UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

Análisis y parametrización de la seguridad en sistemas IoT

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Perera Bartual, Óscar

Tutor: Bonastre Pina, Alberto Miguel

Curso 2017-2018

Resumen

Este proyecto está centrado en los aspectos de seguridad relacionados con los sistemas orientados hacia Internet de las Cosas, y los problemas relacionados que pueden surgir. Desde el análisis de las amenazas que pueden presentarse en estos sistemas, se proponen una serie de buenas prácticas que permiten aumentar el nivel de seguridad de estos ecosistemas. En este proyecto, además, se desarrolla una nueva metodología de análisis que permite auditar un entorno IoT y evaluar su nivel de seguridad, identificando los puntos débiles y fuertes del sistema desde este punto de vista.

Palabras clave: seguridad, internet de las cosas, proteger, amenaza, ataque.

Summary

This thesis is focused on the security aspects related to the systems oriented to the Internet of the Things, and the added problems that can appear. From the threat analysis that can occur in these systems, a series of good practices that allow to increase the security level of these ecosystems are proposed. Furthermore, in this thesis, a new analytic methodology that allows to audit a IoT environment and evaluate its safety level is developed, identifying its weaknesses and strengths of the system from this perspective.

Key words: security, internet of things, protect, threat, attack.

Índice

Estructura

El presente documento está dividido en siete capítulos, más bibliografía y anexo I. El primero de ellos, la introducción, permite conocer qué es el Internet de las Cosas y sus usos. En este mismo apartado encontramos una introducción a los sistemas embebidos, habitualmente empleados en las redes IoT y finalmente, hablamos del estado actual de la seguridad en este ámbito.

En el segundo capítulo presentamos y describimos las amenazas que pueden afectar a estos dispositivos, clasificándolas según su naturaleza.

En el tercer capítulo presentamos, estructuradas en tres grupos distintos, las buenas prácticas necesarias o simplemente recomendables para poder considerar que sistema es seguro.

Con el fin de evaluar el grado de seguridad de los diferentes sistemas y dispositivos, en el capítulo cuatro definimos un parámetro que permitirá medir el nivel de seguridad. Además, describimos una nueva metodología diseñada para evaluar el sistema paso a paso. En el quinto capítulo se establecen los niveles de seguridad en base a este parámetro, con el fin de catalogar el nivel de seguridad del sistema evaluado.

El capítulo seis muestra un ejemplo de uso de dicha metodología sobre un caso real, analizándolo paso a paso.

Por último, se incluyen las conclusiones obtenidas tras este trabajo, las referencias utilizadas como fuente de información y los anexos.

1 Introducción

Desde hace mucho tiempo Internet está presente en nuestras vidas como medio de comunicación y fuente de información, llegando a ser en muchos casos incluso una herramienta imprescindible de trabajo. La evolución de Internet, desde el invento revolucionario que fue inicialmente, hacia los nuevos entornos de comunicación, como son *Internet of Things* (IoT), el mundo *smart* (*smart cities*, *smart farming*, *smart grid*, etc) y la nueva Revolución Industrial 4.0, entre otros, introduce nuevos desafíos cada vez más complejos. Cada vez es mayor el número de dispositivos de uso cotidiano que disponen de conexión a Internet. Esta mayor dependencia de Internet lleva a uno de los principales retos de esta nueva tecnología: la seguridad. La utilización de las nuevas tecnologías conectadas conlleva una cesión importante de información en múltiples planos – personal, profesional, de salud, etc. – que preocupan a los usuarios. Para ilustrar este aspecto basta con hacer hincapié en la cantidad de información que depositamos en dispositivos como nuestros teléfonos móviles, con el riesgo de pérdida o sustracción de los mismos. Resulta muy elevado el peligro físico, económico y/o tecnológico que puede conllevar, especialmente si caen en manos incorrectas, para las entidades involucradas. Según el informe de Julio de 2014 de HP FORTIFY3 [6], el 80% de los dispositivos tienen fallos en la autenticación y 6 de cada 10 dispositivos con interfaz de usuario son vulnerables.

1.1 Justificación y objetivos

Las perspectivas futuras del mundo de Internet de las Cosas (IoT), y las graves amenazas que de un mal uso de estas tecnologías pueden derivarse, justifica prestar especial atención a los aspectos de seguridad en este ámbito.

Por ello, en este trabajo analizamos desde un punto de vista de la seguridad las tecnologías relacionadas con el ecosistema de Internet de las Cosas, introduciendo los conceptos clásicos de seguridad en este nuevo entorno, analizando las amenazas y sistematizando este estudio para proporcionar una herramienta útil para la verificación de estos aspectos de forma sencilla.

Con este propósito en mente, los objetivos del presente proyecto son:

Objetivo General: Incrementar la seguridad en los sistemas IoT

Para ello proponemos en este trabajo una serie de pasos que permiten analizar, evaluar, corregir y proponer medidas y buenas prácticas concretas para abordar el estudio y mejora de la seguridad de los sistemas basados en tecnologías IoT

Objetivo concreto 1: Analizar amenazas

El primer paso de este objetivo consiste en sistematizar el conjunto de amenazas a la seguridad que pueden presentarse en un sistema basado en IoT, atendiendo a los diferentes escenarios tanto en cuanto a la aplicación, como a la heterogénea variedad de dispositivos y módulos de aplicación que pueden formar parte de un ecosistema IoT

Para ello consideraremos las recomendaciones de organismos internacionales vinculados con este entorno, así como de las empresas proveedoras de servicios y/o dispositivos, además de aquellas centradas en la seguridad en general.

Objetivo concreto 2: Recomendaciones básicas de seguridad y técnicas

Partiendo del objetivo anterior, este objetivo trata de proponer una serie de recomendaciones y mejoras que pueden ser incorporadas en todos los sistemas basados en IoT para mejorar su seguridad, abarcando desde mejoras en las políticas de la entidad, así como en mejoras técnicas que ayuden, mediante mecanismos de seguridad, a aumentarla. Por último, también incluimos recomendaciones organizativas de modo que la entidad disponga de planes de actuación/prevención frente a cualquier posible amenaza.

Objetivo concreto 3: Proporcionar una herramienta de análisis de seguridad en IoT

Para comprobar que el sistema dispone de un alto nivel de seguridad y que, por tanto, incorpora todas las recomendaciones propuestas en el objetivo anterior, definimos con este objetivo una nueva metodología que permite auditar/analizar la seguridad del sistema para definir posteriormente en qué nivel se encuentra.

Objetivo concreto 4: Ilustrar esta metodología mediante un ejemplo concreto.

El último objetivo de este trabajo es ejemplificar, a partir de un caso tan real como sea posible, cómo debemos aplicar dicho método y los resultados que nos proporciona a medida que es desarrollado. De este modo conseguimos aclarar posibles dudas que de manera teórica hayan podido surgir.

1.2 Internet de las Cosas

El término *Internet of Things* (Internet de las Cosas o IoT) fue introducido por el tecnólogo Kevin Ashton el año 1999 [16]. Si bien existen múltiples definiciones del mismo, habitualmente se define como un nuevo paradigma de comunicación que prevé un futuro cercano, en el que los objetos de la vida cotidiana estarán equipados con microcontroladores, serán capaces de comunicarse digitalmente, mediante el uso de protocolos adecuados, tanto con los usuarios como con otros objetos, convirtiéndose en una parte integral de Internet [7].

El concepto de IoT, por lo tanto, tiene como objetivo expandir Internet más allá de los dispositivos habituales, incorporando al mismo entorno conectado un conjunto de objetos inteligentes. Por otro lado, el acceso universal estos objetos, implementados mediante una amplia variedad de dispositivos (electrodomésticos, cámaras de vigilancia, redes de sensores, pantallas de información pública, vehículos, etc.) permite obtener una enorme cantidad y variedad de datos relacionados con los usos de estos objetos, habilitando el desarrollo de nuevas aplicaciones que, basándose en esta información, proporcionan nuevos servicios a ciudadanos, empresas y administraciones públicas. Este concepto se ilustra en la Figura 1.

Figura 1: Ecosistema de Internet of Things

La aplicación de estos novedosos conceptos a la industria ha dado como resultado la denominada Revolución Industrial 4.0. Su objetivo es la automatización completa de las operaciones de fabricación y manufactura. Esta denominación parte del informe *Preservación del futuro de Alemania como centro de producción* [17] que, ya en 2013, buscaba el objetivo de alcanzar una automatización total de los medios de producción, permitiendo una total independencia de la mano de obra humana. Este proceso es posible gracias a los denominados *sistemas ciberfísicos* [16], que combinan maquinaria física con procesos digitales, son capaces de tomar sus propias decisiones de una manera descentralizada y de trabajar cooperando entre ellos. Evidentemente, una de las claves para el éxito de esta iniciativa es la integración eficiente de los diferentes sistemas gracias a tecnologías de interconexión abiertas, en la línea de IoT. El objetivo final es, por tanto, la implementación de "fábricas inteligentes", dotadas de redes inteligentes se controlarán a sí mismas a lo largo de toda la cadena de valor.

Otra de las aplicaciones de los ecosistemas basados en IoT es el campo de las Ciudades Inteligentes (*Smart Cities*). Puede definirse una ciudad inteligente como el lugar donde los ciudadanos disfrutan de una calidad de vida sostenible a través de la tecnología: economía y productividad, movilidad, medio ambiente, educación, salud y seguridad [9]. Existen cientos de aplicaciones en este ámbito de las *Smart cities.* Algunos ejemplos relacionados con movilidad pueden ser *Smart Parking* [9], que indica a los conductores donde hay lugares libres para aparcar sus vehículos, el *Smart Traffic* [9] que realiza un estudio del tráfico de la ciudad y propone rutas alternativas a los conductores. Existen otras muchas iniciativas en otros campos, como la energía (Smart Lighting, o gestión eficiente del alumbrado público), gestión de residuos y sostenibilidad, participación ciudadana, etc.

Siguiendo con las aplicaciones de la IoT llegamos a la denominada Inteligencia Ambiental (AmI) [18] El algoritmo analiza el entorno en el que está y procesa la información obtenida, dando lugar a posibles cambios en él. Las tecnologías que podemos destacar en este campo es por ejemplo la RFID que puede ser utilizada para monitorizar a las personas y sus movimientos. Otra de las tecnologías empleadas en este ámbito es el I-Button que son pequeños chips que pueden

incorporarse a las personas u objetos e identificarlos. Uno de los ejemplos que podemos encontrar son las Casas Inteligentes (*Smart Home*). Muchas empresas apuestan por el desarrollo de proyectos en este ámbito, donde destaca la tecnología Zigbee. Las aplicaciones más destacadas son la regulación de la temperatura de las casas, la gestión de la iluminación y ventanas de las casas, así como el control de los frigoríficos. Otro de los ámbitos donde se aplica la AmI es la Asistencia y monitorización de la salud. Grandes investigaciones se centran en este campo para otorgar a los usuarios con discapacidades y otros problemas de salud dispositivos que mejoren su calidad de vida. Este ámbito permite que personas con enfermedades mentales o de movilidad puedan tener mayor libertad viviendo en su hogar y teniendo una vida con menor dependencia a los profesionales de la salud. Otra tecnología emergente en este ámbito es la ayuda a personas con déficits cognitivos y físicos para recordarles, por ejemplo, tareas que deben o como llevarlas a cabo.
Los hospitales son otro de los campos de AmI donde podemos ver su aplicación desde la seguridad de los pacientes, hasta permitir a los profesionales llevar un correcto seguimiento de estos más cómodamente.

Los *Wearables*, o dispositivos [9] que el usuario lleva consigo, son otra de las aplicaciones de la IoT que abarca desde relojes inteligentes, que controlan tanto pulsaciones cardíacas como pasos que realiza el usuario, hasta pulseras de actividad que controlan, por ejemplo, la cantidad de calorías consumidas. Este es otro de las áreas donde se prevé un mayor crecimiento económico en los próximos años. Cada vez más empresas se dedican al diseño, desarrollo y comercialización de estos dispositivos.

1.3 Los Sistemas Embebidos

Un sistema embebido, o empotrado, son dispositivos electrónicos, generalmente programables, de propósito específico, donde cobran importancia factores distintos de las prestaciones, como son el tamaño, el consumo, la fiabilidad, etc. Estos dispositivos serán la base de la integración de los objetos, ahora inteligentes, en la IoT.

Estos sistemas disponen de dos características principales:

- **Autonomía**: El sistema debe ser capaz de funcionar sin interrupción por sí solo, de forma desatendida, proporcionando robustez y fiabilidad.
- **Adaptabilidad**: El sistema debe adaptarse a las variaciones del entorno, para seguir proporcionando una supervisión y control adecuados al proceso o, en caso de no ser posible, llevar a éste a un estado de fallo seguro.

Por su naturaleza, los sistemas embebidos no han llevado los aspectos de seguridad más allá de los requisitos de la aplicación, generalmente centrados en la tolerancia a errores. Sin embargo, en un nuevo entorno de dispositivos conectados en red aparecen múltiples riesgos que en su día no se consideraron. Según CERTSI [14], algunas de las debilidades típicas de los sistemas embebidos son:

- **Compartición de secretos**: Muchas son las aplicaciones de estos sistemas que suelen compartir información sensible (contraseñas, por ejemplo) para mejorar la interacción entre ellas con una baja protección. Esta compartición permite a un atacante poder acceder a diversas aplicaciones.
- **Certificados privados:** En los sistemas embebidos es común utilizar certificados autofirmados, es decir, no disponen de ninguna entidad que respalde la veracidad de los mismos. Este hecho puede ser aprovechado por los atacantes para falsificarlos y utilizarlos con el fin de obtener permisos en los dispositivos.
- **Contraseñas embebidas y puertas traseras**: Las contraseñas embebidas están definidas por el fabricante del dispositivo e impide a los

usuarios cambiarlas. Las puertas traseras permiten a los fabricantes el acceso a los dispositivos embebidos sin importar los cambios realizados por parte del cliente. Todo esto puede ser usado por un atacante permitiéndole el control total del dispositivo.

- **Fallos de código libre**: Muchas partes de código de los sistemas embebidos se basan en procedimientos reutilizados e incluso código libre. Este código no suele revisarse y puede provocar fallos. Estos fallos pueden ser aprovechados por los atacantes como puntos de entrada.
- **Criptografía débil o inexistente**: Los métodos de cifrado utilizados suelen ser pocos. Esta limitación permitiría a un atacante capturar e interpretar el tráfico existente entre dos dispositivos.
- **Autenticación débil o inexistente**: La autenticación de los dispositivos suele ser un código PIN o incluso algunos no disponen de ningún control de accesos. Un atacante podría utilizar fuerza bruta para acceder a los dispositivos o su contenido.
- **DoS y DDoS**: Estos dispositivos no suelen disponer de un control de tramas, de manera que una petición reiterada de información puede llegar a saturar los canales saturándola.

1.4 Seguridad de los sistemas informáticos

1.4.1.1 Definiciones

Garantizar el correcto funcionamiento de un ecosistema IoT no es tarea sencilla. Existen múltiples factores que pueden afectar este funcionamiento, y cada uno de ellos puede hacerlo en varios aspectos. En este apartado comenzamos definiendo claramente cada uno de ellos para evitar cualquier duda y posible ambigüedad en su significado. Tres son los aspectos principales a considerar en nuestro análisis. Estos son:

- **Seguridad**

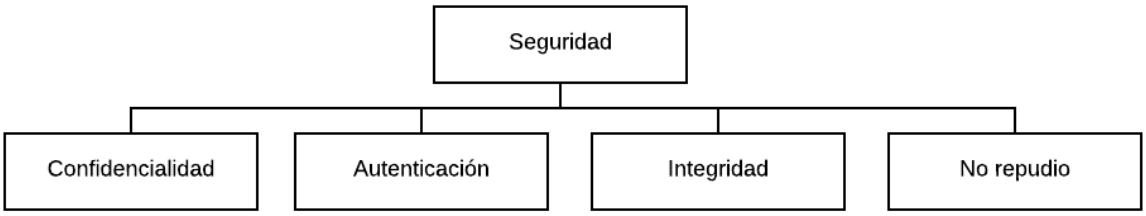
Empezamos definiendo la seguridad informática [19] como un proceso de medidas y acciones para prevenir y, en su defecto, detectar el uso de los recursos de un sistema sin autorización. Este campo de la informática trata de proteger un sistema de agentes externos y/o internos que intenten de manera intencionada o no, hacer uso de él o de sus datos con fines maliciosos.

La seguridad lógica es aquella que trata de proteger el software de los equipos informáticos, es decir, las aplicaciones y los datos de usuario, de robos, de pérdida de datos, entrada de virus informáticos, modificaciones no autorizadas de los datos, ataques desde la red, etc. La seguridad puede ser de dos tipos, activa y pasiva.

- Podemos definir la **seguridad activa** como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos.

- La **seguridad pasiva** complementa a la anterior y se dedica a reducir los efectos causados por aquellos percances que no se ha conseguido atajar mediante la seguridad activa.

El término de **seguridad** abarca cuatro aspectos importantes que deben cumplirse para poder definir un sistema como seguro. Estas cuatro dimensiones se resumen en el siguiente esquema:



Cada uno de ellos aporta un valor necesario para definir la seguridad y, por tanto, necesitamos conocer en profundidad qué significan exactamente cada uno de estos términos. Definimos cada uno de estos términos como:

+ **Confidencialidad**: La confidencialidad consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que, solo aquellos que tengan el acceso permitido podrán hacer uso de esta información. Por lo general, se basa en la utilización de técnicas de criptografía (cifrado) que permiten la interpretación de los datos solo tras la correspondiente autenticación.

+ **Autenticación y autorización:** La **autenticación** es el servicio que trata de asegurar que los agentes que intervienen sobre la información son realmente quienes afirman. Por otro lado, la **autorización** evalúa si el usuario autenticado tiene privilegios suficientes como para realizar las operaciones que requiere. Para la identificación de los agentes que tratan de acceder a la información sensible pueden emplearse diversas formas como, por ejemplo, usando huellas dactilares, contraseñas personales y tarjetas inteligentes entre otras.

+ **Integridad**: Es conocida como la capacidad de garantizar que los datos no han sido modificados desde el momento que fueron creados. Junto a la autenticación, permite garantizar que la información de que disponemos es válida y consistente, puesto que se garantiza que los datos no han sido modificados. Suele implementarse añadiendo un campo que incluya una función hash sobre los datos que enviamos para que el receptor pueda descifrarlos y comprobar que son correctos los que ha recibido al compararlos con los de este campo, es decir, verificar el origen de los datos y cuándo fueron enviados, así como certificar que en recepción los datos no han sido alterados

+ **No repudio**: Esta característica tiene como finalidad garantizar que el emisor de un mensaje – o el origen de una información – no pueda declarar que no ha

sido él dicho autor de ese mensaje. Es habitual que esta característica se implemente mediante firmas digitales, generadas en base a una clave privada, que garantizan la identidad del remitente de la información.

Fiabilidad

La fiabilidad se define como la probabilidad de que un bien funcione adecuadamente durante un período determinado bajo condiciones operativas específicas. Es una medida de la confianza de que los dispositivos de un sistema vayan a funcionar correctamente durante su uso.

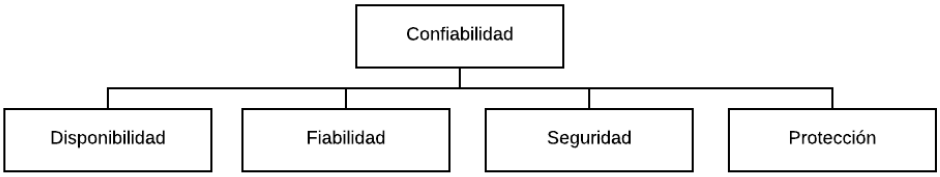
Este aspecto resulta fundamental en la mayoría de los sistemas puesto que los usuarios son remisos a utilizar dispositivos en los que no confía.

La fiabilidad de un sistema se incrementar teniendo en cuenta los siguientes aspectos:

- El sistema debe tener un diseño claro que satisfaga los requisitos del usuario
- El sistema debe diseñarse de forma segura y considerando sus posibles fallos
- El diseño debe facilitar las pruebas e incluir planes de verificación
- El diseño y desarrollo deben seguir estándares de calidad definidos
- Deben realizarse pruebas de funcionamiento durante el desarrollo
- Debe contemplarse el mantenimiento del sistema dentro del ciclo de vida, comenzando en el instante en el que el sistema se active
- Los sistemas debieran estar provistos de mecanismos integrados de tolerancia a fallos
- El sistema debe diseñarse y crearse siguiendo estándares definidos.

Confiabilidad

Podemos definir la **confiabilidad** como la capacidad de un producto de realizar su función de la manera prevista. Por otro lado, la confiabilidad se puede definir también como la probabilidad de que un producto realice su función prevista sin incidentes durante un período de tiempo especificado y bajo las condiciones indicadas. Existen cuatro dimensiones principales de la confiabilidad:



Como podemos apreciar, este término engloba a los dos mencionados anteriormente, es decir, para que un sistema sea confiable, es necesario, aunque no suficiente, que proporcione fiabilidad y seguridad. Adicionalmente, la disponibilidad y la protección de un sistema también son características fundamentales para definir un dispositivo como confiable.

+ **Disponibilidad**: Se define como la capacidad que tiene un sistema de prestar un servicio durante el tiempo para el cual ha sido diseñado.

+ **Protección:** Se define como la capacidad de un sistema para resistir las influencias del entorno.

1.4.1.2 Elementos de un sistema informático

La aplicación de los conceptos anteriores a los sistemas informáticos debe considerar los distintos componentes que pueden ser vulnerados en un sistema (posibles entradas para realizar un ataque) y cómo están relacionados entre ellos:

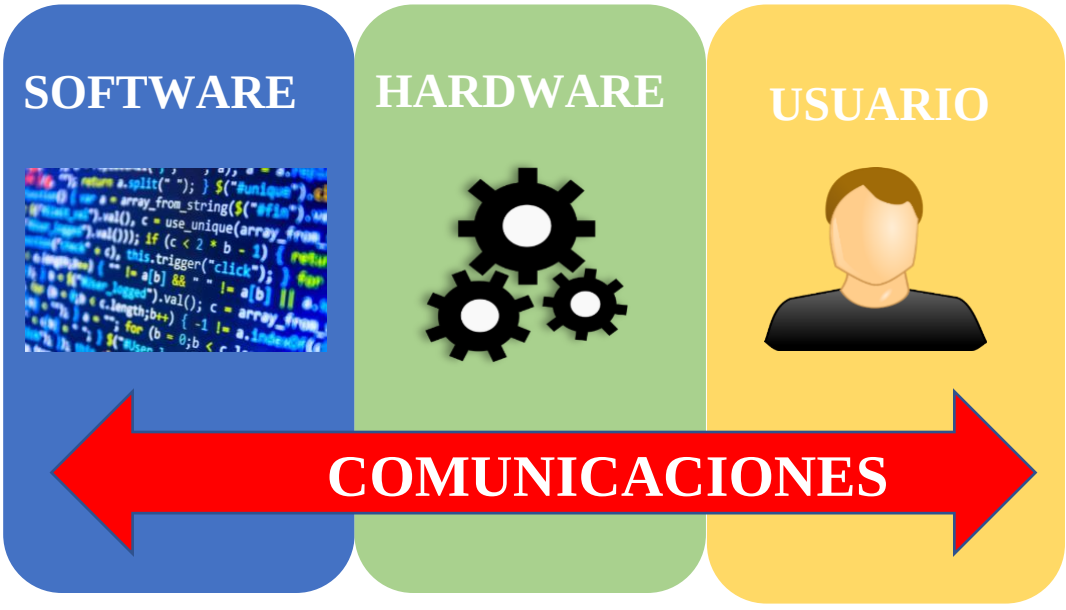


Figura 2: Elementos de un sistema informático

La Figura 2 ilustra los distintos componentes que tradicionalmente forman parte de un sistema informático: Hardware, Software y usuarios.

Para garantizar la seguridad del sistema, es imprescindible que analicemos las vulnerabilidades de cada una de ellas y contemplar las medidas de seguridad necesarias para minimizar las posibilidades de sufrir un ataque.

El software es uno de los principales vectores de entrada a un sistema, en ocasiones aprovechando debilidades de programas o malas configuraciones del sistema, así como fallos en el sistema operativo. Sin embargo, resulta más frecuente que la causa de una vulnerabilidad resida en un fallo técnico de programación, que, en ausencia de una comprobación completa, permite que se den circunstancias indeseadas en el código durante su ejecución.

Por otro lado, el **hardware** es el último recurso por el que se intenta atacar a un sistema, pero también presenta sus puntos débiles. Especialmente, son cuatro los componentes más utilizados como vía de acceso.

1. **Discos Duros**

La mayoría de los ataques realizados a este tipo de dispositivos suelen ser con propósitos destructivos para dejar el disco dañado sin posibilidad alguna de reparación: el firmware del controlador infectado con un código malicioso oculta los sectores que contienen malware y bloquea cualquier intento de fijar el firmware. Es por ello que cualquier intento de erradicar este malware es en vano. La mejor forma de eliminarlo es destruyendo el disco físico. Si bien es cierto, este tipo de ataques suelen ser bastante costosos con lo que es difícil verse afectado por un malware cuya fuente de entrada sea el disco duro.

2. **Interfaz USB**

Otro de los componentes que pueden verse afectados a nivel de hardware son los puertos USB. A pesar de que infectarse a través de esto es un tanto difícil

debido a que es necesario introducir un USB en nuestro dispositivo, sigue siendo una vulnerabilidad notoria. Actualmente, con la unificación de los puertos USB en ciertos dispositivos, haciendo que estos reciban su carga por aquí, este riesgo se ve incrementado puesto que la solución más eficaz era dejar de usar estos puertos y con esta novedad, ya no será posible. A pesar de ser un reto actualmente imposible infectar un ordenador a través de los cargadores ya que estos no poseen memoria, realizando una mejora (o cambio) sobre estos, podría llegar a ser posible.

3. Firmware

El último componente hardware que puede ser vulnerado es el firmware, donde se establece la lógica entre el software y el hardware. Actualmente, se han encontrado vulnerabilidades en sistemas como Intel donde a través de un bug en el firmware, permitía cargar y ejecutar código sin que el usuario pudiese verlo dando como resultado fallos en el sistema.

Algunos de los ejemplos más recientes dónde se ha visto vulnerado un sistema a través del hardware son:

- *Bit-flipping*, o alteración de bits de memoria, con el propósito de causar errores en el sistema que habitualmente conducen a modos degradados con menores medidas de seguridad. En este caso, el componente afectado es la memoria RAM.

- Otra amenaza presentada a nivel de hardware y considerado uno de los más efectivos es el conocido *rowhammer* [20], que consiste en “martillear” un bit constantemente con un valor para cambiar el actual valor en el que se encuentre dicho bit. Esta amenaza afecta a la DRAM.

Por último, hablaremos de los **usuarios**, que suelen ser el vector de entrada más vulnerable.

Para ello, los atacantes utilizan técnicas de ingeniería social, donde hacen creer a los usuarios que la información que reciben es totalmente correcta y fiable. Así pues, los ataques de ingeniería social [21] se basan en una manipulación psicológica a los usuarios para que estos proporcionen información o acceso a

un sistema sin que sean conscientes de ello. Los principales canales de intrusión usados son:

1. Envío de correo electrónico, utilizando la técnica conocida como *phishing*, suplantando la identidad de una entidad o persona.
2. Extorsión de los usuarios a través de las redes sociales.
3. A través de llamadas telefónicas suplantando la identidad de una persona o entidad.
4. A través de dispositivos de memoria externa, infectadas con malware y depositados cerca del sistema que se desee vulnerar confiando que alguno de los usuarios más cercanos lo inserte.
5. Por mensaje de texto, al igual que los correos electrónicos o las llamadas telefónicas, donde se suplanta una identidad para engañar al usuario.

Por ejemplo, en los últimos años [22] se han podido observar diferentes noticias donde grandes organizaciones se han visto afectadas por vulnerabilidades cuya estrategia ha sido mediante un ataque de ingeniería social hacia los trabajadores de dicho organismo. La falta de concienciación por parte de los trabajadores es uno de los factores más influyentes y más aprovechados por parte de los hackers para atacar un sistema.

Como conclusión, podemos citar a Thomas Reid [23] que escribió en una de sus obras, ensayos sobre los poderes activos de la mente humana, *"Una cadena es tan fuerte como su eslabón más débil".* En este caso, el eslabón más débil podríamos decir que, a día de hoy, son los usuarios, por lo que se debe hacer especial hincapié en que estos conozcan cómo protegerse y evitar ser una fuente fácil de ataque.

Tras esta breve introducción a la seguridad en general, podemos ahora hablar sobre la seguridad en *Internet de las cosas*.

1.5 Introducción a la seguridad IoT

Uno de los mayores retos de la IoT es la seguridad. En IoT se almacena información muy sensible, además de que permite manejar muchos componentes y cualquier ataque donde se manipulen estos elementos o el robo de información puede poner en riesgo desde nuestra información personal hasta la integridad física de las personas. Por ello, la seguridad en IoT es un aspecto fundamental, donde debe ser prácticamente imposible romper los sistemas evitando accesos a la red sin consentimiento.

Como hemos citado anteriormente, los dispositivos IoT son dispositivos empotrados en general porque están diseñados con un objetivo específico. Este hecho nos lleva a tener una red heterogénea donde cada dispositivo es de un fabricante, con unas características y un software particulares.

En un sistema tan heterogéneo donde los dispositivos son empotrados apreciamos que el número de conexiones que se van a realizar es elevado y la información va a estar constantemente viajando de un dispositivo a otro. Si todas estas conexiones no disponen de una buena seguridad en la autenticación, en la integridad y en la confidencialidad de los datos puede llevar a que un atacante aproveche esto e intercepte la información, pudiendo incluso modificarla. En este tipo de redes, muchos de los datos son de carácter privado o personal por lo que estos aspectos deben quedar siempre cubiertos y asegurados en los dispositivos. Además de ello, consideramos importante también la propiedad de no repudio, para que así, con tanto intercambio de dispositivos, podamos saber siempre de donde provienen y poder saber quién los ha alterado en caso de ser necesario.

La siguiente propiedad citada, la fiabilidad, también es considerada como crítica, pues en muchos de estos entornos, junto a la disponibilidad, es primordial por las funciones que desempeñan y que alguno de ellos deje de funcionar en un instante determinado o deje de funcionar para siempre supone un riesgo alto. Por ejemplo, contextualizamos esto sobre una red de dispositivos IoT en un ámbito de la salud, es importante que un dispositivo que incorpora un sensor para saber cuándo un paciente entra en parada cardíaca esté siempre en funcionamiento puesto que, en caso de fallo, puede comprometer la salud del paciente.

Por último, pero también muy importante, debemos tener en cuenta que estos dispositivos al ser sistemas empotrados, son accesibles fácilmente por lo que la protección de ellos es muy importante.

A nivel de software, como ya hemos comentado, los dispositivos provienen de muchos fabricantes diferentes por lo que cada uno integra un software diferente. Podemos apreciar que este hecho supone que, a una mayor cantidad de software diferente, mayor probabilidad de que contengan vulnerabilidades en él. También detectamos a nivel de software que dichas aplicaciones hacen uso de los servicios en la nube y dichas plataformas tienen deficiencias en la gestión o actualización lo que puede suponer un vector de entrada de larga duración.

A nivel de hardware destacamos que también aparecen deficiencias, aunque suelen ser menos explotadas. Este tipo de ataques suelen darse cuando la parte software es muy segura y no da lugar a ser explotada. Es por ello, que suelen situar a los dispositivos al menor alcance posible de las personas para evitar que puedan ser manipulados.

Los usuarios de estas redes no podemos saber con certeza quienes van a ser ni sus intenciones, por lo que debemos hacer hincapié en ello e intentar otorgar la menor autoridad posible mientras no sean conocidos.

Existen diversas técnicas para aumentar la seguridad en los componentes de IoT tanto a nivel de software como de hardware. Esta seguridad suele combinarse con unos consejos que aumentan la privacidad de los datos y la combinación de ambas cosas nos permitirá aumentar la seguridad global de nuestros dispositivos y, por tanto, de nuestra red.

En primer lugar, conoceremos algunos de los requisitos que la *ALLIANCE FOR INTERNET OF THINGS INNOVATION* destaca como importantes. Estos son:

- Entendimiento común: Se trata de entender para qué se utilizará cada componente fabricado, es decir, su finalidad. En este punto se trata de promover los objetivos de la protección de datos como limitar el alcance de los datos, segmentarlos, aislamiento, control de datos y acceso.
- No utilizar datos personales por defecto y anonimización por defecto: Debemos evitar utilizar datos personales que vengan configurados por defecto. Es conveniente diseñar capacidades de anonimización para que los datos personales se dejen de estar identificados lo más pronto posible.

Actualmente, los expertos han estimado que los ataques más comunes que violarían la seguridad de los dispositivos pertenecientes a esta red serían:

- Ataques de denegación de servicio como consecuencia de la cantidad de dispositivos conectados simultáneamente.
- Ataques de malware. Gracias a la gran cantidad de dispositivos interconectados, sería muy fácil expandir un malware de un dispositivo a otro.
- Violaciones de datos. El control y espionaje de las comunicaciones y de la información es otro de los ataques más frecuentes que se presentan en estos sistemas.
- Suplantación de dispositivos. La gran cantidad de dispositivos conectados entre sí facilita la posibilidad de que alguno de ellos se fácilmente "sustituido" por otro sin que el entorno sea consciente de ello.

Una vez conocido el estado actual de la seguridad en el Internet de las Cosas y su problemática actual, definiremos a continuación las amenazas y vulnerabilidades que pueden presentarse en un sistema o dispositivo IoT.

2 Amenazas y Vulnerabilidades

Empezaremos este capítulo con la definición de los conceptos de amenaza y vulnerabilidad necesarios para entender los siguientes apartados. Así pues, los definimos [24] del siguiente modo:

- **Vulnerabilidad**: Una vulnerabilidad en un sistema informático es una debilidad presente en el sistema que pone en riesgo la seguridad de este permitiendo que un atacante aproveche la vulnerabilidad para adentrarse en él.

- **Amenaza**: Por su parte, una amenaza es cualquier intención de aprovechar una vulnerabilidad para adentrarse en el sistema o para afectar a este de manera maliciosa.

2.1 Taxonomía de las amenazas

En este apartado describimos una serie de amenazas, que hacen posible que se lleven a cabo estos ataques.
En este caso, situaremos cada amenaza o vulnerabilidad dentro de un grupo en función de la finalidad para la cual se utiliza cada una de ellas.

- **Grupo 1. Abusos/Ataques negativos**

  En este grupo encontramos aquellas amenazas/vulnerabilidades que pretenden adentrarse en el sistema para controlarlo. Entre ellas encontramos:

- Malware: Cualquier tipo de software malicioso que está diseñado para ejecutar acciones no deseadas sobre un sistema sin autorización.
- *Exploit*: Se trata de un código utilizado para aprovechar alguna de las vulnerabilidades encontradas en un sistema. Suele utilizarse como fuente de introducción de los malware.
- Ataques dirigidos: Ataques diseñados para un objetivo concreto que se lanza durante un periodo de tiempo prolongado para poder penetrar lo más profundo posible en un sistema. El atacante tiene claro el objetivo al que

pretende dirigirse y cuál es la recompensa que quiere obtener. Los ataques suelen ser más sofisticados pues el atacante realiza un estudio del sistema para mejorar la técnica y conseguir su objetivo sin ser detectado.

- Ataque distribuido de denegación de servicio(DDoS): Se trata de un ataque desde varios sistemas a un servidor, con la intención de saturarlo para que no proporcione sus servicios.
- Suplantación de dispositivos: Son aquellos dispositivos que intentan imitar a los originales haciéndose pasar por ellos e incluyen en ellos puertas traseras que les permite generalmente realizar los ataques. Suelen ser difíciles de detectar pues es complicado diferenciar un dispositivo original de uno falso.
- Modificación de la información: El objetivo principal de estos ataques es modificar la información con fines lucrativos generalmente. Puede realizarse tanto con códigos maliciosos, como el malware, como por los propios usuarios con acceso a los sistemas.

- **Grupo 2. Interceptores/Secuestradores de comunicaciones**

Este grupo reúne aquellas amenazas amenazas/vulnerabilidades que se utilizan para recolectar información de los dispositivos mientras es transferida a través de redes inseguras. Este grupo comprende amenazas como:

- Ataque de intermediario: El atacante no afecta a ninguno de los dos sistemas directamente. Se sitúa en medio de la comunicación y analiza todo el tráfico intercambiado entre los extremos sin que estos sean conscientes de su presencia. El interceptor puede leer, modificar o insertar información a su voluntad.
- Secuestro del protocolo de comunicación: El atacante consigue controlar la comunicación entre dos extremos pudiendo acceder y obtener toda la información intercambiada por un protocolo de comunicación concreto. Es decir, toda la información que viaje a través de otro protocolo no es interceptada, cosa que no ocurre en el ataque de intermediario. Además, en este ataque la información no puede modificarse como en el ataque de intermediario.
- Intercepción de información: Interceptar los servicios de comunicación privados como llamadas de teléfono o correos electrónicos para obtener la

información a través de ellos. La información no puede ser modificada, solo leída (y/o escuchada) por el interceptor.

- Analizadores de red: Este ataque trata de analizar cómo está la red conectada para conocer mejor al sistema y sus conexiones. Este ataque permite mejorar las técnicas de otros ataques.
- Secuestro de sesión: Secuestro de datos actuando como el *host* legítimo con el fin de alterar la información. Es decir, es un robo de unas cookies de otro sistema con el fin de robar una sesión válida para obtener acceso sin ser autorizado a la información.
- Reproducción de mensajes: Trata de repetir los paquetes enviados reiteradamente para dejar el dispositivo objetivo inactivo. A diferencia del DDoS que va dirigido al servidor para dejarlo inoperativo, este ataque puede utilizarse en contra de cualquier dispositivo, saturándolo de paquetes de datos.

- **Grupo 3. Caídas**

Este grupo abarca todas las amenazas amenazas/vulnerabilidades que surgen tras dejar de funcionar alguna de las partes de la red IoT. Estas son:

- Caída de red: Desconexión de la red intencionada o inesperada.
- Fallo de dispositivos: Fallo en el hardware de los dispositivos.
- Fallo del sistema: Fallo en el software de las aplicaciones de los dispositivos.
- Pérdida de servicios de soporte: Pérdida de acceso a los servicios que posibilitan el funcionamiento de los dispositivos.

- **Grupo 4. Empleados maliciosos**

En este grupo encontramos aquellas amenazas/vulnerabilidades que surgen tras exponerse datos sensibles intencionadamente. Estas son:

- Filtrado de información privada: Descubrimiento de datos privados a otras fuentes sin autorización.

- **Grupo 5. Fallos**

En este grupo encontramos aquellas amenazas que surgen debido a fallos en alguno de los dispositivos de la red. Estas son:

- Vulnerabilidades software: Los dispositivos son vulnerables generalmente como consecuencia de fallos en la configuración, contraseñas débiles y fallos en la programación de su software. Dichas vulnerabilidades son las que aprovechan los *exploits*.
- Fallos de terceros: Cuando un dispositivo conectado a otro, falla y no está bien configurado, el otro dispositivo que sí funciona correctamente puede dejar de funcionar como consecuencia del fallo del primero, pudiendo dejarlo inoperativo o con alguna vulnerabilidad, por ejemplo.
-

- **Grupo 6. Desastres**

En este grupo se recogen las amenazas/vulnerabilidades relacionadas con desastres físicos que pueden afectar a los dispositivos de la red.

- Desastre natural: Todo aquel fenómeno natural como tormentas, avalanchas, etc. que puedan perjudicar físicamente a los dispositivos.
- Desastre ambiental: Desastre en el entorno físico, como derrumbamiento del edificio o explosión de algún componente, en el que se intenta operar con los dispositivos IoT.

- **Grupo 7. Ataques físicos**

En este grupo se hallan aquellas amenazas/vulnerabilidades relacionadas con la manipulación de los dispositivos y/o su destrucción.

- Modificación de dispositivos: Manipulación de los dispositivos como consecuencia de fallos en ellos.
- Destrucción de dispositivos: Ataques a los dispositivos como robo, destrucción, etc.

- **Grupo 8. Efectos inintencionados**

En este grupo encontramos aquellas amenazas/vulnerabilidades como consecuencia de una mala praxis involuntaria.

- Fuga de información: Debido a errores en la administración de los servidores o un mal almacenamiento de los datos.

- Error en el uso o la administración de los dispositivos: Daños causados por falta de profesionales expertos en el área.
- Información extraída de fuentes no fiables: El uso de información extraída de fuentes no conocidas.
- Diseño inadecuado o falta de adaptación: Un mal diseño o una mala adaptación en los dispositivos puede impedir la correcta interacción entre ellos

3 Medidas para aumentar la seguridad

A lo largo de este punto podemos encontrar diversas medidas, conocidas como buenas prácticas(GP), que sirven para contrarrestar las amenazas que hemos conocido en el punto anterior. Las clasificaremos en tres grupos: Buenas prácticas en relación a políticas y estándares, soluciones técnicas y medidas en organización y procesos.

Políticas y estándares

Recogemos en este punto aquellas medidas propuestas por [27] que tengan como finalidad establecer unas políticas de diseño y funcionamiento de los componentes de una red IoT.

- GP.P.1: Contemplar la seguridad de todo el sistema IoT desde un punto de vista coherente durante todo el diseño y desarrollo de sus aplicaciones (y de sus dispositivos) implementándola en cada capa desarrollada.
- GP.P.2: Habilitar todas aquellas opciones que aumenten la seguridad del sistema y mantener deshabilitadas mientras no sean necesarias aquellas que puedan poner en riesgo su seguridad.
- GP.P.3: Integrar la capacidad de añadir nuevas políticas de seguridad.
- GP.P.4: Diseñar el sistema de forma compartimentada en segmentos para poder bloquear un segmento en caso de ser atacado, evitando así que el efecto se expanda al resto del sistema.
- GP.P.5: Añadir elementos software en cada nexo de unión entre los distintos segmentos para asegurar que la información cuando pase de un segmento a otro sea segura y fiable.
- GP.P.6: Establecer un método de análisis para los componentes hardware y software para comprobar que funcionan correctamente y como se espera.
- GP.P.7: Revisar el software a medida que se está implementando para corregir los posibles fallos/errores que puedan surgir durante esta fase.
- GP.P.8: Comprobar el nivel de privacidad de una aplicación antes de lanzarla.
- GP.P.9: Analizar cómo puede verse afectada la actual privacidad al lanzar una nueva aplicación.

- GP.P.10: No compartir información de los clientes a menos que sea expresamente aceptado por parte de dicho cliente.
- GP.P.11: Verificar que las aplicaciones trabajen con el menor nivel de autoridad posible para desempeñar sus funcionalidades.
- GP.P.12: Firmar el código implementado para comprobar la veracidad de este.
- GP.P.13: Asegurar que el sistema cumple con todos los estándares establecidos en base a las leyes de seguridad y privacidad en los sistemas informáticos.
- GP.P.14: Instalar las actualizaciones software y firmware que surjan de los dispositivos tan pronto como sea posible, tras comprobar que están firmadas y verificadas.
- GP.P.15: Imposibilitar volver a versiones anteriores de software o firmware más inseguras
- GP.P.16: Establecer un control para la manipulación del *hardware*.
- GP.P.17: Forzar el cambio de las credenciales impuestas de fábrica en el momento que se accede a los dispositivos.
- GP.P.18: Analizar cualquier dispositivo externo a la red cuando se conecte a la misma.
- GP.P.19: Asegurar que todas las partes involucradas cumplen con el Reglamento General de Protección de Datos.
- GP.P.20: Asegurar que todo hardware utilizado procede de un proveedor certificado, que incorpore medidas de seguridad e integridad.
- GP.P.21: Implementar la autenticación de doble factor.

Organización y procesos

En este punto recogemos todos aquellos criterios organizativos de la seguridad que deben llevarse a cabo para una correcta gestión y mantenimiento de la red.

- GP.O.1: Desarrollar un plan para ser utilizado cuando los dispositivos empiecen a fallar y necesiten ser reparados o sustituidos por defecto.
- GP.O.2: Definir el alcance de la seguridad y su estimación respecto a la duración que tiene en los dispositivos.

- GP.O.3: Establecer un plan de solución frente a ataques, que refleje soluciones seguras y fiables.
- GP.O.4: Establecer un plan de análisis de vulnerabilidades, además de un plan de tolerancia a ataques.
- GP.O.5: Establecer un plan de divulgación de vulnerabilidades colaborando con otras entidades para difundir y ser conscientes de todas ellas rápidamente.
- GP.O.6: Definir estrategias a seguir por parte de los empleados que aumenten la privacidad y la seguridad del entorno IoT.
- GP.O.7: Establecer los permisos de acceso y modificación de cada usuario en función del rol que desempeñe.
- GP.O.8: Definir con aquellos agentes que procesen los datos obtenidos, acuerdos que contengan el alcance de los datos, derechos, obligaciones y límites a cumplir por parte del cliente para definir el uso que pueden hacer de ellos y dar a conocer las restricciones impuestas por parte de la organización sobre los datos procesados.
- GP.O.9: Establecer criterios de responsabilidad dónde se identifique la persona responsable en caso de surgir algún problema en el sistema.
- GP.O.10: Establecer un plan de prevención frente a ataques físicos que incluya pautas de actuación frente a cada uno de ellos.

Técnicas

En este punto agrupamos las medidas referidas a los aspectos técnicos para la protección de la información de la red, es decir, aquellas que, en su mayoría, requieren la implementación de herramientas para cumplirse.

- GP.T.1: Evitar fallos de seguridad al añadir técnicas de ahorro de energía.
- GP.T.2: Establecer criterios de control y gestión de la red y los sistemas.
- GP.T.3: Controlar la ejecución de códigos que no estén firmados por desarrolladores conocidos.
- GP.T.4: Implementar la capacidad de volver a un estado seguro frente a la detección de que estamos en un estado inseguro/vulnerable.
- GP.T.5: Implementar mecanismos de monitorización para observar el comportamiento del dispositivo.

- GP.T.6: Asegurar que los datos personales sean utilizados exclusivamente para el objetivo específico para el cual fueron solicitados.
- GP.T.7: Implementar mecanismos que permitan al sistema hacer un autodiagnóstico que permita la recuperación ante fallos.
- GP.T.8: Incorporar mecanismos seguros para las actualizaciones.
- GP.T.9: Imposibilitar la modificación de los ajustes, tanto de seguridad como de privacidad, así como los ajustes personales de los usuarios, sin consentimiento.
- GP.T.10: Incorporar una política que obligue al cifrado de los datos cuando no estén siendo utilizados.
- GP.T.11: Registrar todos los movimientos del usuario desde que accede al sistema hasta que sale y almacenarlos.
- GP.T.12: Encriptar la sesión del usuario en las aplicaciones web desde el dispositivo al servidor.
- GP.T.13: Implementar mecanismos de aislamiento de la información sensible y datos personales de las partes de firmware y software que no necesiten acceso a ellos.
- GP.T.14: Implementar mecanismos para detectar y controlar la manipulación de los datos.
- GP.T.15: Utilizar protocolos que permitan el aislamiento de los dispositivos que se vean amenazados por un atacante, evitando que el ataque se expanda al resto.
- GP.T.16: Limitar la cantidad de paquetes recibidos para evitar un colapso del canal de comunicación.
- GP.T.17: Asegurar que el canal de transmisión de los datos protege la información y que se trata de una conexión segura.
- GP.T.18: Incluir mecanismos que protejan las credenciales de ser expuestas al exterior.
- GP.T.19: Incorporar mecanismos de validación de los datos antes de permitir que sean incluidos y/o ejecutados sobre el sistema.
- GP.T.20: Incorporar técnicas para la identificación y evaluación de riesgos y amenazas.

4 Análisis de seguridad: metodología

En este apartado mostramos una metodología para analizar la seguridad de un sistema, basada en un parámetro de seguridad, denominado Índice de Seguridad (IS). Posteriormente, se estable un conjunto de rangos de valores de IS nos permite clasificar el sistema bajo estudio en un nivel de seguridad.

4.1 Parámetro de seguridad

Para la aplicación de la metodología propuesta, definimos el índice de seguridad, IS, como una suma ponderada de los pesos asignados a cada una de las diferentes medidas de seguridad contempladas. El valor de este parámetro define el nivel (bajo, medio, alto...) de seguridad del sistema analizado, siendo mejor cuanto mayor es el valor de este parámetro.

En los sistemas de evaluación que presentamos más adelante, otorgamos un valor al IS para cada medida de protección e integración que cumpla el dispositivo y finalmente la suma de todos los valores obtenidos será el IS total del sistema.

El valor del IS varía en función de la importancia de cada característica y en función de lo prioritaria que se considera.

A continuación, procedemos a explicar la metodología de análisis, sus requisitos y la puntuación de cada buena práctica cuyo valor será sumado al total de su grupo y finalmente el valor de cada grupo será sumado al IS total.

4.2 Metodología de análisis

Tras conocer el parámetro IS y cómo lo utilizamos en el método que presentamos, pasamos a describir cómo puntúan las buenas prácticas, los pasos a seguir en esta metodología para la evaluación de un sistema y cómo calcular el valor del IS.

4.2.1 Taxonomía de buenas prácticas

Al igual que hicimos con las amenazas, en este apartado se realiza una clasificación de algunas de las buenas prácticas en grupos. Esto permitirá evaluar los distintos componentes de seguridad de un sistema considerando todas las buenas prácticas relacionadas con el mismo.

- **Grupo 1. Cumplimiento de leyes**. En este grupo se incluyen las buenas prácticas que aseguran a nivel legal de que el sistema es correcto:
    - GP.P.13: Asegurar que el sistema cumple con todos los estándares establecidos en base a las leyes de seguridad y privacidad en los sistemas informáticos.
    - GP.P.19: Asegurar que todas las partes involucradas cumplen con el Reglamento General de Protección de Datos.

- **Grupo 2**. **Diseño de la red**. En este grupo se incluyen las buenas prácticas que optan por hacer un diseño seguro de la red:
    - GP.P.4: Diseñar el sistema de forma compartimentada en segmentos para poder bloquear un segmento en caso de ser atacado, evitando así que el efecto se expanda al resto del sistema.
    - GP.T.15: Utilizar protocolos que permitan el aislamiento de los dispositivos que se vean amenazados por un atacante, evitando que el ataque se expanda al resto.

- **Grupo 3**. **Monitorización y evaluación de la red**. En este grupo se incluyen las buenas prácticas que tratan de llevar un control sobre la red para ver qué ocurre en cada punto:
    - GP.P.1: Contemplar la seguridad de todo el sistema IoT desde un punto de vista coherente durante todo el diseño y desarrollo de sus aplicaciones (y de sus dispositivos) implementándola en cada capa desarrollada.
    - GP.P.5: Añadir elementos software en cada nexo de unión entre los distintos segmentos para asegurar que la información cuando pase de un segmento a otro sea segura y fiable.
    - GP.P.6: Establecer un método de análisis para los componentes hardware y software para comprobar que funcionan correctamente y como se espera
    - GP.T.3: Controlar la ejecución de códigos que no estén firmados por desarrolladores conocidos.

- GP.T.5: Implementar mecanismos de monitorización para observar el comportamiento del dispositivo.
- GP.T.20: Incorporar técnicas para la identificación y evaluación de riesgos y amenazas.

- **Grupo 4**. **Control de actualizaciones**. En este grupo se incluyen las buenas prácticas encargadas de asegurarse que las versiones del software sean actualizadas correctamente:
  - GP.P.14: Instalar las actualizaciones software y firmware que surjan de los dispositivos tan pronto como sea posible, tras comprobar que están firmadas y verificadas.
  - GP.P.15: Imposibilitar volver a versiones anteriores de software o firmware más inseguras
  - GP.T.8: Incorporar mecanismos seguros para las actualizaciones.

- **Grupo 5**. **Privacidad**. En este grupo se incluyen las buenas prácticas encargadas de asegurar la privacidad de los datos:
  - GP.P.8: Comprobar el nivel de privacidad de una aplicación antes de lanzarla.
  - GP.P.9: Analizar cómo puede verse afectada la actual privacidad al lanzar una nueva aplicación.

- **Grupo 6. Protección de datos**. En este grupo se incluyen las buenas prácticas cuya finalidad es proteger los datos de posibles robos o modificaciones en ellas:
  - GP.P.17: Forzar el cambio de las credenciales impuestas de fábrica en el momento que se accede a los dispositivos.
  - GP.P.21: Implementar la autenticación de doble factor.
  - GP.T.12: Encriptar la sesión del usuario en las aplicaciones web desde el dispositivo al servidor.
  - GP.T.14: Implementar mecanismos para detectar y controlar la manipulación de los datos.

- GP.T.16: Limitar la cantidad de paquetes recibidos para evitar un colapso del canal de comunicación.
- GP.T.17: Asegurar que el canal de transmisión de los datos protege la información y que se trata de una conexión segura
- GP.T.18: Incluir mecanismos que protejan las credenciales de ser expuestas al exterior.

4.2.2 Asignación de pesos a los grupos

Para la cuantificación numérica del IS, asignaremos a cada grupo de buenas prácticas un peso en función del grado de seguridad que ofrece el sistema, es decir, las medidas que sí se implementan en el mismo.

Así pues, en cada grupo encontramos unas reglas junto con un valor para el parámetro. La primera de ellas implica que todas las buenas prácticas del grupo se han cumplido y por tanto cada una de ellas otorga el valor indicado al parámetro. La segunda de ellas, implica que no todas las buenas prácticas del grupo se han cumplido y por tanto su valor debe ser el indicado. Por último, encontramos el valor que se otorga al IS por parte de las buenas prácticas del grupo en caso de no cumplirse ninguna, que, para este caso, siempre es 0.

Las buenas prácticas que no estén incluidas en este grupo se evalúan todas por igual, es decir, todas otorgan el mismo valor al IS en caso de cumplirse, que en este caso sería de **1,7** puntos o, por lo contrario, **0** en caso de no cumplirse.

Como podemos apreciar más adelante, aquellas buenas prácticas que estén incluidas en algún grupo, tendrán un valor añadido en caso de que todas las de su grupo se cumplan y en caso de que no todas se cumplan, tienen una penalización.

A continuación, presentamos los grupos definidos, como ya se ha citado.

1. **Cumplimiento de leyes**

- ✓ Cumple todos los estándares oficiales (ISO 27000) y ley de protección de datos(LOPD). IS=2,5.
- ✓ Cumple con los estándares oficiales o con la LOPD, pero no ambos. IS=1.
- ✓ No cumple ninguna de las partes. IS=0.

2. **Diseño de la red**

- ✓ La red está correctamente segmentada y los dispositivos pueden ser aislados si son atacados. IS=3.
- ✓ La red está segmentada o los dispositivos pueden aislados. IS=2.
- ✓ La red no está segmentada. IS=0.

3. **Monitorización y evaluación de la red**

- ✓ Incorpora mecanismos de evaluación para comprobar que se implementa la seguridad en cada de desarrollo y mecanismos para observar el comportamiento de estos durante toda su vida. IS=2.
- ✓ Incorpora mecanismos de evaluación o de observación, pero no ambos. IS=1.
- ✓ No incorpora ningún mecanismo. IS=0.

4. **Control de actualizaciones**

- ✓ Disponen de un sistema de gestión para mantener los dispositivos actualizados y un control de instalación de versiones antiguas. IS=2.
- ✓ Disponen de un sistema de actualización o un control de instalación de versiones antiguas. IS=1.
- ✓ No disponen de ningún sistema de actualización. IS=0.

5. **Privacidad**

- ✓ Las aplicaciones ejecutadas por primera vez no comprometen la privacidad del sistema. IS=3.
- ✓ Las aplicaciones tienen un bajo nivel de privacidad, pero no afecta al sistema. IS=2.
- ✓ Las nuevas aplicaciones pueden comprometer la privacidad. IS=0.

6. **Protección de datos**

- ✓ Establece controles de protección de los datos personales, de la sesión y conexión de un usuario y sus credenciales. IS=2.
- ✓ Establece controles de protección, pero no abarca a todos los datos del usuario. IS=1.
- ✓ No establece ningún control de protección de datos. IS=0.

Para las buenas prácticas individuales (aquellas que no están incluidas en ningún grupo) el método será el siguiente:

- ✓ Se cumple la buena práctica. IS=1,5.
- ✓ No se cumple la buena práctica evaluada. IS=0.

De este modo, si hacemos una suma total del valor que puede alcanzar en caso de que todas las buenas prácticas se cumplan este es un 100%, alcanzando así el nivel máximo de seguridad. Contrariamente, si no se cumple ninguna de ellas, la suma del IS será igual a 0% y, por tanto, nos situamos en el nivel más bajo de seguridad, en el cuál el sistema es totalmente inseguro.

4.2.3 Guía de evaluación

Una vez conocida la metodología referente a cómo se valora cada una de las buenas prácticas, pasamos a explicar la metodología para la evaluación del sistema. Para dicha metodología haremos uso de una tabla, adjuntada en el **Anexo 1**, donde se incluyen todas las buenas prácticas agrupadas en función de si son de políticas, de organización o técnicas, en el eje X de la tabla. En el eje Y encontramos las amenazas descritas en el punto 2.2, también agrupadas en sus respectivos grupos. Cada conjunto A(X)-B(Y), donde A y B son los distintos valores de las casillas pertenecientes a los ejes X e Y, marcado en gris, indica el punto donde indicaremos la puntación otorgada a esa buena práctica. Las casillas grises indican que esa buena práctica ayuda a proteger el sistema de dicha amenaza.

Para ello, hemos definido dos métodos distintos:

1. Método 1. **Ordenado** (recomendado): Este método trata de evaluar las buenas prácticas sobre el sistema evaluando en primera instancia las GP que estén incluidas en los distintos grupos mencionados anteriormente y cuando todos los grupos estén evaluados, se evalúan las GP individuales. Por tanto, la metodología es, en primer lugar, elegir qué grupo vamos a evaluar (no es necesario evaluar el primer grupo en primer lugar, el orden en este caso no es importante, pues son grupos que no dependen entre sí) y, tras esto, buscamos qué buenas prácticas pertenecen a él. Una vez localizadas todas ellas, cogemos la tabla de evaluación y localizamos dichas GP. Como podemos observar, todas estas prácticas o bien pertenecen al grupo de GP políticas o bien al de técnicas. Por un lado, cuando nos encontremos con una GP de política, debemos preguntar al responsable de la entidad si dicha política está incorporada en su sistema y, en caso de respuesta positiva, solicitaremos una prueba que acredite la veracidad de ello. En caso de que la respuesta sea negativa, anotaremos en la tabla que dicha política no se cumple. Para las técnicas, debemos preguntar al responsable si incorporan si incorporan dicho mecanismo y, en caso afirmativo, solicitamos que lo muestren y hagan

una prueba para ver que funciona correctamente. Cuando se evalúe una buena práctica si esta pertenece a un grupo y la respuesta es negativa, ya sabemos cuál será la puntuación del resto que sí se cumplan, pero en caso de que la respuesta haya sido afirmativa, debemos esperar a saber si el resto de GP del grupo se cumplen para saber su valor, y en caso de esta ser la última comprobar si se cumplen todas o no. Por otro lado, la forma de evaluar las buenas prácticas organizativas, es solicitar a la entidad que muestre el plan descrito en cada buena práctica para comprobar que disponen de él, y en caso de tenerlo, marcaremos como cumplida dicha práctica.

2. Método 2. **Libre**: La diferencia entre este método y el anterior es que en el anterior empezamos evaluando primero los grupos y luego las demás buenas prácticas. En esta segunda metodología esta restricción no existe, es decir, el evaluador decide por qué buena práctica empezar a evaluar el sistema. Cuando decida qué buena práctica evaluará o bien puede comprobar si pertenece a algún grupo y evaluar seguidamente a dicho grupo, con lo que podrá poner la puntuación de estas al instante o bien podrá evaluarlas con total libertad y cuando estén todas evaluadas, poner la puntación de ellas. La forma de evaluar cada buena práctica es igual que en el método anterior.

Aunque recomendemos el método 1 por medidas organizativas y poder evitar errores en las puntuaciones, ambos métodos son igual de eficientes y eficaces.
Una vez tengamos la tabla con todas las puntuaciones individuales, debemos sumar el total de cada grupo* y escribimos el resultado en la última columna de la tabla junto a la puntación máxima que puede obtener dicho grupo. Sobre esta fracción final (puntuación obtenida/puntuación total) sacamos un porcentaje (sobre 100) del grupo y, el menor de todos los grupos será el valor del IS que situaremos en la última casilla de toda la tabla. Con este valor podemos ya definir el nivel de seguridad de dicho sistema.

*Al sumar el valor de todas buenas prácticas, solo sumaremos una vez el valor de cada buena práctica. Es decir, si la buena práctica 1 aparece varias veces en un grupo, su valor no se sumará tantas veces como aparezca, solo una vez.

Como podemos apreciar tras esta explicación y observando la tabla, la suma de todas las puntuaciones máximas de los grupos no tiene un total de 100, pues muchas de las buenas prácticas se repiten en distintos grupos. La puntuación suma un total de 100 si sumamos el valor de la fila puntuación (fila que refleja el valor que ha obtenido cada buena práctica al ser evaluada). En este caso, conocemos al IS como IS global para así poder distinguir el que pertenece al sistema en su totalidad del IS mínimo que nos indica el nivel según el componente más vulnerable.

5 Niveles de seguridad

Tras el estudio detallado sobre estos sistemas, es posible definir la seguridad de cada uno en base a cuatro niveles de seguridad empezando desde una seguridad en riesgo hasta llegar al punto de seguridad excelente.

Para definir en qué nivel se encuentra el sistema evaluado, debemos situar el índice de seguridad en uno de los grupos en función de su valor.
Dividimos los niveles en seis partes diferentes:

1. **En riesgo**: En este grupo situamos a aquellos que su índice pertenezca al intervalo **[0-20p]**. El hecho de pertenecer a este grupo nos indica que el sistema tiene muchos fallos de seguridad, o, dicho de otra forma, carece de medidas de prevención frente a ataques físicos como digitales. En ambos casos, la red y los dispositivos son muy vulnerables en este punto y pueden verse comprometidos con facilidad. Este error debería ser corregido lo antes posible si queremos impedir que nuestra red o cualquiera de nuestros dispositivos se vean comprometidos.
2. **Bajo**: En este grupo situamos a aquellos que su índice pertenezca al intervalo **[21-40p]**. En este punto podemos apreciar que el sistema sí que cumple con ciertos requisitos de seguridad, es decir, sí que incorpora políticas, técnicas o planes de actuación/prevención. A pesar de esto, siguen siendo insuficientes para definirlos como un sistema seguro, pues puede verse comprometido también con facilidad.
3. **Medio**: En este grupo situamos a aquellos que su índice pertenezca al intervalo **[41-60p]**. Los sistemas incluidos en este grupo, disponen de un a seguridad media, es decir, incorpora las mínimas políticas, técnicas y medidas organizativas para intentar prever un ataque al sistema. A diferencia de los dos anteriores, estos sistemas están más preparados frente a cualquier amenaza. Sin embargo, el sistema sigue siendo bastante vulnerable y por tanto, es recomendable incorporar nuevos mecanismos para aumentar el nivel de seguridad.

4. **Alto**: En este grupo situamos a aquellos que su índice pertenezca al intervalo **[61-80p]**. Cuando situamos a un sistema en este nivel podemos decir que el sistema es bastante seguro y que cumple con buena parte de las buenas prácticas recomendadas para combatir cualquier amenaza que se presente. Podemos apreciar que el sistema dispone de bastantes recursos de seguridad y que, aunque siga siendo débil en ciertos aspectos, no es fácil alterar el sistema. En este punto, sigue siendo recomendable mejorar, como mínimo, la parte declarada como más débil para reforzarla.
5. **Excelente**: En este grupo situamos a aquellos que su índice pertenezca al intervalo **[81-100p]**. Si un sistema alcanza este nivel podemos decir que el sistema es totalmente seguro (o está a punto de serlo). Este nivel describe un sistema que incorpora con todas o casi todas las recomendaciones de nuestro plan y es, por tanto, es difícilmente atacable. Podemos apreciar que todos los grupos de amenazas quedan cubiertos con una serie de buenas prácticas que, en su mayoría, consiguen imposibilitar que se realice un ataque de ese grupo. Aquellos que no alcancen el 100%, pueden mejorar su seguridad incorporando los pocos mecanismos que les falten, pero en este caso, no son obligatorios pues ya disponen de una alta seguridad, aunque si es recomendable hacerlo.

6 Ejemplo de aplicación

A continuación, exponemos el caso de una organización con un sistema IoT integrado detallando como es la red, los mecanismos que incorpora, así como todos los planes organizativos que incorporan en la organización para hacer frente a diversas situaciones. En primera instancia, conoceremos la red, y tas, ello aplicaremos la metodología para su evaluación.

Caso de estudio: Azulejos LittleHouse S.L

Proponemos la evaluación de las buenas prácticas en materia de seguridad de la empresa citada. Esta empresa dispone de un sistema de fabricación 4.0 donde los elementos de producción (hornos, esmaltadoras, etc.) se comunican entre sí mediante una red Profibus. Los sistemas de control de la maquinaria están implementados mediante diversos microcontroladores, desde ARM Cortex A5, hasta MCS 430. Todos ellos están dotados de un procesador de comunicaciones CP1243-1. Cada grupo de trabajo envía información constante al bus de campo. Todas las conexiones emplean el protocolo SSL. Además del protocolo citado, incorporan un mecanismo de control de transmisión donde se limita el tamaño de los paquetes y la cantidad de estos a enviar por hora a un mismo destinatario. Cada dispositivo dispone de la capacidad de autodiagnóstico que le permite observar si incorpora algún fallo y en caso de ser posible, poder recuperarse el mismo. En el siguiente esquema podemos ver las diferentes redes que existen en el sistema y sus interconexiones, así como los los componentes de la empresa conectados a las mismas:

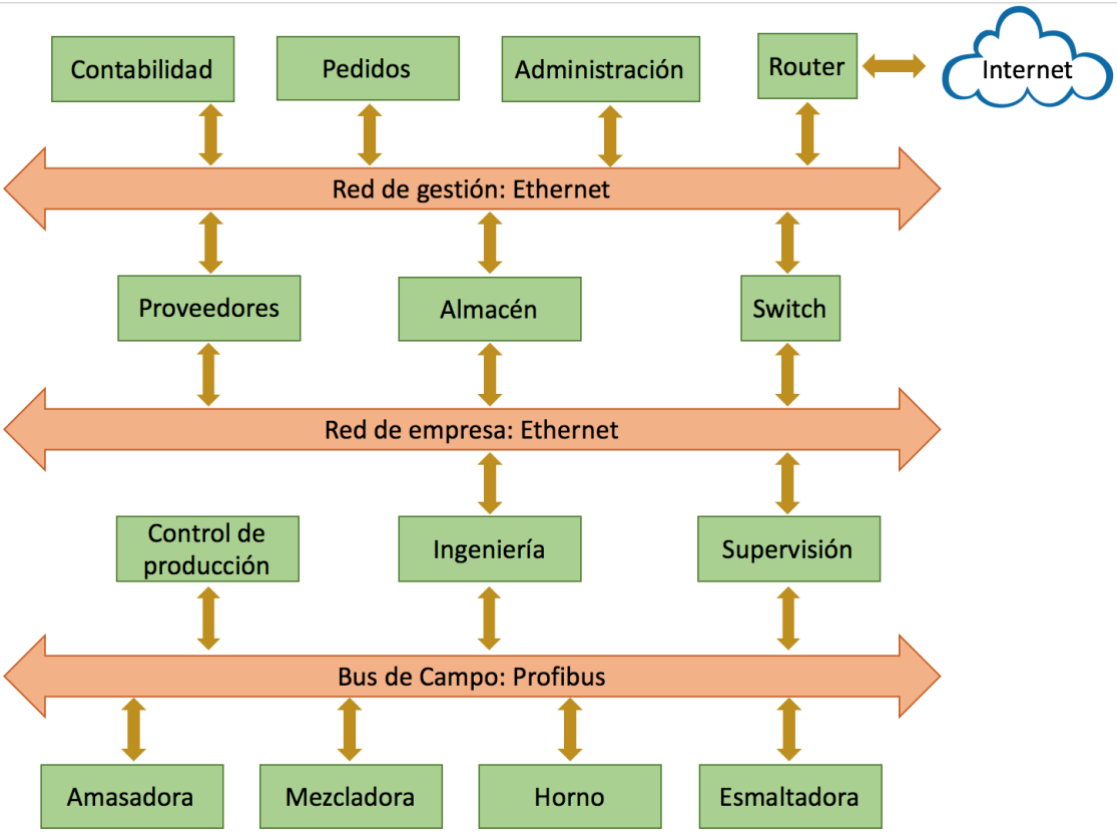


Figura 3: Red de la entidad evaluada

La Figura 3 ilustra los distintos componentes, departamentos y comunicaciones que existen en la red de esta empresa.

A un nivel superior, encontramos tres sectores diferentes; en Control de Producción agrupamos dentro de los analistas a los ingenieros y técnicos de calidad, así como a los técnicos mecánicos, que controlan los procesos de la maquinaria para verificar el correcto comportamiento y funcionamiento. Dicho sector no dispone de una conexión directa a la red de la empresa, pues su único propósito es el control de la maquinaria.

En el sector de Ingeniería cooperan los ingenieros industriales, químicos y mecánicos. Este grupo es el encargado de diseñar los materiales a construir, así como de llevar a cabo estudios de mejora de calidad, eficacia y eficiencia en la producción de estos. También son los encargados del estudio de las necesidades del mercado y analizar pues, la cantidad de material a fabricar en función de la relación oferta / demanda. En este departamento cada cuenta de usuario que se crea a los empleados es personal, es decir, no disponen de una misma cuenta todos para acceder a los sistemas y para verificar la identidad,

emplean una identificación de doble factor. Además de ello, el sistema de ingeniería envía un informe periódico al departamento de supervisión para la revisión de este. Junto a este equipo, encontramos el equipo de Ingenieros en redes y sistemas, encargados de la entidad desde el punto de vista informático. Concretamente, este equipo dispone de un sistema que controla la seguridad en cada dispositivo y en sus comunicaciones. En el año 2016, dicho departamento decide segmentar la red tras darse a conocer numerosos ataques que podrían haber evitado su expansión a lo largo de toda la red si hubiesen implantado dicha medida. Como consecuencia de estas amenazas, también se pudo conocer que podrían haberse evitado con una correcta actualización del software, por lo que, este mismo año, dicho departamento incluye un control de actualizaciones para mantener actualizados todos sus sistemas. En el año 2017, deciden incorporar la nueva política de utilizar la autenticación de doble factor para la identificación de los usuarios. Este departamento también se encarga de la adquisición de los nuevos componentes electrónicos, por lo que, todos los departamentos disponen de controladores, procesadores y tarjetas gráficas, entre otros, con un certificado de garantía de seguridad por parte de la entidad proveedora que recoge archivos de datos para controlarlos. Desde sistemas y redes se definen las nuevas cuentas de usuario y son los únicos que tienen la posibilidad de modificar los ajustes tanto de dichas cuentas como de cualquier sistema, imposibilitando que cualquier otro usuario disponga de dicha capacidad. Anualmente, el encargado de redes y sistemas, audita todas las bases de datos de la empresa para asegurarse que cumplen con el reglamento de protección y privacidad de datos. En el año 2012, este departamento decide redactar un documento donde se indiquen los distintos roles de cada departamento y definir sus responsabilidades y obligaciones, así como sus beneficios, a modo de clarificar qué implica pertenecer a cada uno de estos.

Desde supervisión, los responsables de control reciben los datos de todos los demás departamentos informando de su actividad cifrados y los procesa mediante una aplicación interna desarrollada por el departamento de Ingeniería. Tanto el responsable de este sector como sus empleados, acceden con las mismas credenciales que el departamento les proporcionó, para facilitar la tarea y tener todos los datos en común. Con dicho análisis podemos ver el comportamiento de los sistemas y controlar la actividad de los usuarios. También

podemos ver qué entra y sale por sus puertos, así como saber qué puertos tienen abiertos. En el año 2014, el departamento de supervisión tras observar el comportamiento de los dispositivos y ser capaces de detectar cuando los componentes fallan, deciden definir un plan de actuación para sustituir dichos componentes tan rápido como sea posible para evitar que baje la productividad de la identidad. Este mismo año, deciden redactar también un documento de prevención donde definen la estrategia a seguir en caso de detectar que algún dispositivo ha sido vulnerado. Anteriormente, en el año 2013, ya definieron una estrategia de análisis para reconocer qué componente son vulnerables y cómo hacer frente a dicha situación.

Recientemente este departamento detecta que la mayor parte de las veces que su sistema se ha visto comprometido ha sido por una mala práctica por parte de los empleados. Como resultado, deciden definir una nueva estrategia que ayude a los empleados a no cometer dichos errores y concienciándolos de los peligros que implica una mala operatoria. Dicha estrategia consiste en un plan que todos los integrantes de la organización deben leer donde indica pautas y consejos para evitar fallos tanto por parte suya como ataques de ingeniería social.

En el siguiente nivel, disponemos de dos sectores, proveedores y almacén. En el sector de proveedores, encontramos a un equipo de usuarios que mantienen el contacto con los proveedores de los materiales que se utilizan en esta entidad, negociando con ellos, a partir de los datos obtenidos por el departamento de ingeniería, la cantidad y el precio de los materiales a adquirir. En este departamento tenemos almacenados en una base de datos los datos de todos los proveedores. Todos estos datos se almacenan encriptados mediante el algoritmo AES, y no son compartidos sin consentimiento expreso de los proveedores.

Desde el almacén, los operarios son los encargados de la parte logística, es decir, de recibir la mercancía de los proveedores y anotarlo todo en el sistema para contabilizar el stock de cada material. Son también responsables de proporcionar a los clientes el material vendido y registrar dicha actividad en el sistema. En el almacén disponen de una red de sensores integrada en la plataforma IoT que detecta la actividad de entrada y salida de todos los camiones con las mercancías para registrar todos los accesos a este edificio. Con cada entrada de cada camión, el sensor, tras detectarlo, activa la cámara que lee la

matrícula del vehículo para que el operario identifique al cliente y el sistema le indique qué mercancía le corresponde. Los datos del cliente están almacenados en la base de datos, cifrados también. El acceso a dicha base de datos está restringido a los miembros de almacén, donde disponen de las credenciales predeterminadas. Toda esta información queda registrada en una plataforma a la que administración y contabilidad acceden para realizar sus transacciones.

En el nivel más alto encontramos finalmente los sectores de contabilidad, pedidos y administración, así como la conexión a internet mediante un *router* gestionado por el departamento de Ingeniería y que, por tanto, las credenciales solo son conocidas por ellos ya que fueron cambiadas por las predeterminadas en el instante en que se adquirió dicho elemento.

El departamento de contabilidad formado por asesores, consultores y financieros es el encargado de llevar las cuentas de la empresa, de pagar a los empleados, proveedores, así como de recibir los pagos de los clientes. Para todo ello, disponen de una base de datos, compartida con administración, donde almacenan todos los datos personales de cada usuario. Todas las aplicaciones que son utilizadas por ese departamento, trabajan con el mismo nivel de autoridad independientemente de la función que desempeñe cada una.

Desde pedidos, los trabajadores son los encargados de recoger la demanda de los clientes y negociarla con ellos. Los operarios almacenan dicha información en la base de datos para que los otros departamentos puedan disponer de ella, necesaria tanto para planificar la adquisición de las materias primas, así como para organizar la fabricación de los productos demandados, de forma asociada al cliente para proporcionárselo en el momento de la recogida. Desde pedidos disponen de una única cuenta de acceso a las aplicaciones y a la base de datos, que incorpora una autenticación de doble factor donde cada vez que intentan realizar alguna modificación de los datos, envía un código al correo de la entidad.

Finalmente, en administración disponemos del servicio de atención al cliente, con varios psicólogos en plantilla, y el departamento legal, con dos abogados. Estos últimos, junto a los administradores, se encargan de que la entidad cumpla con todas las leyes y obligaciones, incluyendo la ISO 27001. Con la nueva actualización de la ley de protección de datos, son los encargados de hacer que la GDPR esté en vigor y se cumpla dentro de la entidad. Es por ello, que el pasado 10 de junio de 2018 deciden revisar y hacer cumplir ambas partes.

Evaluación de Azulejos LittleHouse S.L.

Para empezar la evaluación debemos decidir por qué método de los dos citados haremos la evaluación, y, en este caso, es por el método ordenado, donde se estudian los grupos secuencialmente

El primer grupo a estudiar será grupo 1. Empezamos evaluando las buenas prácticas pertenecientes a él. Asumiendo que hemos leído la situación de la entidad, podemos notar que, las GP.P.13 y la GP.P.19 sí se cumplen puesto que disponen de los encargados de cumplirlo y que recientemente han actualizado su sistema para cumplirlas. Como ambas buenas prácticas se cumplen, marcamos en la tabla un valor de 2,5 para ambas y pasamos al siguiente grupo.

El siguiente grupo a evaluar es el grupo 2, donde nos encontramos con la GP.P.4 y la GP.T.15. Podemos apreciar que en el año 2014 y en el año 2016, como citamos en el caso, las dos se cumplen y, por tanto, asociamos el valor máximo establecido en el grupo a ambas, que, en este caso, es 3.

Continuando con el grupo 3, podemos ver que sí disponen de un sistema de monitorización de los elementos, así como de control de todos los dispositivos mediante el envío de informes para ver su comportamiento, con lo que las GP.P.1, 5 y 6 quedan cubiertas. También apreciamos que, en el año 2013 se realiza la propuesta de un plan de análisis de vulnerabilidades, con lo que la GP.T.20 se cumple. La GP.T.5 también queda cubierta con los informes que envían todos los departamentos, y, por último, la GP.T.3, no se cumple pues no disponen de ninguna herramienta que analice un código para ver si es conocido o no, y en caso de no serlo, que lo inspeccione. Por tanto, a pesar de que casi todas se cumplen, debemos otorgar el valor medio a todas ellas, es decir, 1.

Seguimos con el análisis por grupo y esta vez lo hacemos sobre el grupo 4. En él se incluyen tanto la GP.P.14 como la GP.P.15 y ambas se cumplen, ya que, en el año 2016, se incorpora un control para ello. Podemos pues, asegurar también que la GP.T.8 se cumple pues el mecanismo son los propios informáticos y, por tanto, una fuente segura y fiable. Reflejando esto sobre la tabla de evaluación, asignamos un valor de 2 a las 3 GP.

El grupo 5 consta de dos GP, la GP.P.8 y la GP.P.9 pero ninguna de ambas se cumple, pues no se cita ningún control sobre el impacto de las aplicaciones a la privacidad de los datos, por tanto, el valor que otorgamos ambas es 0.

El último grupo a evaluar es el 6, dónde se incluyen la GP.P.17 y la GP.P.21 en primera instancia. Podemos apreciar, que, aunque en ciertas áreas si se cumplen ambas prácticas, ninguna de las dos se cumple en todas ellas, por lo que su valor es 0. De las GP técnicas pertenecientes a este grupo, podemos destacar el cumplimiento de la GP.T.16, ya que el sistema incorpora un mecanismo de control de transmisión, así como de la GP.T.17 pues el protocolo usado en las conexiones es SSL. El resto de ellas, la GP.T.12, GP.T.14 y GP.T.18 no se cumplen pues no se cita ningún mecanismo que ayude a cumplirlas. Por tanto, el valor de GP.T.16 y GP.T.17 será de 1 y de las demás de 0.

Tras haber hecho el análisis de todos los grupos, debemos ahora evaluar cada buena práctica individual para comprobar si se cumplen también o no.

Respecto a la GP.P.2, no podemos afirmar que se cumpla pues no disponen de ningún control para las opciones por lo que su valor es 0.

En cuanto a la GP.P.3, sí que hemos observado que se cumple pues en el paso de los años, han incorporado nuevas políticas por lo que su valor es 1.

La GP.P.7 podemos afirmar que no se cumple, pues, aunque sí se cita que hay herramientas desarrolladas por ellos, no aparece indicado que utilice ningún mecanismo ni política para comprobar que el desarrollo es seguro.

Siguiendo con las políticas, podemos decir que la GP.P.10 sí se cumple pues, con el informe periódico que envían todos donde se registran sus movimientos podemos analizar si alguno de ellos ha sido el envío o filtrado de algún dato sin consentimiento.

La GP.P.11, tras declarar que todas las aplicaciones son ejecutadas con el mismo nivel de autoridad sin ningún tipo de restricción, podemos afirmar que no se cumple, por lo que su valor es 0.

La GP.P.12 no se cumple, pues, aunque sí se cita que hay herramientas desarrolladas por ellos, en ningún instante se afirma que el código de dicha aplicación esté firmado, por lo que su valor, también es 0.

Respecto a la GP.P.16, su valor también es 0 porque no disponen de ningún control sobre el hardware y quien puede alterarlo físicamente.

Lo mismo ocurre para la GP.P.18, donde el sistema no incorpora de ninguna herramienta que analice la seguridad ni el contenido de un dispositivo nuevo en la red.

Este hecho cambia cuando se trata de la GP.P.20 ya que, si se cita que todo el hardware utilizado está certificado por la entidad proveedora, por lo que el valor de esta política, es de 1.

En cuanto a las buenas prácticas de organización y procesos, podemos decir que la GP.O.1, GP.O.3, GP.O.4, GP.O.6 y GP.O.7 sí se cumplen pues todos los planes están definidos en el caso de estudio y en su defecto, el resto no lo están por lo que sobreentendemos que no disponen de ellos. Para los que sí se cumplen añadimos a la tabla un 1 y un 0 a los que no.

Por último, de las buenas prácticas técnicas que nos faltan por analizar empezamos por la GP.T.1, la cual no se cumple puesto que no disponen de ningún mecanismo que ayude al ahorro de energía.

En cuanto a la GP.T.2, sí podemos decir que se cumple pues mediante los informes que envían todos los dispositivos y los mecanismos de control de para limitar paquetes podemos definir un control sobre ella.

La siguiente evaluada es la GP.T.4, que declaramos como no cumplida.

La GP.T.6 podemos decir que sí se cumple porque los datos de cada usuario están almacenados cifrados en bases de datos donde solo unos departamentos determinados tienen acceso y además con los informes se puede controlar la actividad de todos ellos y revisar si se han utilizado algunos datos para otros fines.

El caso define que los dispositivos tienen la capacidad de autodiagnóstico y recuperarse en caso de ser posible por lo que la GP.T.7 también se cumple.

La gestión de las cuentas de los usuarios, así como de sus ajustes solo es gestionada por el departamento de informática por lo que para modificar algo en ellos, deben tener el consentimiento de algún miembro de dicho departamento, por lo que podemos decir que la GP.T.9 también se cumple.

La GP.T.10 podemos afirmar que se cumple porque todos los datos, estén siendo utilizados o no, viajan y se almacenan cifrados.

Además, como ya hemos citado anteriormente, todos los movimientos de los usuarios quedan registrados por lo que la GP.T.11 también se cumple.

Sin embargo, si analizamos la GP.T.13, podemos comprobar que no existe ninguna medida ni herramienta que cumpla con ella.
Por último, la GP.T.19 no se cumple, pues no existe ningún mecanismo que compruebe que los datos sean los correctos o solicitados.

Tras haber asignado a cada buena práctica su puntación correspondiente, procedemos a sacar la puntuación de cada grupo sumando el valor de todas las buenas prácticas que participan en él. Recordamos que aquellas que aparezcan repetidas solo se suman una única vez en cada grupo.

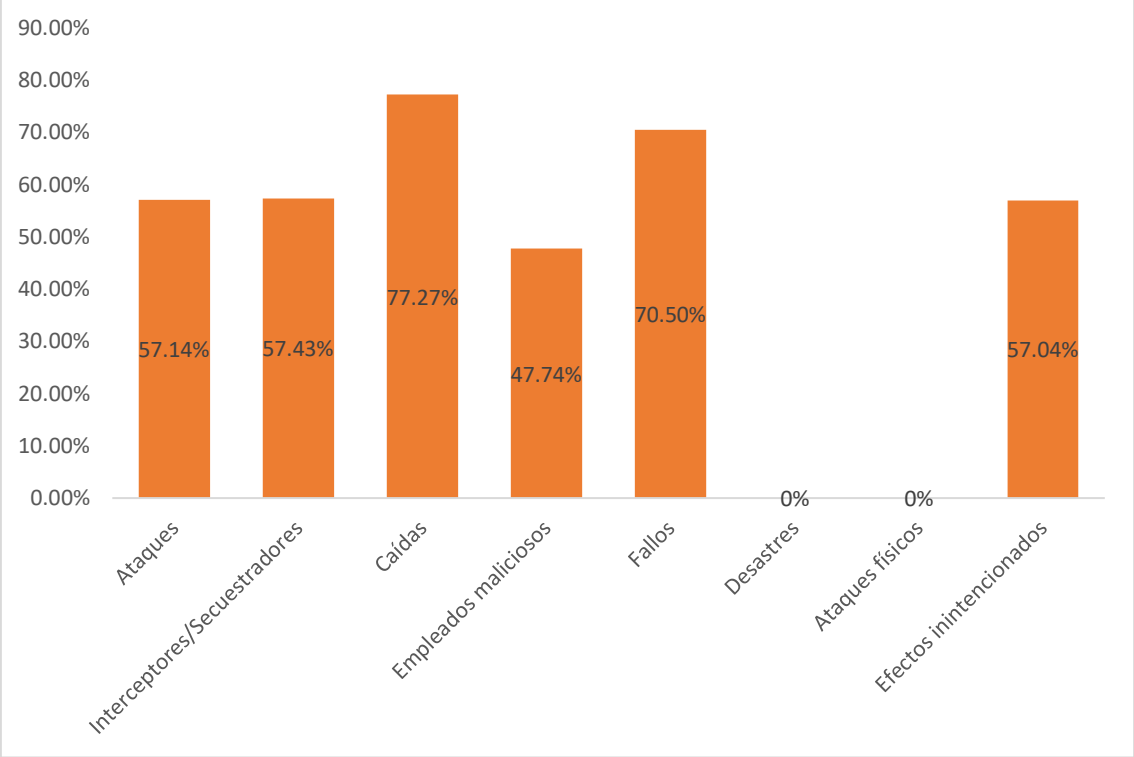
El resultado obtenido sobre la tabla sería el siguiente:

Amenazas / Buenas prácticas		Políticas																					Organizativas										Técnicas																	Total
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Abusos/ Ataques negativos	Malware	1,7	0	1,7	3	1,7						0			2	2		0	0		1,7	0		0	1,7	1,7	0	1,7						1,7	0	0	1,7			2		1,7	1,7			0	3			0		1,7	39,2 / 68,6
	Exploit	1,7	0	1,7	3	1,7		0				0	0		2	2		0			1,7			0	1,7	1,7	0	1,7						1,7	0	0				2			1,7				3					1,7	
	Ataques dirigidos	1,7	0	1,7	3							0			2	2					1,7			0	1,7	1,7	0	1,7						1,7		0							1,7				3					1,7	
	Ataques DDoS	1,7	0	1,7	3										2	2					1,7			0	1,7	1,7	0	1,7						1,7		0							1,7					1,7				1,7	
	Suplantación de dispositivos	1,7	0	1,7			1,7					0			2	2		0	0		1,7			0	1,7	1,7	0	1,7						1,7		0	1,7						1,7				3					1,7	
	Modificación de la información	1,7	0	1,7								0			2	2					1,7			0	1,7				1,7					1,7	0	0					1,7	1,7	1,7		0	0				0		1,7	
Interceptores/ Secuestradores	Ataque de intermediario		0	1,7														0	0		0			0					1,7					1,7			1,7						1,7	0					1,7		1,7	17 / 29,6
	Secuestro protocolo comunicación		0	1,7																				0					1,7					1,7			1,7						1,7	0					1,7		1,7	
	Intercepción de información		0	1,7														0	0					0					1,7					1,7									1,7	0					1,7		1,7	
	Reconocimiento de red		0	1,7															0					0					1,7					1,7									1,7						1,7		1,7	
	Secuestro de sesión		0	1,7														0						0					1,7					1,7			1,7						1,7	0					1,7		1,7	
	Reproducción de mensajes	1,7	0	1,7																	1,7			0					1,7					1,7									1,7	0				1,7			1,7	
Caídas	Caída de red		0	1,7			1,7					0											1,7		1,7					1,7			0	1,7					1,7													13,6 / 17,6
	Fallo de dispositivo						1,7														1,7		1,7										0					1,7										1,7				
	Fallo del sistema		0	1,7			1,7					0											1,7						1,7				0	1,7					1,7													
	Pérdida de servicios						1,7					0											1,7						1,7				0	1,7					1,7													
Empleados maliciosos	Filtrado información privada		0	1,7					0	0	0	0		2,5						2,5							1,7	1,7	0	1,7							1,7		1,7		1,7		0	0				0			16,9/35,4
Fallos	Vulnerabilidades software	1,7						0							2	2										1,7													2	1,7											1,7	23,9 / 33,9
	Fallos de terceros		0	1,7	3										2	2			0				1,7			1,7							0													3	1,7			1,7	
Desastre	Desastre natural																															0																			0 / 1,7
	Desastre ambiental																															0																			
Ataques físicos	Modificación de dispositivos																0															0																			0 / 3,4
	Destrucción de dispositivos																0															0																			
Efectos inintencionados	Fuga de información		0	1,7					0	0	0	0		2,5	2	2	0			2,5								1,7	1,7		1,7			1,7									0					0		1,7	24,3 / 42,6
	Error uso administración dispositivo		0	1,7			1,7					0					0	0										1,7	1,7													1,7									
	Información extraída de fuentes no fiables		0	1,7		1,7																																											0		
	Diseño inadecuado/ falta de adaptación												0																					1,7																	
Puntuación		1,7	0	1,7	3	1,7	1,7	0	0	0	0	0	0	2,5	2	2	0	0	0	2,5	1,7	0	1	0	1	1	0	1,7	1,7	0	1,7	0	0	1,7	0	0	1,7	1,7	1,7	2	1,7	1,7	1,7	0	0	0	3	1,7	1,7	0	0	1,7	

Obteniendo los porcentajes de cada grupo sobre 100, obtenemos los siguientes resultados:

1. Ataques: 57,14%
2. Interceptores/Secuestradores: 57,43%
3. Caídas: 77,27%
4. Empleados maliciosos: 47,74%
5. Fallos: 70,5%

6. Desastres: 0%
7. Ataques físicos: 0%
8. Efectos inintencionados: 57,04%



Con los datos obtenidos podemos decir que tanto el grupo de ataques como el de interceptores/secuestradores y el de daños inintencionados están situados en el nivel es medio, acerándose a alto. El grupo de caídas observamos que es el que mayor puntación tiene, junto a fallos, ambos incluidos en el nivel alto. El grupo de daños lo situamos en un nivel medio. Por último, apreciamos que tanto desastres como ataques físicos están en el nivel más bajo, por lo que, por su parte, el sistema está en riesgo.

Observamos que el valor mínimo es un 0%, por lo que declaramos el sistema con un IS = 0 y esto nos lleva a definir el nivel de seguridad como un sistema en riesgo. Si calculamos el IS_{global} el resultado es de 50,6% situando al sistema, a nivel global en el nivel medio de seguridad.

7 Conclusiones

A lo largo de este trabajo hemos definido qué es el Internet de las Cosas y cuál es su situación actual en el ámbito de la seguridad. A continuación, a través de la documentación consultada, hemos averiguado cuáles son las principales amenazas que se presentan en estos sistemas y cuáles son las mejores formas de combatirlas.
Finalmente, en este trabajo se ha propuesto una nueva metodología para la evaluación de sistemas IoT con el fin de definir su nivel de seguridad.

El principal problema que hemos encontrado en este trabajo ha sido durante el desarrollo de la nueva metodología propuesta, pues ninguno de los implicados en el trabajo ha desarrollado una y, a medida que hemos ido testeando las ideas que surgían, nos hemos dado cuenta que o bien no era eficiente y lo suficientemente innovador, o bien no era lo que buscábamos. Finalmente, conseguimos encontrar una solución que alcanzara todas nuestras expectativas de la mejor forma posible.

El desarrollo de esta nueva metodología también ha sido posible gracias a los conocimientos que hemos ido adquiriendo durante el grado en asignaturas como tecnologías en servicios y sistemas de la red, seguridad en redes y en el resto de asignaturas que hemos ido viendo a lo largo de todo el grado. Estos conocimientos nos han permitido entender tanto la parte más técnica del trabajo para el correcto desarrollo como saber qué recursos debemos emplear para que llegar exitosamente a un punto final.

Esta nueva metodología se demuestra eficiente y eficaz pues necesita menos tiempo que otras tecnologías con el mismo fin para analizar los sistemas y es capaz de analizar todos los aspectos de la seguridad y evaluarlos satisfactoriamente. Además de ello, podemos destacar de esta nueva metodología que no necesita que su evaluador sea un experto en seguridad pues no requiere que el evaluador conozca detalladamente herramientas informáticas para evaluar el sistema. Esta propuesta es, por tanto, muy útil para aquellos que se incorporen recientemente al mundo de la seguridad por ejemplo y carecen de

conocimientos y destreza como evaluadores y también para aquellos que con unos conocimientos básicos de informática quieran evaluar un sistema, como sería el caso de, por ejemplo, responsables de entidades que quieran comprobar la seguridad de su red y dispositivos.

Aunque la metodología presente estas grandes ventajas, todavía está en su primera fase de desarrollo. A pesar de ello, hemos podido comprobar que es un buen método y, por tanto, quedamos satisfechos con el trabajo realizado.

8 Bibliografía

Nota: todas las referencias fueron accedidas por última vez en junio de 2018

[1] Recomendaciones de seguridad en dispositivos IoT. Página web. Accesible en:
https://www.ithinkupc.com/blog-es/recomendaciones-de-seguridad-en-dispositivos-iot

[2] Seguridad física de los sistemas. Red Iris. Página web. Accesible en: https://www.rediris.es/cert/doc/unixsec/node7.html

[3] Ingeniería del software. Séptima edición. Ian Sommerville. Accesible en: https://books.google.es/books?id=gQWd49zSut4C&pg=PA43&lpg=PA43&dq=confiabilidad+sistemas+informaticos&source=bl&ots=s702qnrCtg&sig=_zDmhfCXaJsjh8DQoofjTT6psGg&hl=es&sa=X&ved=0ahUKEwiVrZH1jsvXAhXEzqQKHWxLAmkQ6AEIXjAL - v=onepage&q=confiabilidad sis

[4] Smart Grid Spain. Revista Tecnológica Española de Redes Eléctricas. Accesible en:
http://smartgridspain.org/web/blog/2016/08/16/las-10-principales-areas-de-aplicacion-de-la-iot/

[5] Internet of Things for Smart Cities. IEEE Explore. Digital Library. Accesible en: http://ieeexplore.ieee.org/document/6740844/?reload=true

[6] Estado del arte de la seguridad en IoT. Centre de seguretat TIC Generalitat Valenciana. Accesible en:
http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D_Informe-Internet_de_las_Cosas.pdf

[7] Qué es y hacia dónde va el Internet de las cosas. FHIOS. Página web. Accesible en:

https://www.fhios.es/el-internet-de-las-cosas/

[8] El IoT y sus riesgos. Oficina de seguridad del internauta. Página web. Accesible en:

https://www.osi.es/es/actualidad/blog/2017/10/02/la-ciberseguridad-es-una-responsabilidad-de-todos-el-iot-y-sus-riesgos

[9] Campos de aplicación de IoT. Página web. Accesible en:

http://www.evaluandosoftware.com/campos-de-aplicacion-de-internet-of-things-o-internet-de-las-cosas/

[10] Construyendo la IoT. IEEE Computer society. Accesible en:

https://www.computer.org/web/computingnow/archive/building-the-internet-of-things-july-2015-spanish-version

[11]Seguridad informática. Página web. Accesible en:
https://infosegur.wordpress.com/tag/confidencialidad/

[12] ¿Qué es una vulnerabilidad software? Instituto Nacional de Tecnologías de la comunicación. Observatorio de la seguridad de la información. Accesible en:
https://www.jesusamieiro.com/wp-content/uploads/2011/08/Que_son_las_vulnerabilidades_del_-software.pdf

[13] Thoughts on reliability in the Internet of Things. James Kempf, Jari Arkko, Neda Beheshti, Kiran Yedavalli. Accesible en:
https://iab.org/wp-content/IAB-uploads/2011/03/Kempf.pdf

[14] Introducción a los sistemas embebidos. CERT de seguridad e industria. Accesible en:
https://www.certsi.es/blog/introduccion-los-sistemas-embebidos

[15] Riesgos y retos de seguridad y privacidad IoT. CERT de seguridad e industria. Accesible en:
https://www.certsi.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

[16] Sistemas ciberfísicos. IT Solutions. Grupo garatu. Accesible en:
https://grupogaratu.com/que-son-sistemas-ciber-fisicos-cps/

[17] La estrategia alemana, Industria 4.0. Wolfgang Schroeder. Friedrich Ebert Stiftung. Accesible en:
https://www.uni-kassel.de/fb05/fileadmin/datas/fb05/FG_Politikwissenschaften/PSBRD/FES_Madrid_Schroeder_Industria_4.0_ES.pdf

[18] Ambient intelligence: Technologies, applications and opportunities. Diane J. Cook, Juan C. Augusto, Vikramaditya R. Jakkula. Accesible en:
http://www.elsevier.com/locate/pmc

[19] Qué es la seguridad informática y cómo puede ayudar. VIU. Página web. Accesible en:
https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/

[20] Rowhammer, la vulnerabilidad que afecta a la DRAM. HostDimeBlog. Página web. Accesible en:
http://blog.hostdime.com.co/rowhammer-la-vulnerabilidad-que-afecta-la-dram/

[21]Ataques de ingeniería social: qué son y cómo evitarlos. BBVA. Ana Gómez Blanco. Accesible en:
https://www.bbva.com/es/ataques-ingenieria-social-evitarlos/

[22] Ataque bajo el logo de Correos. Periódico ABC tecnología. Ana Martínez. Accesible en:
https://www.abc.es/tecnologia/informatica-software/20150330/abci-virus-correos-201503272129.html

[23] Thomas Reid. Philosophica. Enciclopedia filosófica online. Accesible en:
http://www.philosophica.info/voces/reid/Reid.html

[24] Amenaza vs Vulnerabilidad. Instituto nacional de ciberseguridad. Accesible en:
https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[25] Cyber Security Standards, Practices and Industrial Applications: Systems and methodologies. Embbebed Systems Security. Muhammad Farooq-i-Azam, Muhammad Naeem Ayyaz.

[26] Buenas prácticas en Internet de las Cosas. CCN-Cert. Centro criptológico nacional. Accesible en:
https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2258-ccn-cert-bp-05-16-internet-de-las-cosas/file.html

[27] Cyber Security and Resilience of smart cars. Good practices and recommendations. ENISA. Accesible en:
https://www.enisa.europa.eu/

9 Anexos

9.1 Anexo 1