2019). OneM2M Architecture Based Secure MQTT Binding in Mbed OS. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 48-56. https://doi.org/10.1109/EuroSPW.2019.00012
Palacios Román, J. (2019). Seguridad y privacidad en internet de las cosas. http://openaccess.uoc.edu/webapps/o2/handle/10609/107086

Patni, P., Iyer, K., Sarode, R., Mali, A., & Nimkar, A. (2017). Man-in-the-middle attack in HTTP/2. 2017 International Conference on Intelligent Computing and Control (I2C2), 1-6. https://doi.org/10.1109/I2C2.2017.8321787
Perez, N. B., Bustos, M. A., Berón, M., & Rangel Henriques, P. (2018). Análisis sistemático de la seguridad en internet of things. XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste). http://sedici.unlp.edu.ar/handle/10915/68387
Ramos, D., Noriega, R., Laínez, J. R., & Durango, A. (2017). Curso de Ingeniería de Software: 2a Edición. IT Campus Academy.

Reyes-Flores, E. (2019). Tipos de Sensores. Con-Ciencia Serrana Boletín Científico de la Escuela Preparatoria Ixtlahuaco, 1(2), 31-33.
Rodríguez, D. H. (s. f.). Detección de ataques de Denegación de Servicios en la Nube. 11.
Otero, M. (2018). Evaluación del desempeño de protocolos de control de acceso al medio para comunicaciones máquina a máquina (M2M), (Tesis de Licenciatura). Universidad Central Marta Abreu de Las Villas, Facultad de Ingeniería Eléctrica, Departamento de Electrónica y Telecomunicaciones. https://dspace.uclv.edu.cu/bitstream/handle/123456789/10050/Miguel%20Alejandro%20Otero%20Rojas.pdf?sequence=1&isAllowed=y
Romero, T. (2017). La protección de datos ante el internet de las cosas. (Tesis de Licenciatura). Universidad Politécnica de Madrid. http://oa.upm.es/47426/1/TFC_MARIA_TERESA_ROMERO_GARCIA.pdf
Ruan, L., Dias, M. P. I., & Wong, E. (2019). Machine Learning-Based Bandwidth Prediction for Low-Latency H2M Applications. IEEE Internet of Things Journal, 6(2), 3743-3752. https://doi.org/10.1109/JIOT.2018.2890563
Russell, B., & Duren, D. V. (2018). Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem, 2nd Edition. Packt Publishing Ltd.
Segura Gavilán, A. (2019). Seguridad en la internet de las cosas: Propuesta de implantación segura de un sistema de seguridad con dispositivos IoT en una PYME. http://openaccess.uoc.edu/webapps/o2/handle/10609/97447
Seguridad y ciberseguridad: ¿Qué hemos aprendido en esta década? ¿Cuáles con los retos a 2030? (2020). https://sistemas.acis.org.co/index.php/sistemas/issue/view/14/11
Shancang Li, Da Li. (2017). Securing the internet of things. Oreilly.
Tan, W., Fan, Y., Ghoneim, A., Hossain, M. A., & Dustdar, S. (2016). From the Service-Oriented Architecture to the Web API Economy. IEEE Internet Computing, 20(4), 64-68. https://doi.org/10.1109/MIC.2016.74

Taylor, T., Hu, X., Wang, T., Jang, J., Stoecklin, M. P., Monrose, F., & Sailer, R. (2016). Detecting Malicious Exploit Kits using Tree-based Similarity Searches. Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, 255-266. https://doi.org/10.1145/2857705.2857718
Uribe, Félix. (2019). El Internet de las cosas IoT y su uso como vector de ataques cibernéticos e incidentes de privacidad. 10.
Vega, C. (2017). Artículo en formato IEEE: Concienciación en seguridad de la información. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/2667
Villacres, P., & David, J. (2016). Desarrollo e implementación de un gateway para una red de sensores inalámbricos BLE integrado al sistema IOTMACH. http://repositorio.utmachala.edu.ec/handle/48000/7608
Yli-Ojanperä, M., Sierla, S., Papakonstantinou, N., & Vyatkin, V. (2019). Adapting an agile manufacturing concept to the reference architecture model industry 4.0: A survey and case study. Journal of Industrial Information Integration, 15, 147-160. https://doi.org/10.1016/j.jii.2018.12.002
Zambrano, J. A. O., Ortiz, J. M. E., Bernabe, M. del C. T., & Castillo, K. N. L. (2017). Propuesta de un programa de tecnología en redes informáticas y telecomunicaciones. Dominio de las Ciencias, 3(3), 1159-1180.
Ziegler, S. (Ed.). (2019). Internet of Things Security and Data Protection. Springer International Publishing. https://doi.org/10.1007/978-3-030-04984-3