Universitat Oberta de Catalunya

uoc.edu

Aplicación de metodología de seguridad en un entorno IoT doméstico

Autor: Daniel Garrido Escalera
Máster Interuniversitario en Seguridad de las Tecnologías d la Información y la Comunicación (MISTIC)
Seguridad en la Internet de las cosas

Director del TFM: Jorge Miguel Moneo
Profesor/a responsable de la asignatura: Helena Rifà Pous

26/10/2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Aplicación de metodología de seguridad en un entorno IoT doméstico*
Nombre del autor:	*Daniel Garrido Escalera*
Nombre del consultor/a:	*Jorge Miguel Moneo*
Nombre del PRA:	*Helena Rifà Pous*
Fecha de entrega (mm/aaaa):	10/2021
Titulación:	*Máster Interuniversitario en Seguridad de las Tecnologías d la Información y la Comunicación (MISTIC)*
Área del Trabajo Final:	*Seguridad en Internet de las cosas*
Idioma del trabajo:	*Castellano*
Palabras clave	*Iot, security, framework*

Resumen del Trabajo

Podemos definir la Internet de las cosas (IoT) como la interconexión de objetos o máquinas a través de Internet. Este concepto cada vez va teniendo más aplicaciones en diferentes ámbitos; agricultura, urbanismo, domótica, salud, logística, Industria …Las particularidades de estos proyectos nos hacen plantearnos la validez de los diseños de seguridad basados en modelos tradicionales.

Por ello, este trabajo tiene como objetivo descubrir, a partir de esas singularidades, los mejores modelos para diseñar la seguridad en proyectos del entorno IoT.

Se analizarán casos reales de diversos ámbitos, a partir de los cuales podamos extraer amenazas comunes a este tipo de proyectos y así poder definir un modelo de seguridad específico.

Se desarrollará un prototipo de proyecto IoT doméstico sobre el que aplicaremos el modelo planteado.

Abstract:

We can define the Internet of Things (IoT) as the interconnection of objects or machines through the Internet. This concept has more and more applications in different areas; agriculture, urban planning, home automation, health, logistics, Industry… The particularities of these projects make us consider the validity of security designs based on traditional models.

Therefore, this work aims to discover, based on these singularities, the best models for designing security in projects in the IoT environment.

Real cases from various fields will be analyzed, from which we can extract common threats to this type of project and thus be able to define a specific security model.

A prototype of a domestic IoT project will be developed on which we will apply the proposed model

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El término IoT o Internet de las cosas es más antiguo de lo que muchos podemos pensar. Fue propuesto por Kevin Ashton en 1999 a la compañía Procter and Gamble (P&G) para dar nombre a un sistema de identificación de productos por radiofrecuencia.
Durante algunos años no se volvió a hablar del tema, pero diferentes factores, tales como la popularización de Internet y los protocolos sin cable (*Wi-Fi, LoRa, ZigBee, Bluetooth …)* , la computación en la nube, el fenómeno *Big Data*, el abaratamiento de los sensores y los dispositivos móviles, han provocado su eclosión.
La Internet de las cosas hace referencia a la interconexión de máquinas o dispositivos a través de Internet. Actualmente las aplicaciones son muy diversas y las podemos encontrar en diferentes ámbitos; agricultura, urbanismo, domótica, salud, industria, logística …Nos permite, por tanto, desde monitorizar la humedad y temperatura de una zona de cultivo, hasta gestionar las zonas de aparcamiento libres en un barrio, pasando por controlar las constantes vitales de un paciente o controlar la temperatura de un envío refrigerado. Las posibilidades son casi infinitas, pero también lo son las amenazas.
Según el estudio *Internet of Things (IoT) in Europe* de Statista [1] , el número de plataformas públicas de IoT en 2019 era de 620.

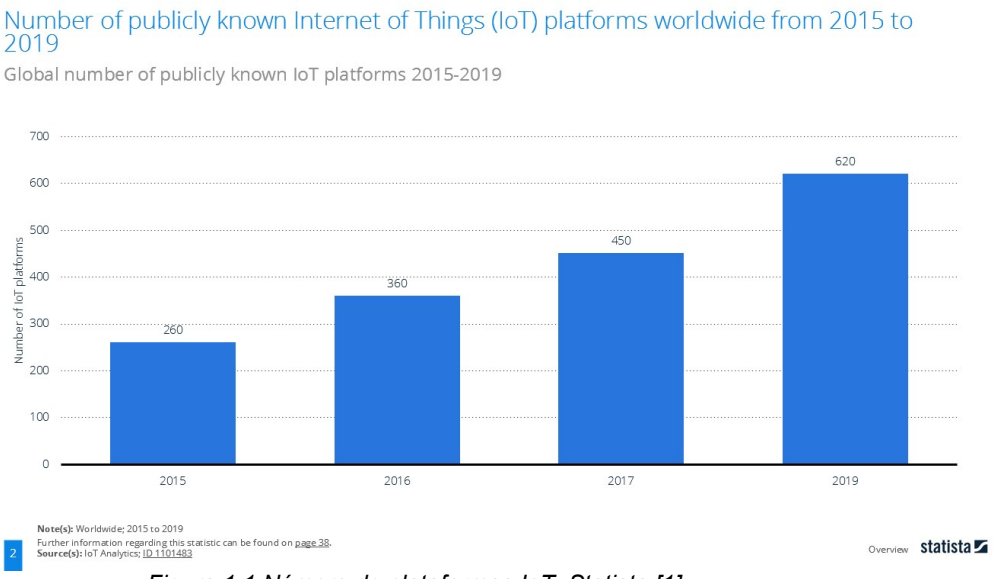


Figura 1.1 Número de plataformas IoT. Statista [1]

Dicho estudio también muestra algunos de los principales retos a los que se enfrentan este tipo de proyectos, como son los relacionados con la seguridad (22%) y la privacidad (19%)

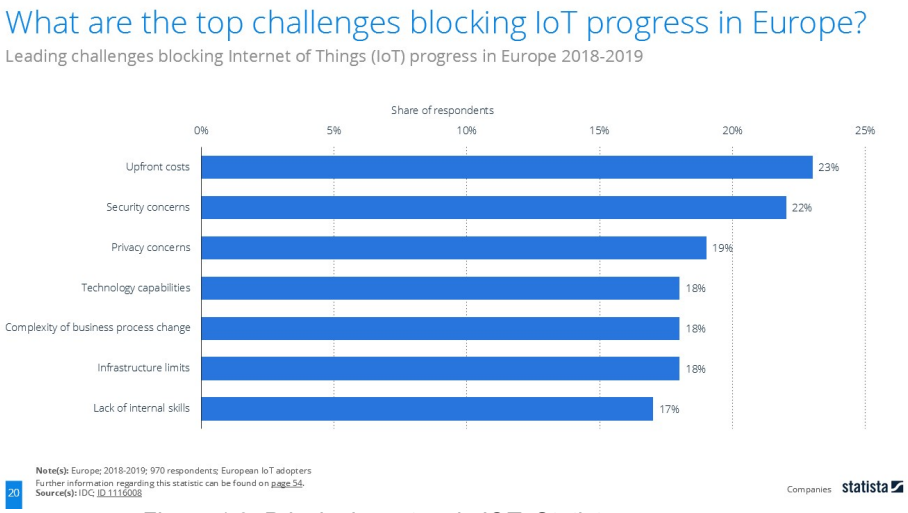


Figura 1.2. Principales retos de IOT. Statista

Teniendo en cuenta este contexto, este trabajo tiene como objetivo descubrir cuáles son las amenazas propias de esta tipología de soluciones y qué adaptaciones o modificaciones deben realizarse en los modelos clásicos de seguridad para garantizar la seguridad de las mismas.
Para ello, se analizarán los componentes de un sistema IoT; dispositivos de adquisición de datos, equipos de cálculo y plataformas existentes. La gran variedad de estos elementos hace imposible un análisis exhaustivo de todos ellos, por lo que se tomarán como referencia los más representativos, en base a su popularidad.
Una vez identificadas las amenazas más habituales, definiremos un modelo de seguridad IOT. Para ponerlo en práctica implementaremos un pequeño proyecto IOT, al que aplicaremos nuestro modelo.

La motivación a la hora de realizar este trabajo tiene dos vertientes; por un lado, la personal, con un interés particular en temas varios como la domótica, herramientas o plataformas abiertas, como *Raspberry Pi, Docker, Node-Red* … y por otro lado, otra vertiente profesional, con la intención de profundizar en la temática IoT y llegar a aplicarla de alguna manera en mis actividades profesionales. Debo indicar que, aunque interesado en ellas, no tengo un conocimiento profundo de dichas herramientas, y por tanto este TFM va a impli
car también el reto de descubrirlas en profundidad para poder llevar a cabo la implementación con éxito.

1.2 Objetivos del Trabajo

El objetivo principal del trabajo es definir una metodología o marco de trabajo que garantice la seguridad en el diseño e implementación de un sistema IoT.

Para ello, nos apoyaremos en la consecución de los siguientes objetivos específicos:

- ✓ Identificar dispositivos / sensores IoT más habituales
- ✓ Seleccionar plataformas IoT de mayor popularidad
- ✓ Identificar y describir amenazas más habituales en proyectos IoT
- ✓ Proponer mejoras metodológicas en modelo de seguridad IoT
- ✓ Desarrollar proyecto piloto de IoT en el que aplicar el modelo definido.

Podemos decir que este trabajo pretende también contribuir, de manera indirecta, al cumplimiento de los objetivos de desarrollo sostenible (ODS) de las Naciones Unidas. Concretamente, las aportaciones de este trabajo se centrarán en los siguientes objetivos:

ODS 3 Salud y Bienestar: En el ámbito de la salud encontramos diferentes soluciones IoT;

- Asistencia a personas mayores (detección de caídas),
- Vigilancia de pacientes (medición de constantes vitales, niveles de glucosa, monitorización marcapasos …)
- Medición radiación ultravioleta

En este ámbito la seguridad, tanto desde el punto de vista de la integridad, como la confidencialidad y la disponibilidad, es muy importante. Por tanto, si el proyecto puede contribuir a que estos sistemas sean más seguros, estará contribuyendo en cierta medida a mejorar la salud y bienestar de las personas.

ODS 9 Industria, innovación e Infraestructuras.
Uno de los objetivos del ODS 9 es "*Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad"* [13]
Ciertos proyectos IoT, como los relacionados con la red eléctrica inteligente, instalaciones fotovoltaicas, o la congestión del tráfico, contribuyen a este objetivo. Nuevamente, igual que en el anterior ODS, si el proyecto contribuye a hacer más seguros este tipo de proyectos IoT, estará contribuyendo al cumplimiento del objetivo.

1.3 Enfoque y método seguido

El enfoque se basará en realizar un estudio del estado actual de las soluciones IoT,desde el punto de vista de la seguridad.
A partir de los incidentes en seguridad més relevantes estableceremos las amenazas y el plan de prevención de las mismas.

Planteamos desarrollar un prototipo de solución IoT de tipo doméstico, que nos permita experimentar y comprobar el modelo de seguridad propuesto. Aunque los proyectos domésticos e industriales tienen diferentes prioridades y objetivos, nos decidimos implementar uno doméstico por ser más asequible y accesible. Incidiremos en las características que comparten ambos mundos, y no en la especifidad de cada uno de ellos.

1.4 Planificación del Trabajo

De cara a poder implementar un prototipo de solución IoT con el que experimentar y verificar nuestras hipótesis, utilizaremos los siguientes recursos:

Hardware

- PC portátil
- Raspberry Pi 4 8GB RAM Microordenador de bajo coste
- Switch 5 puertos
- Sensores varios (presencia/ temperatura / humedad / presión…)
- Disco SSD

Software

- Docker Herramienta para el empaquetado de aplicaciones
- Mosquitto Broker MQTT servidor de mensajes de código abierto
- Node-Red Herramienta de desarrollo para interconectar dispositivos
- InfluxDB: Base de datos de código abierto
- Grafana. Software libre para visualización
- Home Assistant. Software de Código abierto para automatización del hogar

	Nombre de tarea	Duración	Comienzo	Fin
1	**Plan de Trabajo**	**10 días**	**mié 15/09/21**	**mar 28/09/21**
2	Explicación problema a resolver	2 días	mié 15/09/21	jue 16/09/21
3	Investigación y Documentación	2 días	mié 15/09/21	jue 16/09/21
4	Definición Objetivos	3 días	vie 17/09/21	mar 21/09/21
5	Establecimiento metodología	3 días	vie 17/09/21	mar 21/09/21
6	Planificación	2 días	mié 22/09/21	jue 23/09/21
7	Entrega PEC1	0 días	mar 28/09/21	mar 28/09/21
8	**Análisis y Diseño**	**20 días**	**mié 29/09/21**	**mar 26/10/21**
9	Estudio sensores y dispositivos IOT más habituales	5 días	mié 29/09/21	mar 05/10/21
10	Estudio plataformas / software IOT	7 días	mié 29/09/21	jue 07/10/21
11	Estudio tipologías proyectos IOT	4 días	mié 29/09/21	lun 04/10/21
12	Definición arquitectura proyecto piloto	3 días	vie 08/10/21	mar 12/10/21
13	Selección componentes proyecto piloto	2 días	mié 13/10/21	jue 14/10/21
14	Definición modelo seguridad proyectos IOT	8 días	vie 15/10/21	mar 26/10/21
15	Entrega PEC2	0 días	mar 26/10/21	mar 26/10/21
16	**Implementación y conclusiones**	**20 días**	**mié 27/10/21**	**mar 23/11/21**
17	Desarrollo proyecto piloto	10 días	mié 27/10/21	mar 09/11/21
18	Aplicación modelo seguridad al proyecto piloto	10 días	mié 10/11/21	mar 23/11/21
19	Entrega PEC3	0 días	mar 23/11/21	mar 23/11/21
20	**Memoria Final**	**25 días**	**mié 24/11/21**	**mar 28/12/21**
21	Redacción memoria final	25 días	mié 24/11/21	mar 28/12/21
22	Entrega PEC4	0 días	mar 28/12/21	mar 28/12/21
23	**Presentación vídeo**	**5 días**	**mié 29/12/21**	**mar 04/01/22**
24	Elaboración vídeo	5 días	mié 29/12/21	mar 04/01/22
25	Entrega PEC5	0 días	mar 04/01/22	mar 04/01/22
26	**Defensa TFM**	**5 días**	**lun 10/01/22**	**vie 14/01/22**

Figura 1.3. Lista de tareas planificadas

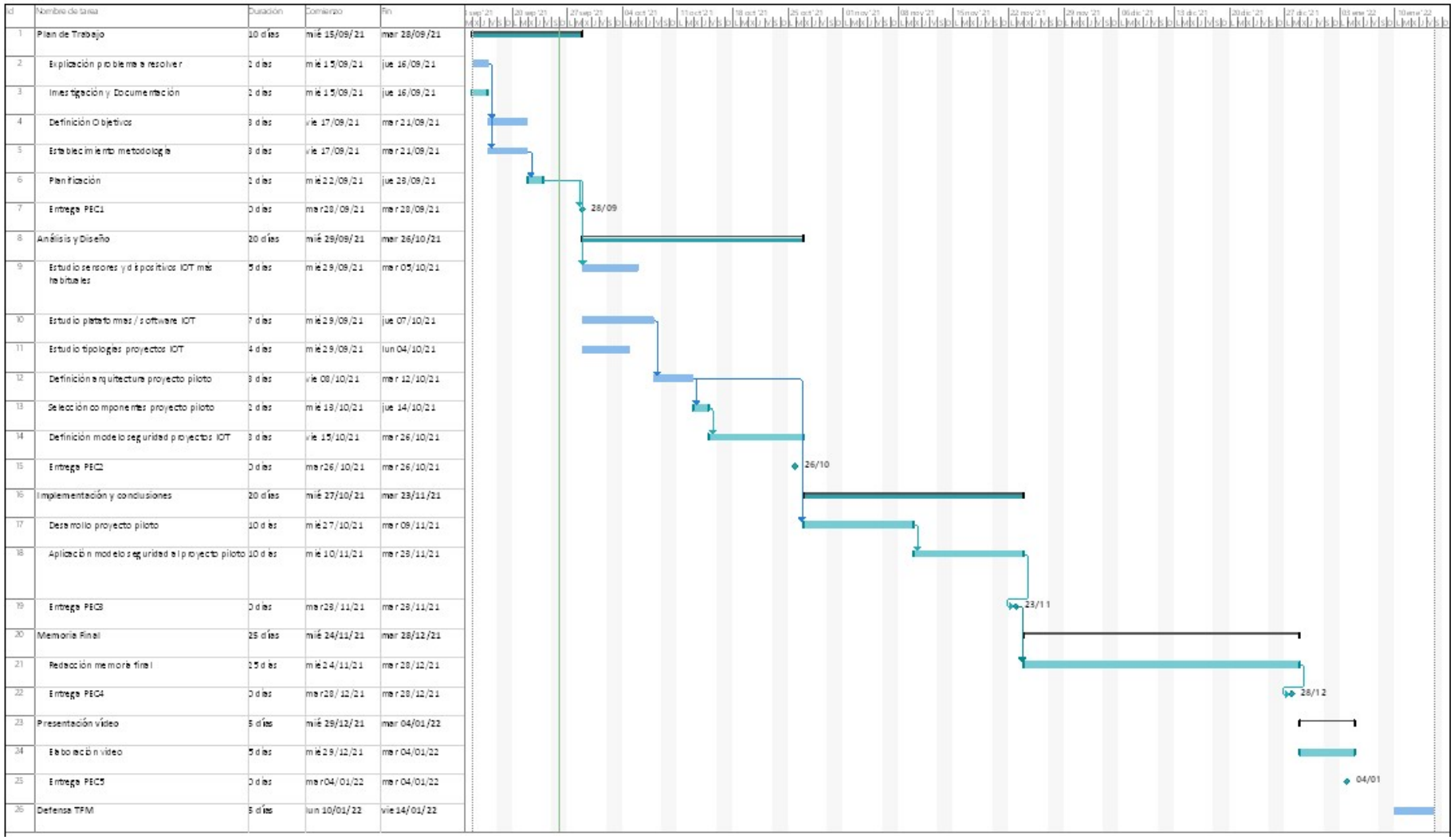


Figura 1.4. Diagrama Gantt con planificación del TFM

1.5 Estado del arte

Se ha realizado un estudio preliminar para evaluar el estado del arte, que se revisará en profundidad durante la fase de análisis.
Podemos concluir que se han realizado diferentes aproximaciones a la cuestión de la seguridad en proyectos de IoT.
Citamos algunos específicos, como los trabajos de Khoo,[15], centrado en los dispositivos RFID, o Granjal et al. [16], que propone el uso de IPv6, así como Weber and Boban, [17], centrados en la privacidad y confidencialidad, o Gupta and Shukla [18] y Chaudhary et al [19].
En los últimos años han aparecido diferentes documentos o publicaciones que intentan solucionar diferentes aspectos de la seguridad en IoT. Así, podemos citar los siguientes:

Ámbito doméstico:
Diferentes países y organizaciones han elaborado guías con el objetivo de prevenir incidentes en el área del consumidor final

Technical Specification for Cyber Security for Consumer Internet of Things publicado por el Instituto Europeo de Normas de Telecomunicaciones (European Telecommunications Standards Institue, ETSI) [21], que proporciona una serie de recomendaciones o buenas prácticas, dirigidas a proyectos IoT domésticos.

UK's Code of Practice for Consumer IoT Security, publicado por el Departamento de Digital, Cultura, Media y Deportes de Reino Unido [22]

Securing the Internet of Things for Consumers Code of Practice, publicado por el gobierno de Australia en 2020 [23]

Por otro lado, la Unión Europea, a través de ENISA, *European Union Agency for Network and Information Security* también ha elaborado diferentes documentos,dirigidos al ámbito de las infraestructuras y la industria. Así, podemos mencionar *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* [24]
Esta misma organización, ENISA, ofrece una herramienta interesante de obtención de recomendaciones y normativas [25] relacionadas con la seguridad de proyectos IoT de los siguientes ámbitos; Smart Cars, Smart Hospitals, Smart Airports, Smart Cities, Industry 4.0.

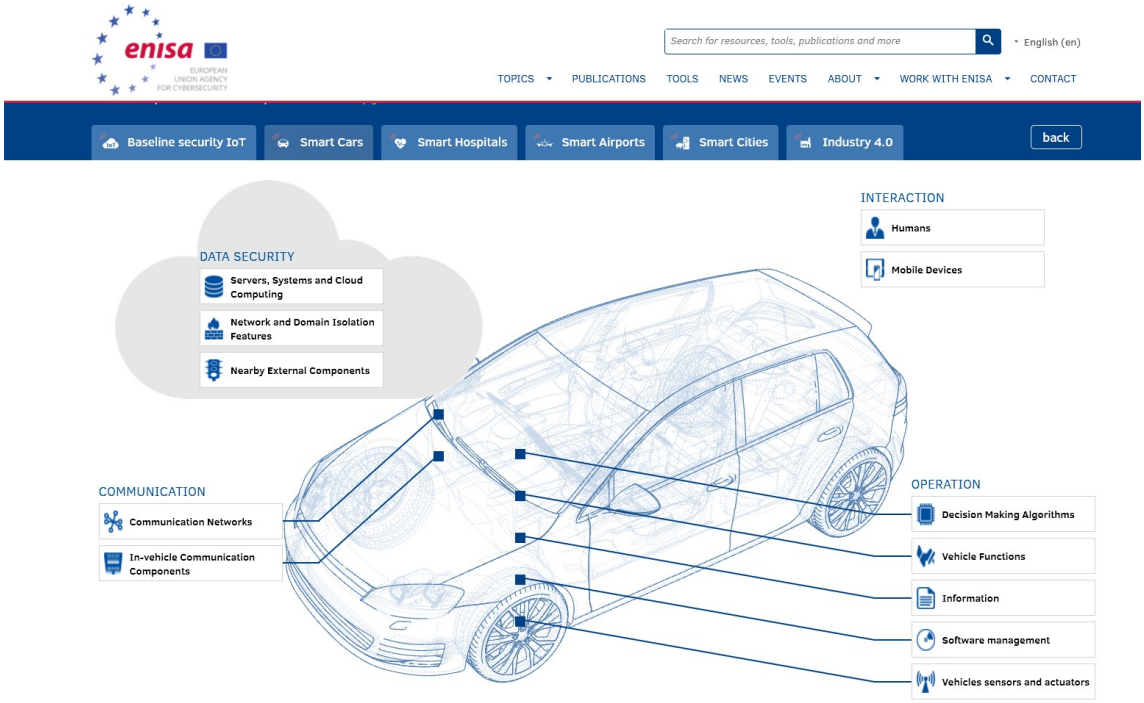


Figura 1.5. Herramienta de búsqueda de información de buenas prácticas seguridad IoT de ENISA [25]

Otra herramienta muy interesante es la publicada por el DCMS, Ministerio de Cultura, Medios de Comunicación y Deportes de Reino Unido. [26]
De manera gráfica, representa una serie de entidades, públicas y privadas, que han publicado información relativa a la seguridad IoT. Entre las organizaciones incluidas encontramos NIST,IEEE,OWASP,ENISA,Cisco,Microsoft…
Haciendo click en el círculo correspondientes a cada entidad, accedemos a la documentación publicada por la misma.

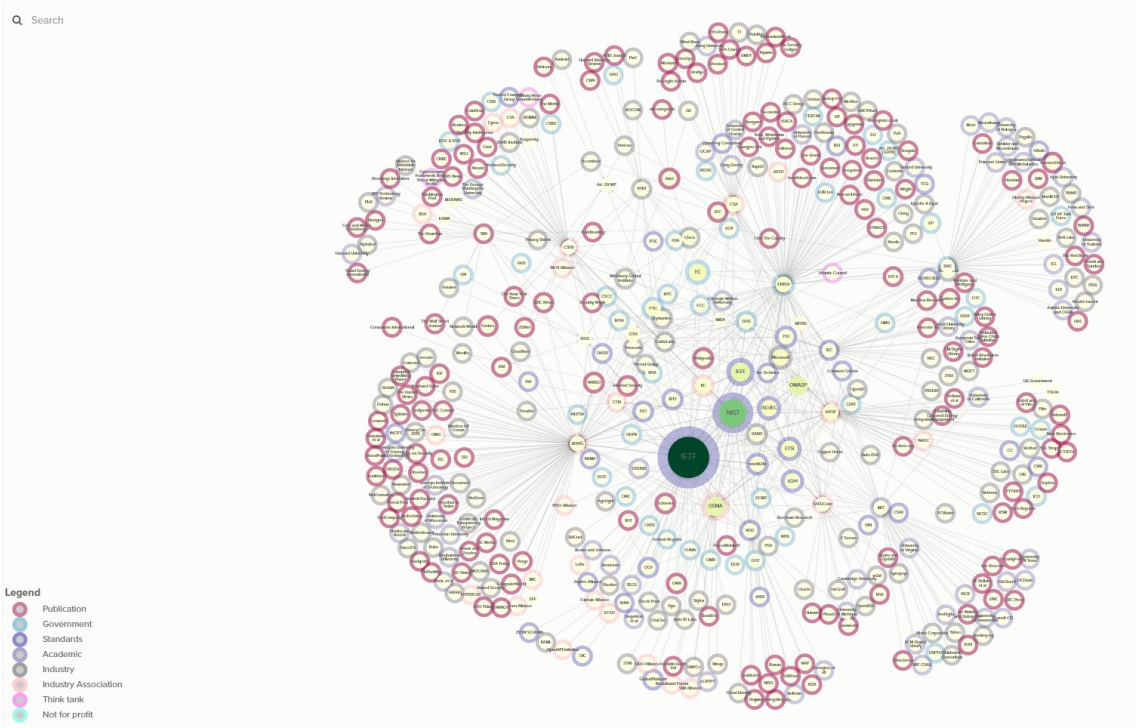


Figura 1.6. Herramienta de búsqueda de información de buenas prácticas seguridad IoT de DCMS[26]

El Instituto Nacional de Estándares y Tecnología de estados Unidos (NIST National Institute of Standards and Technology tiene en marcha el programa Ciberseguridad para IoT (NIST Cybersecurity for IoT Program) [27] que soporta el desarrollo y aplicación de estándares, guías, y otras herramientas que permitan mejorar la seguridad en en entornos IoT.

También han surgido iniciativas que no están asociadas a empresas ni gobiernos, como *I Am The Cavalry* [28], constituida por voluntarios de la comunidad de investigadores de seguridad.Se centran en cuatro ámbitos; dispositivos médicos, hogar, automóvil e Infraestructuras públicas. Muchos de los objetivos y capacidades descritas en su juramento hipocrático (Hippocratic Oath) [30] para dispositivos médicos conectados han sido adoptados por la FDA en sus criterios regulatorios para aprobar dispositivos médicos.

OWASP, Open Web Application Security Project, fundación sin ánimo de lucro, conocida entre otras cosas, por publicar cada año la lista de 10 amenazas de seguridad más críticas en aplicaciones web, también publicó en 2014 la lista de 10 amenazas más graves en IoT. La última versión es la correspondiente al año 2018. [31]

1.6 Breve sumario de productos obtenidos

Los productos obtenidos serán las entregas parciales del proyecto TFM:

PEC1 Plan de trabajo. Se define la justificación, los objetivos, metodología, planificación de tareas y recursos necesarios para el desarrollo del trabajo.

PEC2 Análisis y Diseño de la solución
Esta entrega incluye los resultados del análisis teórico; amenazas más habituales y modelo propuesto para su mitigación.

PEC3 Implementación y conclusiones
La tercera entrega incluirá la descripción de la implementación del prototipo o proyecto piloto, así como la aplicación del modelo diseñado.

PEC4 Memoria final: documento de entre 50 y 70 páginas que recoge todas las fases del trabajo.

PEC5 Presentación en vídeo: Audiovisual de 15 minutos como máximo

2. Arquitectura típica de un proyecto IoT

Los componentes típicos de un proyecto IoT son:

2.1. Sensores y actuadores

Existen multitud de sensores y dispositivos IoT; sensores de humedad, temperatura, luz, enchufes inteligentes, bombillas ..

Señalamos algunos de ellos, a modo de ejemplo, que podemos encontrar en aplicaciones de IoT doméstico, por su facilidad a la hora de utilizarlos en placas Arduino y/o Raspberry. No pretende ser un listado exhaustivo, ni mucho menos, sinó una muestra de la diversidad de elementos existentes.

- Sensor de Temperatura y Humedad DHT22

Contiene un sensor capacitivo de humedad y un termistor para medir la temperatura del aire circundante. Muestra los datos mediante una señal digital en el pin de datos. No dispone de salida analógica.

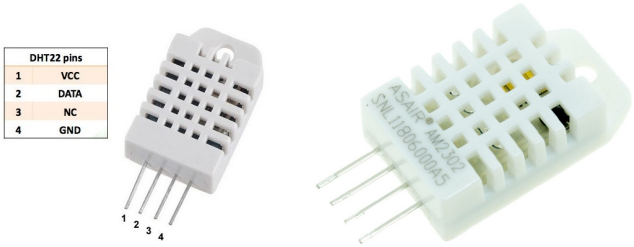


Figura 2.1. Imágenes del sensor DHT22 [42]

ESPECIFICACIONES TÉCNICAS

- Voltaje de Operación: 3V - 6V DC
- Rango de medición de temperatura: -40°C a 80 °C
- Precisión de medición de temperatura: <±0.5 °C
- Resolución Temperatura: 0.1°C
- Rango de medición de humedad: De 0 a 100% RH
- Precisión de medición de humedad: 2% RH
- Resolución Humedad: 0.1%RH
- Tiempo de sensado: 2s
- Interface digital: Single-bus (bidireccional)
- Modelo: AM2302
- Dimensiones: 20*15*8 mm
- Peso: 3 gr.
- Carcasa de plástico blanco

Figura 2.2. Especificaciones técnicas del sensor DHT22[42]

- Alarma de Calidad del Aire MQ135

El MQ-135 es un sensor de calidad del aire que permite detectar algunos gases peligrosos como Amoniaco, Dióxido de Nitrógeno, Alcohol, Benceno, Dióxido y Monóxido de carbono

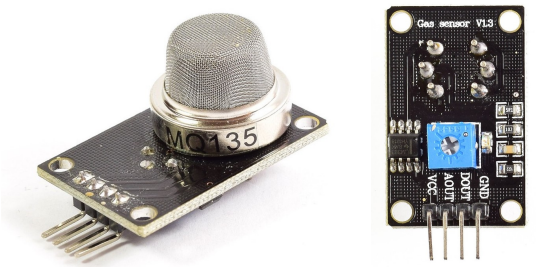


Figura 2.3. Imágenes del sensor MQ135[43]

ESPECIFICACIONES TÉCNICAS

- Voltaje de operación: 5V DC
- Corriente de operación: 150mA
- Potencia de consumo: 800mW
- Tiempo de precalentemiento: 20 segundos
- Resistencia de carga: Potenciómetro (Ajustable)
- Detección de partes por millón: 10ppm~1000ppm
- Concentración detectable: Amoniaco, sulfuro, benceno, humo
- Concentración de oxígeno: 2%~21%
- Humedad de operación: <95%RH
- Temperatura de operación: -20°C~70°C

Figura 2.4. Especificaciones técnicas del sensor MQ135[43]

- Alarma de Gas AE09/GM

Detector de gas metano (gas ciudad).
Indicador luminoso y acústico y salida tipo relé, que puede utilizarse para desconectar electroválvula.
Existen diferentes modelos que permiten alimentarlo a 220v, 12v ó 24v.

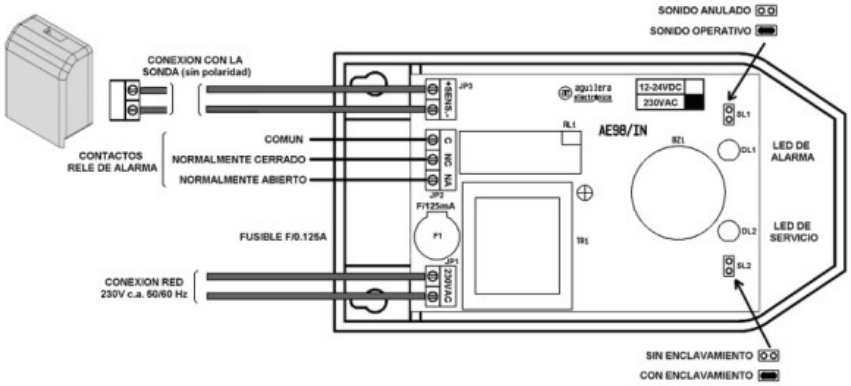
Figura 2.5. Imagen del sensor AE09/GM [44]

- Detector de inundación AE98/IN220

Detector de fugas de agua formado por dos elementos; sonda y dispositivo electrónico.
Indicador luminoso y acústico y salida tipo relé

Figura 2.6. Imagen del dispositivo (izda.) y sonda (derecha) del detector AE98/IN220 [45]

Esquema de Conexionado



CARACTERISTICAS TÉCNICAS		
Alimentación:		230 Vc.a. +/- 10%, 50/60Hz.
Consumo:		2W
Fusible de protección:		F/ 0.125 A
Longitud máxima total cable de conexión:		50 metros.
Cable de conexión de sonda:		2 hilos x 0.75 mm2
Número máximo de sondas:		3
Dimensiones:	Detector:	Alto 130 mm Ancho 70 mm Fondo 52 mm
	Sonda:	Alto 40mm Ancho 33 mm Fondo 17 mm
Material: ABS		1

Figura 2.7. Especificaciones técnicas del detector AE98/IN220[45]

- Detector de fuego y humos AE085/R220B

Detector de humo con indicadores luminosos y zumbador.
Incorpora también relé de salida.

Figura 2.8.. Imagen del dispositivo AE085/R220B [46]

2.2. Aplicación móvil

Los sistemas IoT acostumbran a disponer de una aplicación móvil que permite gestionar y visualizar el estado de la instalación.
Pueden ser desde aplicaciones proporcionadas por el fabricante de un dispositivo, como alarmas, bombillas o enchufes inteligentes, hasta desarrollos complejos para gestionar el tráfico o los aparcamientos de una ciudad.

2.3. Protocolos de comunicaciones en red

Los sistemas IoT utilizan diferentes protocolos de comunicaciones, que podemos agrupar en las siguientes tipologías:

- TCP/IP ; mDNS,DNS-SD,UPnP,WS-Discovery, DICOM.
  Son protocolos TCP/IP diseñados para trabajar de manera más eficiente en redes pequeñas.

- Radio corto alcance: NFC, RFID, Bluetooth, BLE.
  Se utilizan en aplicaciones en las que los dispositivos comunican a corta distancia; relojes inteligentes, dispositivos médicos como bombas de insulina, bombillas …

- Radio largo alcance: LoRa, LoRaWAN, Sigfox.
  Se utilizan en aplicaciones en las que los dispositivos comunican a gran distancia; mediciones inteligentes de agua, electricidad, agricultura, ciudades inteligentes …

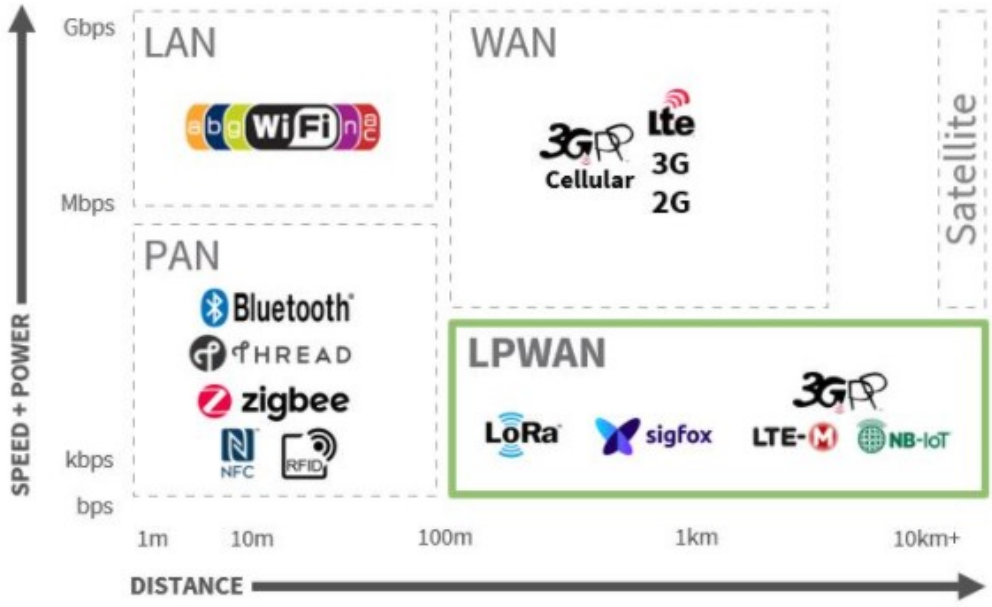


Figura 2.8. Protocolos inalámbricos habituales en sistemas IoT[46]

2.4 Plataformas Cloud

Existen diferentes plataformas en la nube en la que desarrollar aplicaciones IoT. Remarcamos algunas de las más extendidas:

➢ AWS IoT

Conecta los dispositivos IoT a otros dispositivos IoT, así como a los servicios de la red AWS

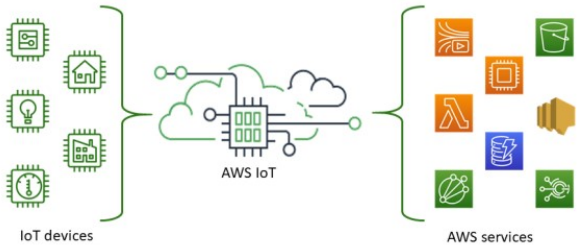


Figura 2.9. AWS IoT [48]

Soporta los protocolos siguientes:

- ✓ MQTT
- ✓ MQTT sobre WSS (Websockets Secure)
- ✓ HTTPS
- ✓ LoraWan

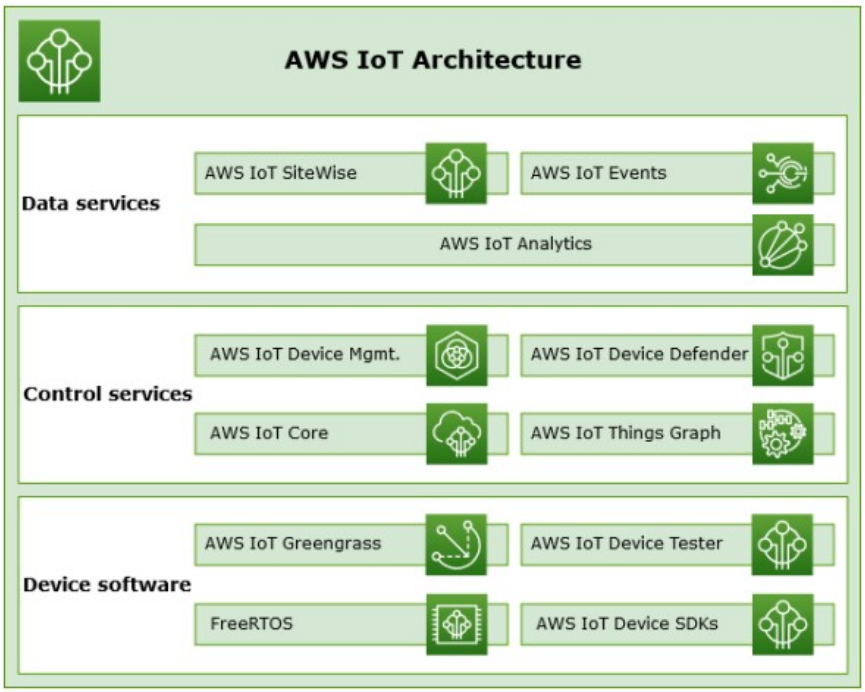


Figura 2.10. Arquitectura AWS IoT [48]

➢ Azure IoT

Admite comunicación mediante MQTT v3.1.1, HTTP 1.1 o AMPQ 1.0 de forma nativa.

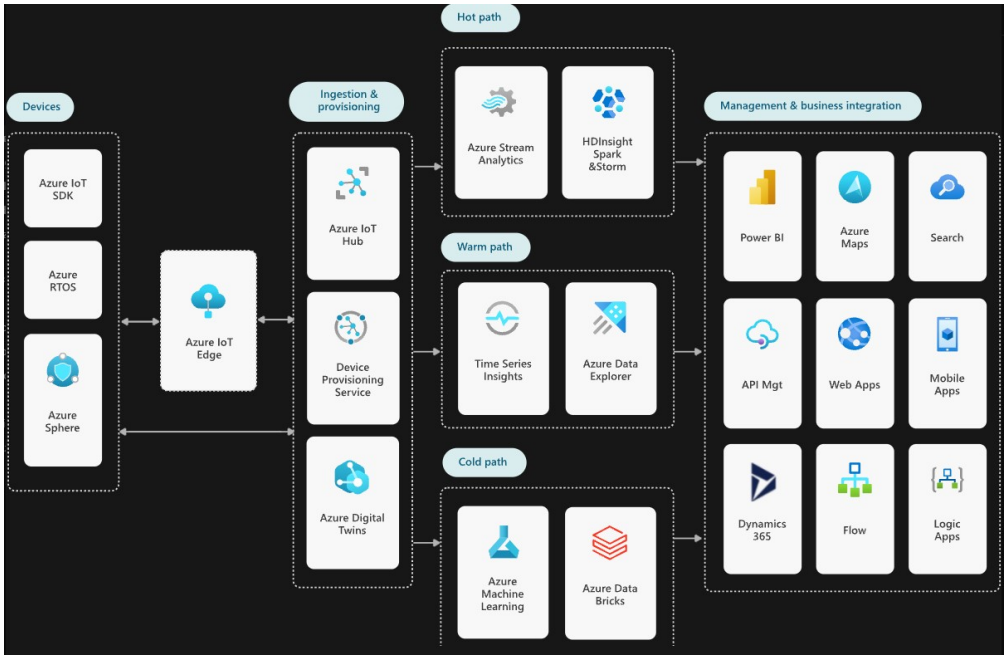


Figura 2.11. Arquitectura Azure IoT [49]

➢ Google Cloud IoT

Soporta comunicación MQTT y HTTP

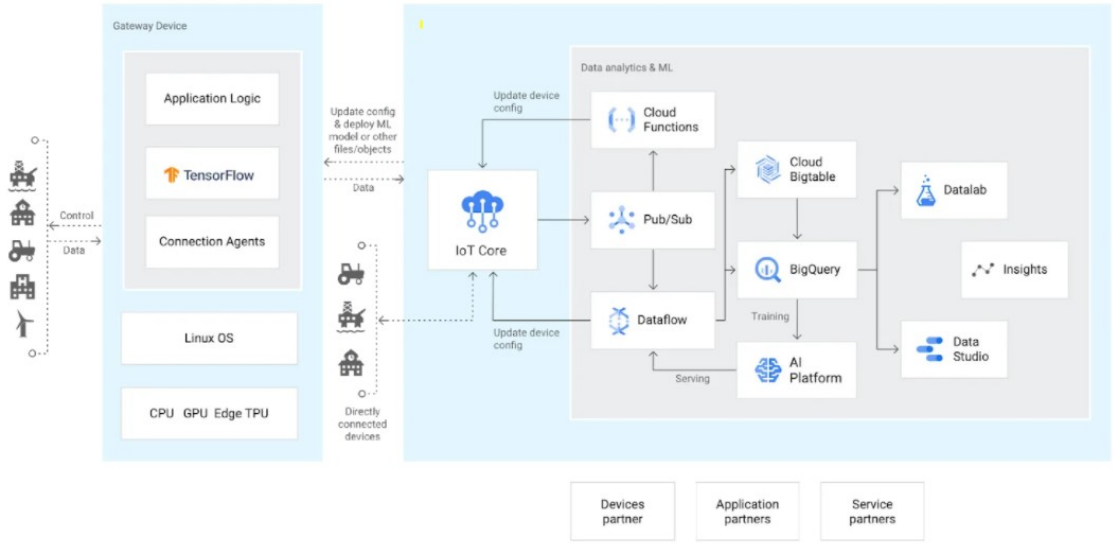


Figura 2.12. Arquitectura Google Cloud IoT [50]

➢ IBM Watson IoT

Soporta comunicación MQTT y HTTP

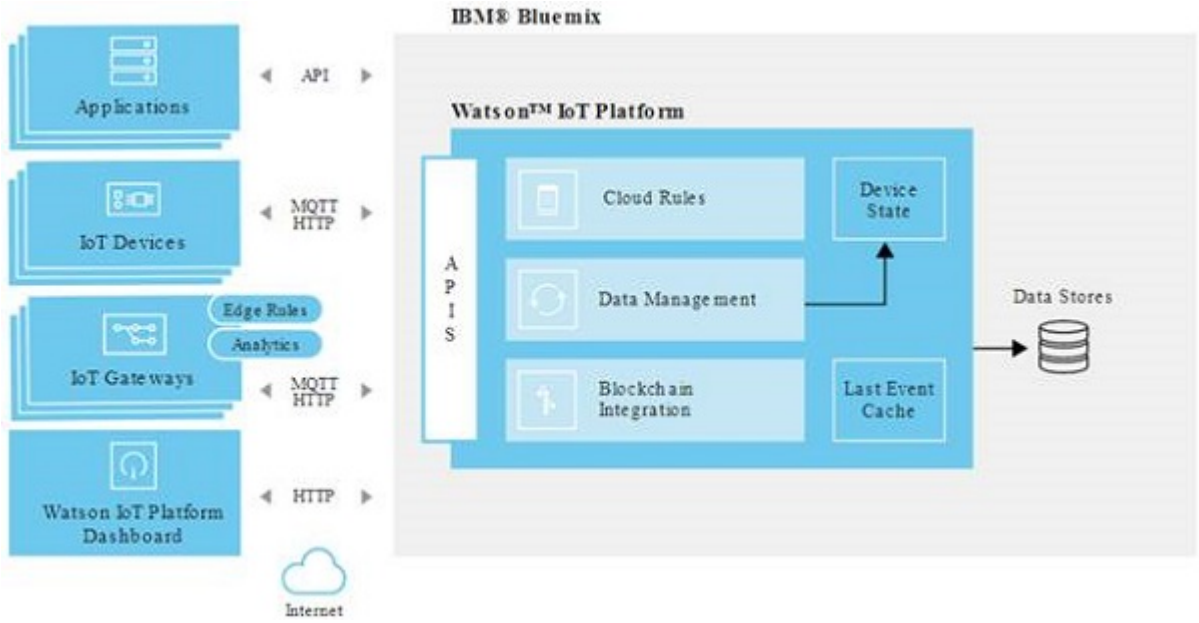


Figura 2.13. Arquitectura IBM Watson IoT [50]

Sin entrar en detalles de cada una de ellas, concluimos que los protocolos más extendidos para comunicar los dispositivos con las diferentes plataformas son MQTT y HTTP. Es habitual que dispongan de planes gratuitos para evaluar la solución, y ofrecen diferentes servicios de cálculo, tratamiento y base de datos.

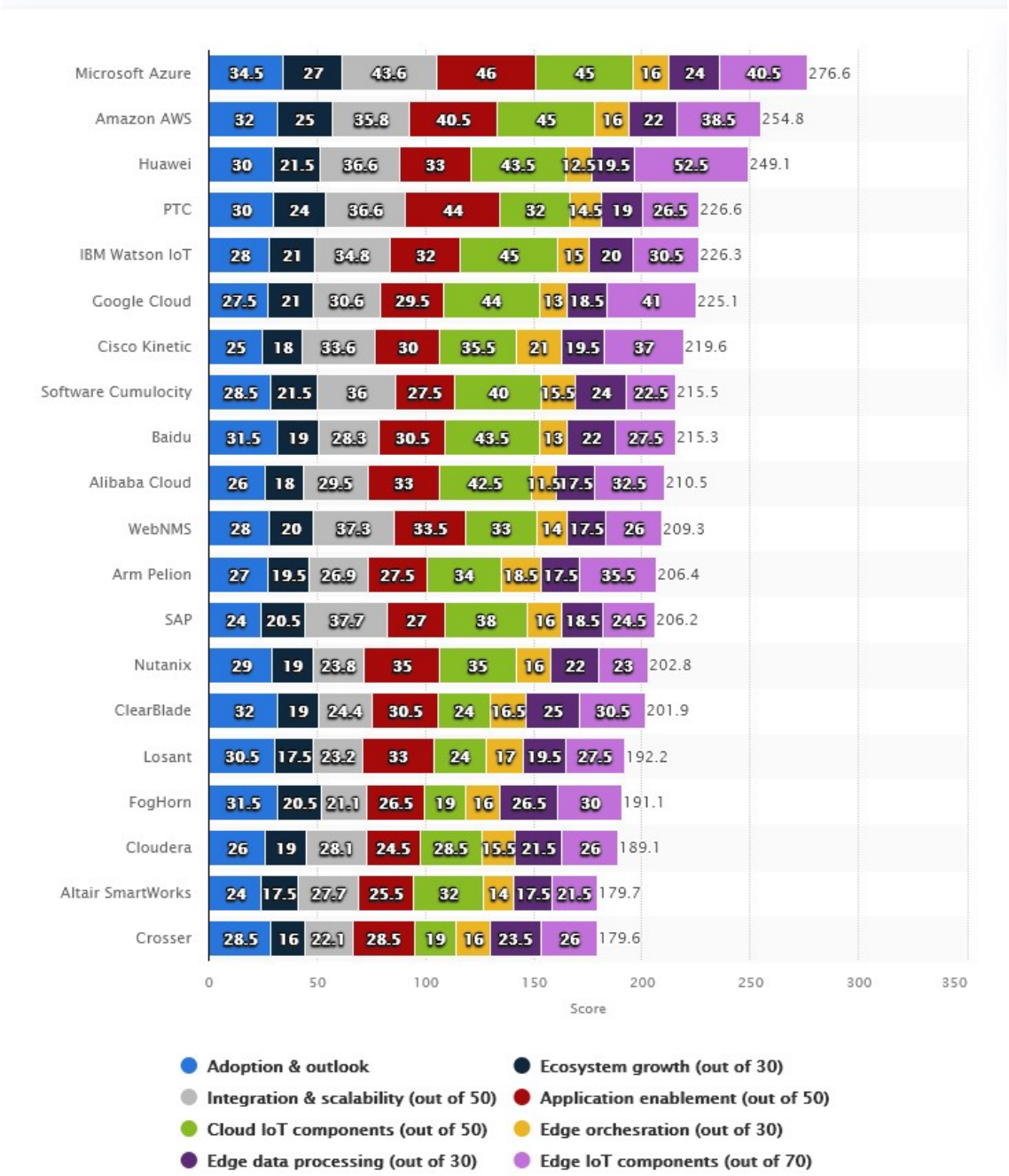


Figura 2.14. Ranking de plataformas IoT 2020. Statista [51]

3. Seguridad en IoT

A diferencia de pruebas de seguridad tradicionales, las pruebas de seguridad IoT requieren examinar y desmontar los dispositivos y trabajar con unos protocolos de red que no se encuentran en otros entornos, analizar aplicaciones móviles para controlar dispositivos, y examinar cómo los dispositivos se comunican con los servicios web el en el *cloud*.
Por otro lado, las restricciones impuestas por la propia tipología del sistema, como el uso de dispositivos pequeños, de bajo coste y bajo consumo aumentan la inseguridad de los mismos.Así, por ejemplo, en lugar de usar criptografía de clave pública, usan claves simétricas, ya que consumen menos recursos.Además, estas claves a menudo no son únicas y están grabadas en el firmware o el propio hardware, con lo que los atacantes pueden extraerlas.

3.1 Vulnerabilidades

Según OWASP [31], los 10 problemas de seguridad más graves de IoT son los siguientes:

1. Contraseñas fáciles o grabadas en el dispositivo
   Mediante ataques de fuerza bruta es relativamente sencillo acceder a los dispositivos.

2. Servicios de red inseguros
   Servicios de red inseguros, en ocasiones innecesarios, que se ejecutan en el dispositivo ponen en riesgo la confidencialidad, integridad y disponibilidad de los datos.

3. Interfaces inseguros
   Los diferentes interfaces (web, API, cloud, aplicaciones móviles) con las que comunica el dispositivo adolecen en muchos casos de falta de autenticación / autorización y encriptado inexistente o débil.

4. Mecanismos de actualización inseguros
   Existen diferentes carencias a la hora de actualizar los dispositivos; validación del firmware, entrega segura, inexistencia de notificaciones …

5. Uso de componentes inseguros u obsoletos
   El uso de componentes o librerías inseguros u obsoletos pueden comprometer el acceso al sistema.

6. Insuficiente protección de la privacidad
   Datos personales utilizados de manera inadecuada o sin permiso

7. Transferencia de datos y almacenamiento inseguro
   Falta de encriptado y control de acceso a datos sensibles

8. Falta de gestión del dispositivo
   Falta de soporte de seguridad en dispositivos en funcionamiento

9. Configuración por defecto insegura

Dispositivos comercializados con configuraciones inseguras.

10. Falta de *'Physical hardening'*
    No se adoptan medidas que puedan evitar o limitar los accesos no autorizados a los dispositivos.

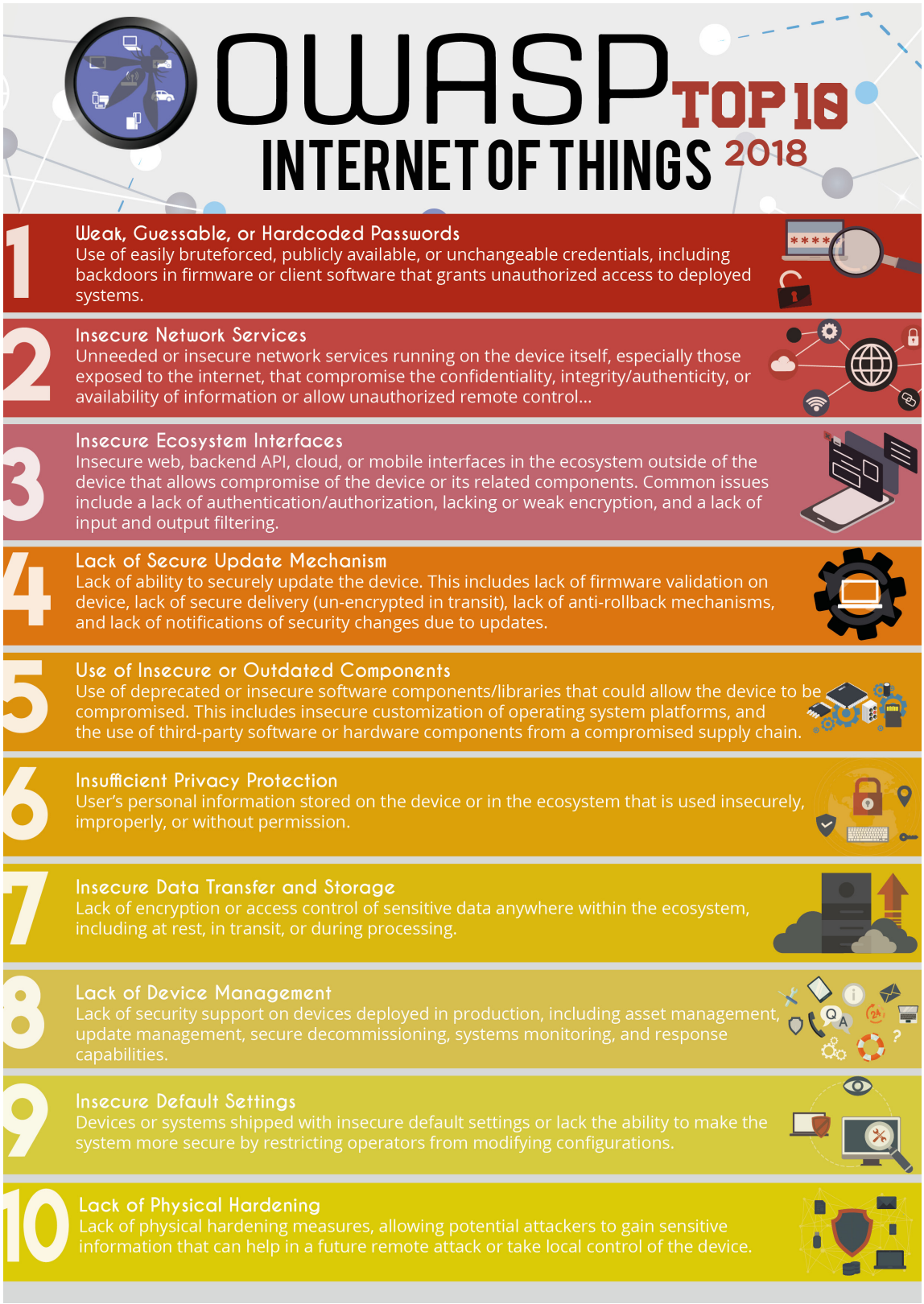


Figura 3.1. Top 10 riesgos IoT según OWASP [31]

3.2 Modelado de Amenazas

En cuanto al modelado de amenazas, no difiere del que se realiza en otro tipo de sistemas. Así, es normal el uso de marcos de trabajo habituales, como STRIDE, de Microsoft, PASTA, Trike, OCTAVE [32],VAST, Security Cards o Persona non Grata [33]

	Maturity	Focus/Perspective	Time/Effort	Mitigation	Consistent results
STRIDE	High	Defender	High	Yes	No
PASTA	High	Risk	High	Yes	No
LINDDUN	High	Assets/Data	High	Yes	No
CVSS	High	Scoring	High	No	Yes
Attack Trees	High	Attacker	High	No	Yes
PnG	Medium	Attacker	Medium	No	Yes
Security Cards	Medium	Attacker	Medium	No	No
hTMM	Low	Attacker/Defender	High	No	Yes
Quantitive TMM	Low	Attacker/Defender	High	No	Yes
Trike	Low	Risk	High	Yes	No
VAST	High	Attacker	High	Yes	Yes
OCTAVE	Medium	Risk/Organization	High	Yes	Yes

Figura 3.2. Características de los principales métodos de modelado de amenazas [33]

Las amenazas más típicas son las siguientes:

- ✓ Ataques de interferencia de señal
  El atacante interfiere la comunicación entre dos sistemas

- ✓ Ataques de repetición
  El atacante repite una operación o reenvía paquetes ya enviados.

- ✓ Ataques de modificación de la configuración
  El atacante se aprovecha de la falta de verificación de integridad de un componente para alterar su configuración.

- ✓ Ataques a la integridad del hardware
  Comprometen la integridad del dispositivo físico.

- ✓ Clonado de nodos
  El atacante crea nodos falsos en una red para comprometer su fiabilidad.

Los protocolos utilizados en IoT no son muy sofisticados, lo que propicia este tipo de ataques.

- ✓ Brechas de seguridad y privacidad
  Es una de las amenazas más importantes en IoT. A menudo, existe muy poca protección de los datos confidenciales.

- ✓ Conciencia de seguridad del usuario
  Probablemente la amenaza más complicada de afrontar.

3.3. Metodología de verificación de seguridad en sistemas IoT

Los sistemas IoT habitualmente están formados por diferentes componentes que interactúan entre sí. Por ello es necesario seguir una metodología completa y robusta en el análisis de seguridad. Una de ellas, basada en análisis de capas conceptuales, la encontramos en [21]. Se basa en los siguientes apartados:

3.3.1. Reconocimiento pasivo (*Passive reconnaissance*)

También conocido como OSINT, Open Source INTelligence, hace referencia al proceso de recopilar información sin comunicar directamente con el sistema.
Así, algunas de las fuentes a las que podemos recurrir son:

- ➢ Manuales
  Los manuales de dispositivos pueden aportarnos información tan variada como usuarios y contraseñas por defecto, especificaciones detalladas del sistema, diagramas de la arquitectura, o apartados de resolución de problemas, que pueden conducirnos a identificar puntos débiles.

- ➢ Patentes
  Las patentes pueden proporcionarnos información sobre el funcionamiento interno de ciertos equipos. Podemos consultarlas en https://patents.google.com [34]

- ➢ Conocimiento del usuario
  A través de redes sociales, fórums, y otras páginas web podemos recabar información sobre algunos sistemas. Investigando opiniones de un determinado dispositivo en *Amazon*, páginas de consumidores, foros relacionados con el mismo, podemos obtener indicios de algunas vulnerabilidades.
  Por otro lado, investigando perfiles profesionales de ingenieros de fabricantes de equipos, podemos llegar a deducir qué tecnologías o hardware se han empleado en la construcción del mismo.

3.3.2. Capa física o hardware

Uno de los vectores de ataque más importantes es el hardware.

- ➢ Interfaces de periferia

Consideramos interfaces de periferia cualquier puerto de comunicación que permita conectar dispositivos externos, como teclados, discos duros, tarjetas de red …
Verificamos si los puertos USB están activos y son arrancables; se puede acceder al contenido del disco de muchos sistemas arrancando con un sistema operativo desde un puerto USB.

- Entorno de arranque
  En sistemas con *BIOS* convencional se debe verificar que esté protegida con contraseña y que en el orden preferido de arranque los dispositivos removibles no se encuentren en primer lugar, ya que ello permitiría arrancar con otro sistema operativo sin tener que modificar la BIOS.
  Revisaremos también si el sistema tiene habilitado *PXE, Preboot Execution Environment,* que puede permitir al atacante introducir servidores de arranque en la red.
  Unified Extensible Firmware Interface (UEFI) Secure Boot es un standard de seguridad que valida el arranque comprobando la firma de los drivers *UEFI* con el sistema operativo.
  Existen tecnologías de arranque seguro, *Trusted Execution Environment (TEE)*, en platafomas de los fabricantes *Qualcomm* y *Arm*.

- Cierres
  Verificar si el equipo tiene algún sistema de cierre o bloqueo, y si resulta fácil evitarlo. Comprobar también si existe una llave universal que abre los cierres de todos los dispositivos, o si realmente la llave es la misma.

- Detección y protección contra manipulaciones
  Verificar si el equipo es resistente a manipulaciones y muestra evidencias de ello. Existen diferentes sistemas, como cierres con *epoxy*, pintura en tornillos, fusibles que borran contenido sensible si se desmonta el dispositivo.
  Los sistemas de detección de manipulación envían alertas o crean ficheros de log.

- Firmware
  El firmware es el software que comunica y controla los componentes hardware de un equipo
  Es importante examinarlo e intentar modificarlo para descubrir posibles problemas de seguridad. Para ello, podemos seguir la metodología *OWASP Firmware Security Testing Methodology*, FSMT [35]

- Interfaces de depuración
  Revisar interfaces de depuración, puntos de test que los fabricantes utilizan para verificar el producto durante el proceso de fabricación. Conectándonos a ellos podemos tener acceso de usuario administrador. Los puntos de depuración más comunes son *UART,JTAG,SPI* e *I2C*. Por lo tanto, necesitaremos cierto conocimiento en estos protocolos y hardware para el conexionado; clips *SOIC*,conversor serie-*USB* …

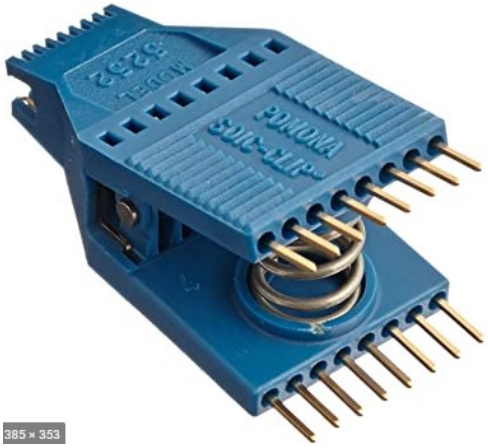


Figura 3.3. Clip SOIC de 8 pines

Figura 3.4 Conversor USB Serie

- Robustez física
  Verificar las limitaciones debidas a las características físicas del dispositivo. Así, por ejemplo, asegurar el sistema ante ataques de descarga de batería, en los que el atacante fuerza el envío de tramas del sistema continuamente, propiciando así la descarga de la batería [35]
  Otro tipo de ataque son los ataques de fallo (*glitching attacks*) que intentan provocar fallos de hardware durante operaciones sensibles [36]

3.3.3. Capa de red

La capa de red, que incluye todos los elementos que comunican directa o indirectamente a través de una red de comunicaciones, es normalmente el vector de ataque más grande. Lo dividimos en los siguientes apartados:

- Reconocimiento
  Ya hemos comentado el reconocimiento pasivo previamente; ahora incluimos también el reconocimiento activo, que requiere interactuar con el elemento en cuestión.

- Descubrimiento de servidores
  Consiste en determinar qué equipos existen en el sistema, mediante el uso de diferentes técnicas; envío de paquetes *ICMP (Internet Control Message Protocol),* escaneos de puertos *TCP/UDP*, escuchar el tráfico broadcast de la red, o peticiones *ARP*.

- Detección de versiones de servicios
  Una vez detectados los equipos existentes en la red, se trata de descubrir los servicios que están escuchando. Para ello, podemos utilizar herramientas como *Nmap*.

- Identificación de sistema operativo
  Se trata de identificar el sistema operativo de cada equipo. Nuevamente, podemos hacer uso de la herramienta *Nmap*.

- Mapeo de Topología
  Este punto hace referencia al caso en el que el sistema no disponga de todos los elementos en el mismo segmento de red, sinó que se hallen interconectados a través de enrutadores y *firewalls*. Disponer de un mapa de la red puede ser útil el modelado de amenazas; ayuda a ver cómo un ataque que explota una cadena de vulnerabilidades en diferentes servidores puede conducir a un evento crítico en el sistema.

➢ Protocolos de red y ataques a servicios
- Escaneo de vulnerabilidades
  El primer paso sería revisar bases de datos, como *NVD, National Vulnerability Database*, buscando vulnerabilidades conocidas en los servicios expuestos.

- Análisis de tráfico de red
  Realizar una captura del tráfico de red mediante alguna herramienta como *Wireshark* o *tcpdump*. Posteriormente, analizar esas capturas buscando protocolos vulnerables, como *UPnP*, y protocolos propietarios, que requerirán un examen detallado o ingeniería inversa.

- Protocolos de Ingeniería Inversa
  Se debería utilizar ingeniería inversa en cada protocolo propietario que se descubra

- Explotación de protocolo o servicio
  El último paso consiste en desarrollar un pequeño programa que pueda explotar las vulnerabilidades detectadas.

➢ Chequeo protocolos Wireless
El chequeo de los protocolos sin cables se solapa con los puntos ya comentados de *Análisis de tráfico de red* y *Protocolos de Ingeniería*

inversa en el apartado anterior, *Protocolos de red y ataques a servicios*.
Para esta fase se necesitará hardware especial, chipsets *Wi-Fi*, como *Atheros*, *dongles Bluetooth* como *Ubertooth*, y herramientas de radio como *HackRF* o *LimeSDR*

- RFID
  RFID surgió para reemplazar los códigos de barras. Funciona transmitiendo datos a través de ondas de radio. Existen diferentes rangos de frecuencia, y cada una de estas tecnologías RFID sigue un protocolo distinto.
  Con lectores de tarjetas RFID como *Proxmark3*, es posible clonar algunas tarjetas, como las *MIFARE Classic cards*, unas de las más vulnerables.

- BLE, Bluetooth Low Energy
  BLE es una versión de *Bluetooth* de bajo consumo, por lo que es muy utilizada en dispositivos IoT.
  Necesitaremos hardware específico para interactuar con BLE, y también software específico, como *BlueZ*[39] o *Hciconfig*

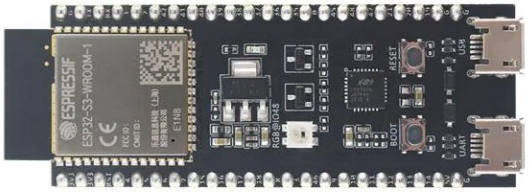


Figura 3.5. ESP32-S3-DevKitC-1-N8 [39]

- Wi-Fi
  Revisar uso de WEP, fácilmente descifrable, y de WPA/ WPA2 con credenciales débiles.
  Para realizar pruebas necesitaremos disponer de una tarjeta Wi-Fi que soporte *Access Point* en modo monitor e inyección de paquetes, como la tarjeta Alfa Atheros AWUS036NHA.

Figura 3.6. Tarjeta Alfa AWUS036NHA

- LPWAN, Low-Power Wide Area Network
  LPWAN es un grupo de tecnologías sin cables, bajo consumo y red extensa diseñadas para comunicaciones de largo alcance y baja frecuencia de transferencia. Estas redes pueden alcanzar más de 10 kilómetros, y las baterías pueden durar hasta 20 años.

3.3.4. Aplicación web

Existen muchos recursos para la evaluación de aplicaciones web; muchos de ellos los podemos encontrar en OWASP[32]. Por ello, nos centramos en técnicas que aplican a aplicaciones web halladas en dispositivos IoT.

- Mapeo de aplicación
  El objetivo es descubrir todos los puntos de entrada, explorando el *website* visible, oculto y el contenido por defecto. Por ejemplo, en alguna cámara se ha descubierto una URL oculta que permitía conectarse de manera anónima y tomar fotografías.

- Controles lado cliente
  Los controles del lado cliente incluyen campos ocultos, cookies y applets de Java. Hay muchas aplicaciones en dispositivos embebidos que realizan la autenticación en el lado cliente.

- Autenticación
  Un buen número de sistemas IoT disponen de credenciales preconfiguradas muy débiles. Se pueden realizar ataques de fuerza bruta con ficheros de diccionario para verificar su robustez.
  Revisar también si la transmisión de credenciales se realiza por *http* en lugar de *https*, examinar las funcionalidades de contraseña olvidada.

- Gestión de la sesión

- Control de Acceso y autorización
  Verificar el control de acceso y los privilegios asignados a cada usuario, en función del rol que tenga asignado.

- Validación de entradas
  Revisar que la validación de los datos introducidos por el usuario se realiza correctamente. Los ataques por inyección habitualmente ocupan los primeros lugares en la lista TOP 10 OWASP [31]

- Fallos de lógica de la aplicación

- Servidor de la aplicación
  Revisar que el servidor que aloja la aplicación web es un servidor seguro

3.3.5. Revisión configuración servidor

- Cuentas de usuario
  Revisar la configuración de las cuentas de usuario en el sistema; la existencia de cuentas por defecto, así como las políticas relativas a las mismas (caducidad de contraseñas, mecanismos de bloqueos …)
  No es extraño encontrar usuarios locales con contraseña que no caduca idéntica al nombre de usuario.

- Fortaleza de la contraseña
  Revisar la fortaleza de la contraseña; requisitos de complejidad.

- Privilegios de las cuentas
  Revisar que las cuentas y servicios están configuradas siguiendo el principio del mínimo nivel necesario; deben acceder exclusivamente a los recursos que necesiten, y nada más.

- Nivel de parcheo
  Revisar que el sistema operativo, las aplicaciones y las librerías se encuentren actualizadas.

- Mantenimiento remoto
  Revisar la seguridad del mantenimiento y las conexiones remotas de soporte.

- Controles de Acceso al sistema de ficheros
  El principio del mínimo privilegio debe aplicar también a los ficheros y directorios importantes.

- Encriptado de datos
  Revisar que los datos sensibles estén encriptados.

- Errores de configuración del servidor
  Servicios mal configurados pueden ser inseguros. Evitar que existan servicios ejecutándose con usuarios por defecto, por ejemplo.

3.3.6. Aplicación móvil y *cloud*

Hoy en día utilizamos el móvil para encender la televisión, gestionar la alarma, apagar las luces o cambiar la hora de encendido del enchufe inteligente. Por ello, si un atacante tomara el control del teléfono, podría controlar la casa.

- Aplicaciones móviles
  Nuevamente, podemos consultar *OWASP*, que nos presenta la lista *OWASP Mobile Top 10 [52]* y otros documentos, como *Mobile Security Testing Guide [53]* y *Mobile Application Security Verification.[54]*

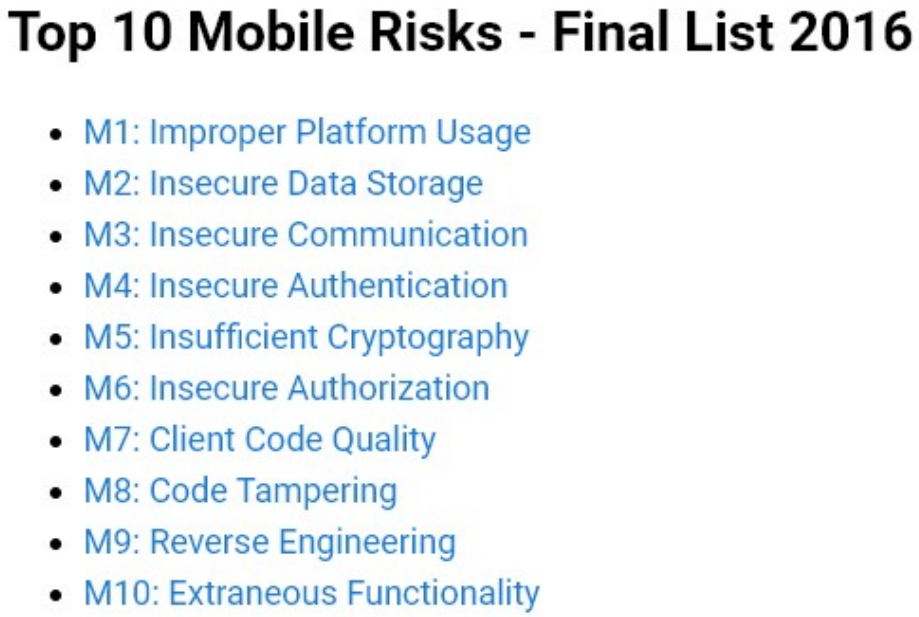


Figura 3.6. OWASP Mobile Top 10 [52]

- Cloud
  Examinar las interacciones entre el cloud y los dispositivos IoT.
  Existe un rango amplio de vulnerabilidades relacionadas con el *cloud;* claves API embebidas en el código de aplicaciones móviles y/o en firmware binario, exposición de los servicios de Intranet …

4. Arquitectura proyecto piloto

Una vez hemos descrito la metodología de seguridad a aplicar en proyectos IoT, planteamos el desarrollo de un sistema IoT doméstico, sobre el que aplicar dicho modelo.

4.1 Componentes hardware

Utilizaremos una serie de sensores:

- Sensor de temperatura y humedad DHT22
- Detector de incendios AE85 o similar
- Detector de inundaciones AE98 o similar
- Bombilla inteligente
- Cámara vigilancia

Como dispositivo central, usaremos una RaspBerry Pi 8Gb
Monitor 22,5 pulgadas
Disco duro externo 128 Gbytes
Switch 5 puertos

4.2 Componentes software

Software Home Assistant

- Software de Código abierto para la automatización de hogares

App móvil Home Assistant

Servicio IFTT

4.3 Diseño

Diseñaremos el control domótico de una casa, visualizando las lecturas de los sensores y activando una serie de alarmas al cumplirse las condiciones establecidas.

La aplicación nos permitirá interactuar con los elementos, encendiendo y apagando bombilla, consultar imágenes cámara, valores sensores…

Concretamente, nos debe permitir las siguientes operaciones:

- Visualizar temperatura y humedad
- Visualizar estado de detector de incendios
- Visualizar estado de detector de inundaciones
- Recibir alarma en caso de activarse detector de incendios (visual en aplicación y mensaje correo electrónico)
- Recibir alarma en caso de activarse detector de inundaciones (visual en aplicación y mensaje correo electrónico)
- Visualizar imagen de la cámara
- Encender y apagar bombilla

Una vez operativo el proyecto piloto IoT, procederemos a aplicar la metodología de seguridad descrita en el apartado 3, teniendo en cuenta los apartados que sean de aplicación a este proyecto concreto.

5. Conclusiones

6. Glosario

AMQP (Advanced Message Queuing Protocol): Protocolo abierto de la capa de aplicaciones.

API (Application Programming Interface): Capa de software intermedia que permite a dos aplicacions hablar entre ellas.

ARP (Address Resolution Protocol): Protocolo que sirve para associar una dirección IP a una dirección física (dirección MAC).

Big Data: Conjuntos de datos cuyo tamaño, complejidad y volumen de crecimiento hace que no puedan ser gestionados mediante métodos y herramientas tradicionales.

BIOS (Basic Input Output System): Programa grabado en una memoria no volátil y que sirve para realitzar las operaciones de inicio al poner en marcha el equipo.

BLE (Bluetooth Low Energy): protocolo de comunicaciones que prmite la transmisión inalámbrica de datos a corta distancia y con bajo consumo de energia.

Bluetooth: protocolo de comunicaciones que permite la transmisión inalámbrica de datos a corta distancia (menos de 10 metros).

DICOM (Digital Imaging and Communications): Estándar internacional para comunicar y gestionar imágenes y datos médicos.

DNS (Domain Name System): Sistema de nomenclatura jerárquico y descentralizado para dispositives conectados a redes IP. Permite associar nombres a direcciones IP.

DNS-SD (DNS Service Discovery): Protocolo ligero para la búsqueda de servicios en la red.

FDA (Food and Drug Administration): Agencia del gobierno de los Estados Unidos, responsable de alimentos, medicamentós y cosméticos.

FSTM (Firmware Security Testing Methodology): Metodología de testeo de firmware de OWASP

HTTP (Hyper Text Transfer Protocol): Protocolo de comunicación en la capa de aplicaciones.

I2C (Inter-Integrated Circuit): Protocolo utilizado para establecer comunicación entre dos o más circuitos integrados.

ICMP (Internet Control Message Protocol): Protocolo IP utilizado para enviar mensajes de error e información operativa.

IIoT: Industrial Internet of Things o internet de las cosas Industrial. Hace referencia a la interconexión de màquines a través de Internet en el ámbito industrial.

IoT: Internet of Things o Internet de las cosas. Hace referencia a la interconexión de máquinas a través de Internet.

JTAG (Join Test Action Group): Nombre comúnmente aceptado para la Norma IEEE 1149.1, Standard Test Access Port and Boundary-Scan Architecture, utilitzada para la verificación de placss de circuitos Electrónicos.

LoRa (Long Range): Tecnología inalámbrica de largo alcance (10 a 20 Km) y bajo consumo (hasta 10 años de duración una bateria), desarrollada por la compañía Semtech.

LoRaWAN (Long Range Wide Area Network): Hace referencia a una red de nodos Lora.

mDNS (multicast DNS): Servicio diseñado para la resolución de nombres en redes pequeñas.

MQTT: Protocolo de red basado en sistema publicación-suscripción

NFC (Near Field Communication): Tecnología inalámbrica de alta frecuencia y muy colot alcance (10 – 15 cm).

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation): Metodología de análisis de riesgos desarrollada por la Universidad Carnegie Mellon en el año 2001**.** Estudia los riesgos en base a tres principios; Confidencialidad, Integridad y Disponibilidad.

OSINT (Open Source INTelligence): Conjunto de técnicas y herramientas para recopilar información pública.

OWASP (Open Web Application Security Project): Fundación sin ánimo de lucro, formada por empreses y profesionales que promueven el desarrollo de software seguro

PASTA (Process for Attack Simulation and Threat Analysis): Modelado de amenazas que combina la perspectiva del atacante con el anàlisis de riesgos e impacto.

PnG (Persona non Grata): Modelado de amenazas que se centra n las motivacions y habilitades de las persones atacantes.

PXE (Preboot Execution Environment): Entorno para arrancar e instal·lar el sistema operativo a través de la red.

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges): modelo de amenazas desarrollado por Praerit Garg y Loren Kohnfelder en Microsoft

RFID (Radio Frequency Identification): Sistema de identificación y transmisión de información a través de ondas de radiofrecuencia.

Security Cards: Sistema de modelado de amenazas basado en el uso de 42 cartas y técnicas de *brainstorming*.

Sigfox: Red IoT de bajo consumo.

SOIC (Small Outline Integrated Circuits): Tipo de encapsulado de chips.

SPI (Serial Peripheral Interface): Estándar de comunicaciones usado para la transferència de información entre circuitos integrados.

Trike: Sistema de modelado de amenazas desde la perspectiva de la gestión de riesgos y la defensa.

SSD: Solid State Drive o Disco de Estado Sólido. Tecnología de almacenamiento sin uso de componentes mecánicos.

TEE (Trusted Execution Environment): Entorno de ejecución de código con alto nivel de confianza en los activos que rodean al entorno.

UEFI (Unified Extensible Firmware Interface): Código de firmware en la placa base que ofrece funciones adicionales a las de la BIOS.

UART (Universal Asynchronous Receiver-Transmitter): Dispositivo que controla los puertos y serie.

UPnP (Universal Plug and Play): Protocolo de comunicación en una red privada que permite descobrir a otros dispositives y establecer comunicación.

VAST (Visual, Agile,Simple, Threat modelling): Metodología de modelado de amenazas centrada en el ciclo de desarrollo del software.

Wi-Fi: Tecnología que permite la interconexión de diferentes dispositivos sin utilizar cables.

Wi-Fi Direct: Tecnología inlamámbrica para la comunicación directa entre dispositives.

WS-Discovery (Web Services Dynamic Discovery): especificación técnica que definí un protocolo de descubrimiento de Servicios en la red.

ZigBee: protocolo de comunicaciones inalámbricas de uso habitual en domótica.

7. Bibliografía

[1] Internet of Things (IoT) in Europe Statista https://www-statista-com.eu1.proxy.openathens.net/study/42750/internet-of-things-iot-in-europe/ Visitado 24/09/2021I

[2] **Iria da Cunha** El trabajo de fin de grado y de máster: Redacción, defensa y publicación. Primera Edición. Oberta UOC Publishing S.L. Octubre 2015

[3] **Rodrigo Martínez Jacobson** Comparativa y estudio de plataformas IOT. Trabajo fin de Grado en Ingeniería Informática. UPC. Primavera 2017

[4] **Daniel Torán Mercadé** Comparison of different Internet of Things platforms Trabajo fin de Grado en Ingeniería Industrial ETSEIB. UPC. Enero 2018

[5] **Anandika sharma y Dr.Amardeep Singh** Review on Internet of Things Attacks and Their Countermeasure using Lightweight Cipher Algorithms *International Journal of Advanced Research in Computer Science* p. 2375-2379 Volume 8, No. 5, May – June 2017

[6] **Lo'ai Tawalbeh Fadi Muheidat,Mais Tawalbeh and Muhannad Quwaider** IoT Privacy and Security: Challenges and Solutions *Applied Sciences 2020,10, 4102.* Published 15 June 2020

[7] **Rohit Malik, Kamna Solanki, Sandeep Dalal** LITERATURE REVIEW ON SECURITY ASPECTS OF *IOT International Journal of Advanced Research in Computer Science* p.123-126 Volume 9, No. 2, March-April 2018

[8] **Enric Nogales Romero** SUPERVISIÓ DE DADES D'UNA PLANTA MITJANÇANT TECNOLOGIES IoT Trabajo fin de Grado en Ingeniería Electrónica Industrial y Automática. UPC. Junio 2017

[9] **Oriol Solà Campillo** Security Issues in Internet of Things Proyecto final de carrera Ingeniería Telecomunicaciones. UPC 2017.

[10] **Hiren Dutta, Parama Bhaumik** Survey on systems architecture for Internet of Things (IoT) *i-manager's Journal on Software Engineering* p.23-39 Vol. 15 No. 1 July - September 2020

[11] **Ferran Fàbregas** Aprender Raspberry Pi 4 con 100 ejercicios prácticos 3ª Edición.Ed. Marcombo. 2020

[12] **Gregorio Chenlo** Home Automation with Raspberry, Google & PythonPrinted by Amazon Italia 2020

[13] Objetivos de Desarrollo Sostenible. Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación https://www.un.org/sustainabledevelopment/es/infrastructure/ Visitado 25/09/2021

[14] **Alfonso González Fernández** Seguridad en Smartphones. Análisis de riesgos, de vulnerabilidades y auditorías de dispositivos.Trabajo fin de Máster MISTIC. UOC. Enero 2018.

[15] **Benjamin Khoo** RFID as an Enabler of the Internet of things: Issues of Security and Privacy iThings/CPSCom 2011: 709-712 2011 IEEE International Conference on Internet of Things (iThings) & 4th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom), Dalian, China, October 19-22, 2011. IEEE Computer Society 2011, ISBN 978-1-4577-1976-9

[16] **Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva** Security for the IoT: A Survey of Existing Protocols and Open Research issues IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 3, THIRD QUARTER 2015

[17] **Mario Weber and Marija Boban** Security challenges of the Internet of things MIPRO 2016, May 30 - June 3, 2016, Opatija, Croatia

[18] **KrishnaKanth Gupta and Sapna Shukla** Internet of things: Security Challenges for Next Generation Networks 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)

[19] **Gurpreet Singh Matharu, Priyanka Upadhyay and Lalita Chaudhary** The Internet of things: Challenges & Security Issues 2014 International Conference on Emerging Technologies (ICET)

[20] **Aditya Gupta** The IoT Hacker's Handbook Apress 2019

[21] **ETSI European Telecommunications Standards Institute** Technical Specification for Cyber Security for Consumer Internet of Things

[22] **UK Department for Digital, Culture, Media & Sport** Code of Practice for Consumer IoT Security 2018.

[23] **Australian Government** Securing the Internet of Things for Consumers Code of Practice. 2020

[24] **ENISA, European Union Agency for Network and Information Security** Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures November 2017

[25] **ENISA Good practices for IoT and Smart Infrastructures Tool**
https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT Visitado 15/10/2021

[26] **Mapping Security & Privacy in the Internet of Things**
https://iotsecuritymapping.uk/by-sector-and-body/Visitado 15/10/2021

[27] **NIST Cybersecurity for IoT Program**
https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
Visitado 15/10/2021

[28] **I AM THE Cavalry** https://iamthecavalry.org/ Visitado 15/10/2021

[29] **Hippocratic Oath for Connected Medical Devices**
https://iamthecavalry.org/issues/medical/oath/
Visitado 15/10/2021

[30] **OWASP**
https://owasp.org
Visitado 15/10/2021

[31] **OWASP Internet of Things TOP 2018**
https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main
Visitado 15/10/2021

[32] **Fotios Chantzis and Ioannis Stais** Practical Iot Hacking: The Definitive Guide to Attacking the Internet of Things Random House US. 2021

[33] **Introducción al análisis de riesgos – Metodologías (II)**
https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/
Visitado 16/10/2021

[34] **Nataliya Shevchenko, Brent R. Frye, and Carol Woody, PhD**
THREAT MODELING FOR CYBER-PHYSICAL SYSTEM-OF-SYSTEMS: METHODS EVALUATION
Carnegie Mellon University Software Engineering Institute September 2018

[34] **Google Patents**
https://patents.google.com
Visitado 16/10/2021

[35] **OWASP Firmware Security Testing Methodology (FSTM)**
https://scriptingxss.gitbook.io/firmware-security-testing-methodology/
Visitado 23/10/2021

[36] **IEEE Institute of Electrical and Electronic Engineers** Std 1149.1 – 1990 IEEE Standard Test Access Port and Boundary-Scan Architecture 1993

[37] **Il-Gu Lee, Kyungmin Go and Jung Hoon Lee**
Battery Draining Attack and Defense against Power Saving Wireless LAN Devices *MDPI sensors* Published April 2020 Sensors 2020, 20(7), 2043

[38] **J. Korczyc and A. Krasniewski,** "Evaluation of susceptibility of FPGA-based circuits to fault injection attacks based on clock glitching," 2012 IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2012, pp. 171-174, doi: 10.1109/DDECS.2012.6219047

[39] **Espressif Development boards**
https://www.espressif.com/en/products/devkits
Visitado 23/10/2021

[40] **Mouser Electronics**
https://www.mouser.es/ProductDetail/Espressif-Systems/ESP32-S3-DevKitC-1-N8?qs=Wj%2FVkw3K%252BMCTHFMHLvA1pQ==
Visitado 23/10/2021

[41] **BlueZ Official Linux Bluetooth protocol stack**
https://bluez.org
Visitado 23/10/2021

[42] **Naylamp Mechatronics**
https://naylampmechatronics.com/sensores-temperatura-y-humedad/58-sensor-de-temperatura-y-humedad-relativa-dht22-am2302.html
Visitado 23/10/2021

[43] **Naylamp Mechatronics**
https://naylampmechatronics.com/sensores-gas/73-sensor-mq-135-gas-calidad-aire.html
Visitado 23/10/2021

[44] **Aguilera Electrónica**
https://aguilera.es/documentacion/Equipos%20Aut%C3%B3nomos/Manuales/ae09-gm-manual.pdf
Visitado 23/10/2021

[45] **Aguilera Electrónica**
https://aguilera.es/documentacion/Equipos%20Aut%C3%B3nomos/Fichas%20tecnicas/ae98-in220-ficha-tecnica.pdf
Visitado 23/10/2021

[46] **Detectores Autónomos de Humos**
http://www.climacity.com/2006/imprimirproducto.php?cod=507
Visitado 23/10/2021

[47] **An introduction to wireless technologies in IoT- LPWAN**
https://www.allion.com/iot-lpwan/
Visitado 23/10/2021

[48] **AWS IoT Core Developer Guide**
https://docs.aws.amazon.com/es_es/iot/latest/developerguide/iot-dg.pdf#what-is-aws-iot
Visitado 25/10/2021

[49] **Arquitectura de referencia de Azure IoT**
https://docs.microsoft.com/es-es/azure/architecture/reference-architectures/iot
Visitado 25/10/2021

[50] **IoT Core**
https://cloud.google.com/iot-core?hl=es-419
Visitado 25/10/2021

[51] **Ranking of Internet of Things (IoT) platforms by completeness/end-to-end capabilities, as of 2020**
https://www-statista-com.eu1.proxy.openathens.net/statistics/1132818/iot-platforms-ranking-worldwide/
Visitado 25/10/2021

[52] **OWASP Mobile Top 10 List**
https://owasp.org/www-project-mobile-top-10/
Visitado 25/10/2021

[53] **Bernhard Mueller, Sven Schleier, Jeroen Willemsen, Carlos Holguera** MSTG Mobile Security Testing Guide OWASP Version 1.2 July 25, 2021

[54] **Bernhard Mueller, Sven Schleier** Mobile Appsec Verification Standard OWASP Pre-release 0.9

[55] **Antonio Ramos Varón Carlos A. Barbero Muñoz**
Hacking práctico de redes wifi y radiofrecuencia
Editorial Ra-Ma 2014

8. Anexos