Trabajo Final Integrador

Título: Análisis Forense de Entornos IoT

Caso de estudio: “Sistema Inteligente para la Captura de Datos de Medidores de Energía Eléctrica”

POSGRADO ESPECIALIZACIÓN EN INFORMÁTICA FORENSE

Autor: Herminia Beatriz Parra de Gallo

Director:

Mg. Ing. Miguel Ángel Solinas

Publicación: 06/05/2022

UNIVERSIDAD FASTA

FACULTAD DE INGENIERÍA

AGRADECIMIENTO

Este trabajo no hubiera sido posible sin la ayuda de un conjunto de personas que con su aporte me permitieron llegar hasta esta instancia.

En primer lugar, el Mg. Ing. Miguel Ángel Solinas, a quien le debo su tiempo de colaboración para la lectura y ajuste del Trabajo Final. Su experiencia, paciencia y disposición para corregir, sugerir, aportar y orientar la investigación fue destacable.

El Ing. Santiago Salamandri también destinó tiempo y dedicación para la definición del Caso de Estudio utilizado, y a él le agradezco su atenta predisposición, experiencia y acompañamiento en la temática de Internet de las Cosas.

Mis compañeros de la carrera de Especialización en Informática Forense, que crearon un espacio compartido de opiniones y experiencia que resultó altamente motivante para avanzar y finalizar la cursada, al igual que el equipo docente y directivo de la carrera y de la Facultad de Ingeniería de UFASTA que siempre estuvo dispuesto para el acompañamiento hasta esta instancia de finalización.

A todos ellos muchísimas gracias.

RESUMEN

Internet de las Cosas (IoT) es el entorno del futuro, donde se conectan componentes de cualquier tecnología, haciendo posible el procesamiento y control de funcionalidades mediante un marco único e integrado.

Este contexto, de impacto en la economía y la industria, también está disponible para quienes delinquen en internet. Y desde esa óptica se aborda el entorno IoT, proponiendo una guía de acción para el análisis forense adecuado y suficiente de la evidencia digital en estos contextos.

Se revisan varias metodologías para forensia de IoT, derivándose una Guía de Actuación Forense para Entornos IoT, que se ejemplifica en un caso de estudio particular.

Se tomará como caso de estudio el proyecto de "Sistema Inteligente para la Captura de Datos de Medidores de Energía Eléctrica", de la tesis "Sistema de Telemedición de servicios públicos basado en Inteligencia Artificial" del Ing. Santiago Salamandri, para la Maestría en IoT de la UBA. Y se aplica esta propuesta tomando los medidores domiciliarios de consumo de energía, para analizar los ataques más comunes a entornos de IoT, identificando las vulnerabilidades presentes en un evento de acceso indebido supuesto, y finalizando con recomendaciones de seguridad para la mejora de la arquitectura de seguridad del modelo propuesto.

Palabras Claves

Forensia Digital, IoT, vulnerabilidad IoT

ÍNDICE

Capítulo 1. Introducción

El presente trabajo consiste en la definición de una propuesta metodológica para el análisis forense de entornos de IoT, considerando como caso de aplicación un **Sistema Inteligente para la Captura de Datos de Medidores de Energía Eléctrica (SICaMEe),** el cual -a la fecha- se encuentra en etapa de diseño experimental.

Con carácter de investigación aplicada, y bajo el enfoque de un proyecto tecnológico, se pretende analizar los ataques de seguridad más comunes a entornos de IoT, identificando las vulnerabilidades que pudieran detectarse en un ejemplo como el caso de estudio señalado, para finalizar con una propuesta de posibles mejoras y recomendaciones de seguridad informática en el modelo tecnológico propuesto para SICaMEe.

Suponiendo este sistema en particular y un escenario de ataque según diferentes técnicas y herramientas para vulnerar alguno de sus componentes, se debe formular una propuesta de análisis forense en términos de un *proyecto de ingeniería*.

Desde ese enfoque, se ha seguido el esquema de desarrollo de un proyecto tecnológico, tomando el modelo PMI según la propuesta de Ameijide (Ameijide García, 2016), a la que se agregaron componentes del enfoque socio-comunitario de los Proyectos de Desarrollo Tecnológico y/o Impacto Social (PDTS).

Así, es posible recurrir a las herramientas metodológicas de uso habitual en la ingeniería, a la que se agrega la resolución de una necesidad del mercado, identificado a partir de un demandante de la tecnología desarrollada.

Por su parte, la guía GAFIoT desarrollada en el Capítulo 3 del presente trabajo, se basa en la metodología PURI (Di Iorio et al., 2017) por lo que de por sí, cuenta con las características propias de un proyecto tecnológico:

- Se encuentran definidos los componentes esenciales: actividades, recursos, planificación y responsabilidades, más la aplicación de criterios metodológicos reconocidos.
- Se respeta el ciclo de vida de un proyecto: inicio, organización y preparación, ejecución del proyecto y cierre; con las correspondientes instancias de feedback e iteración de las fases, tareas y actividades involucradas
- Se sigue el modelo universal de secuenciación de procesos, en términos de entradas (internas o externas), actividades y herramientas adecuadas, y salidas (a otros procesos internos o externos).
- Pero es importante identificar el enfoque social del proyecto, en términos de un PDTS (Proyecto de Desarrollo Tecnológico y Social) y considerar los aspectos del producto a generar, la demanda, originalidad, su relevancia y pertinencia, entre otros criterios asociados a la *demanda social* del proyecto tecnológico.

Al respecto de estos criterios -y considerando el caso de SICaMEe- se puede decir que:

- Trabajar en el proceso de medición del consumo energético, con herramientas tecnológicas que abaraten tiempos y recursos, puede generar un impacto importante en las empresas

distribuidoras de energía domiciliaria, al trabajar analíticamente los datos recabados en ambientes de Big Data e IA.

- El consumidor final puede organizar más eficientemente su consumo si puede acceder a información diaria o más detallada sobre el gasto energético que se genera en su hogar, permitiendo una estrategia más ajustada para el uso de la electricidad. Por ejemplo: ¿en cuál momento del día se dan los picos de consumo? ¿cuál es la variación estacional de mis consumos?
- La aplicación de recomendaciones de seguridad informática impacta en el fortalecimiento de un sistema tecnológico confiable y eficiente, permitiendo mejorar la calidad del servicio energético que se brinda a la comunidad.
- En términos de la ***demanda social*** el proyecto SICaMEe cubre todos los actores del ambiente en que actúa: empresas distribuidoras (particularmente los administradores y gestores de datos), instaladores del servicio y consumidor final del servicio energético. Para todos ellos, un sistema que cuente con herramientas de soporte para la toma de mejores y más rápidas decisiones es de vital importancia, a fin de lograr un uso racional de la energía optimizando su consumo.
- Se destaca la característica de ***originalidad*** en la innovación de procesos al incorporar herramientas tecnológicas emergentes, como lo son: IoT, sistemas embebidos propios e inteligencia artificial.
- La característica de ***pertinencia*** que se pide en un PDTS consiste en considerar si la estrategia de investigación, la metodología propuesta, y su consistencia, son adecuadas para resolver el problema identificado en el contexto local de aplicación. Todo ello se observa en este caso porque la incorporación del análisis forense previo al desarrollo del producto final (como estrategia y metodología de estudio del tema), supone una mejora desde el diseño del propio sistema, con todas las ventajas que ello significa para que el sistema resultante sea más útil para la comunidad que lo utilizará.

El objetivo final del SICaMEe se encuentra alineado con las políticas de uso eficiente de la energía y particularmente con el 7° ODS de la ONU[1]: "*Garantizar el acceso a una energía asequible, segura, sostenible y moderna*". Esto marca la característica de ***relevancia*** que se pide desde un PDTS.

Para una mejor organización del contenido de este Trabajo Final Integrador, se siguió la distribución temática en capítulos.

El Capítulo 2 describe "***La Seguridad Informática en los entornos de IoT***" incluyendo el análisis de las vulnerabilidades identificadas en base a los casos de ataques más frecuentes en ambientes IoT.

El Capítulo 3 identificado como "***Forensia de IoT***" incluye un breve análisis del estado del arte sobre ese tema, así como un estudio comparativo de las diferentes metodologías existentes para el análisis forense de entornos IoT, para concluir con una propuesta específica para el caso de estudio que se abordará.

En el Capítulo 4 denominado "***Caso de Estudio - Sistema Inteligente para la Captura de Datos de Medidores de Energía Eléctrica (SICaMEe)***" se describe el modelo de procesamiento, sistema

[1] https://www.un.org/sustainabledevelopment/es/energy/

embebido y los componentes necesarios para definir el contexto que se toma como ejemplo para la aplicación de la propuesta de análisis forense definido en las secciones anteriores.

En el Capítulo 5 se aborda la "***Propuesta de Análisis Forense del Caso de Estudio***" para el caso de estudio descripto el capítulo anterior, bajo la suposición de que esté presente alguna de las vulnerabilidades de entornos IoT señaladas en el Capítulo 2 del trabajo.

El Capítulo 6 describe las "***Recomendaciones sobre Seguridad Informática para el SICaMEe***", con sugerencias de mejoras de propiedades de seguridad y las recomendaciones de monitoreo de esas propiedades para el caso de estudio considerado

En el Capítulo 7 se señalan las "***Conclusiones"*** arribadas en base a la problemática, la solución planteada y las posibles líneas de investigación que podrían abordarse a futuro.

Por último, en el Anexo I se detallan las características de los tipos de ataques a entornos IoT.

Capítulo 2. La Seguridad Informática en los Entornos IoT

La seguridad informática es una de las cuestiones de mayor interés generadas a partir del cambio cultural y tecnológico devenido luego del año 2020. El avance tecnológico logrado a partir de la pandemia COVID-19 trajo aparejado también un espacio virtual que todavía no se encuentra debidamente protegido ante el avance de la ciberdelincuencia. Los dos ámbitos crecen raudamente por igual: la tecnología y el delito virtual.

En este contexto, es conveniente abordar algunos aspectos de la seguridad informática vinculadas a los entornos IoT que son de interés para este trabajo:

- IoT desde las estadísticas
- La cultura de la seguridad informática
- Vulnerabilidades a la que está expuesta la tecnología IoT

2.1 IoT desde las estadísticas

El informe "La lista definitiva de estadísticas de Internet de las cosas para 2022" (Steward, 2022) señala datos distintivos para el contexto de IoT que se avecina en los próximos años:

- Habrá 35.82 mil millones de dispositivos IoT instalados en todo el mundo para 2021 y 75.44 millones para 2025. Los dispositivos de IoT están en todas partes, desde relojes inteligentes hasta asistentes de voz, y están dando forma a los modos en que trabajamos, hablamos y nos relacionamos entre nosotros.
- Habrá 1.9 mil millones de suscripciones celulares 5G para 2024. Con la rápida expansión de 5G, Ericsson predice que 5G continuará impulsando el crecimiento de IoT. Se espera que el mercado norteamericano experimente el mayor crecimiento, con el 63 % de las suscripciones móviles.
- Se espera que el número de conexiones de IoT por celulares alcance los 3.5 millones en 2023. Esto es el resultado de una combinación de inteligencia artificial, aprendizaje automático y procesos de datos proporcionados por las soluciones de IoT. Los expertos predicen que el norte de Asia albergará más de 2 millones de dispositivos IoT para 2023.
- Las empresas podrían invertir hasta $ 15 billones (de dólares) en IoT para 2025. Las empresas están comenzando a ver el potencial de los dispositivos de IoT y las estadísticas de IoT muestran que varios proveedores de atención médica, fabricantes y gobiernos ya han optado por invertir en esta tecnología.
- El 54% de las empresas encuestadas consideran la reducción de costos como principal razón para la inversión en IoT. Los datos recopilados de 1.600 empresas y sus proyectos de IoT revelaron que la clara mayoría reconoció la reducción de costos como el objetivo principal (54%). Solo el 35% de los proyectos de IoT estaban relacionados con un aumento de los ingresos e incluso un número menor para la seguridad (24%).
- Casi el 70% de todos los vehículos nuevos a nivel mundial estarán conectados a Internet en 2023. En un informe de 2018 realizado por *IDC*[2], el número proyectado de automóviles conectados a Internet alcanzará casi 76 millones de unidades para 2023. Esto equivale a aproximadamente el

[2] https://www.idc.com/

70% de la cifra total; mientras tanto, la porción estadounidense será el 90% de todos los vehículos nuevos.

- Los dispositivos IoT generarán 79.4 zettabytes (ZB) de datos para 2025. Según el IDC, los dispositivos de IoT generarán 79.4 ZB de datos para el 2025. Los datos totales de Internet utilizados combinadamente representaron 4.4 ZB el año 2019. Sin embargo, para 2025, se espera que crezca a 175 ZB, de los cuales más de la mitad (79.4 ZB) se deberían a los dispositivos de IoT.

En particular, respecto de ***seguridad en entornos IoT*** (Steward, 2022) señala:

- El gasto anual en medidas de seguridad de IoT aumentará a 631 millones de dólares para 2021. A medida que crece el mercado de IoT, solo se espera que aumente la importancia de asegurar e integrar las redes de IoT. El gasto anual en seguridad de IoT creció más de 6 veces desde 2016 a 2021 (de $91 millones a $ 631 millones). Esta estadística de crecimiento augura que IoT se encamina hacia un auge masivo en los próximos diez años.
- Según *NETSCOUT* [3] , los dispositivos IoT suelen ser atacados dentro de los cinco minutos posteriores a la conexión a Internet. Se espera que esta tendencia crezca a medida que se conecten más dispositivos cada año.
- El 75% de los casos de ciberataques se llevan a cabo a través de enrutadores. Para *Symantec*[4] la mayoría de los ataques cibernéticos a dispositivos IoT son el resultado de enrutadores de red. Los enrutadores de red son objetivos favoritos de muchos ciberdelincuentes, con un promedio de 5.200 enrutadores atacados por mes.
- El 74% de los consumidores globales se preocupan por perder sus derechos civiles debido a IoT. Según la encuesta sobre la privacidad de IoT desarrollada en (McCauley & Lara, 2018) el 74% de los consumidores globales se preocupan por perder sus derechos civiles sobre IoT, 1600 consumidores en 8 países afirmaron que el 92% desea controlar el tipo de información personal que se recopila automáticamente.
- El 48% de las empresas admiten que no pueden detectar las brechas de seguridad de IoT en su red. Según Thales[5], aproximadamente la mitad de las empresas que utilizan IoT no pueden identificar cuándo su red está comprometida.

De la lectura de estos números se deduce que los entornos IoT son propicios para el desarrollo de la delincuencia digital, y son bien aprovechados por quienes eligen ese camino.

A partir de la pandemia, se observó un gran avance de los incidentes de seguridad en el mundo virtual. Son varios los tipos de ataques que se llevan a cabo con o por medio de los dispositivos digitales: malware, phishing, estafas, ransomware, ciberbulling, etc.

La mayoría de estas acciones intrusivas tienen en común dos características:

- La falta de una cultura de la seguridad informática en los usuarios, sean estos desarrolladores, gestores de datos o usuarios finales, y

[3] https://www.netscout.com/es

[4] https://securitycloud.symantec.com/cc/landing

[5] https://www.thalesgroup.com

- El aprovechamiento de las vulnerabilidades de las tecnologías, sean éstas de software, hardware, estructuras de datos o redes de transmisión de datos.

Ambas características se abordan particularmente en los siguientes apartados de esta sección.

2.2 La Cultura de la Seguridad Informática

El Diccionario de la Real Academia Española[6] define *cultura* como "*Conjunto de conocimientos que permite a alguien desarrollar su juicio crítico. Conjunto de modos de vida y costumbres, conocimientos y grado de desarrollo artístico, científico, industrial, en una época, grupo social, etc.*". En términos generales, la cultura se asocia a los conceptos de valores, actitudes, principios, creencias y comportamientos de una persona, un grupo de ellas o una organización. En el contexto de la seguridad informática, esa cultura implica la asimilación de estos elementos, pero asociados bajo un objetivo: la protección de los datos.

Se puede decir que la cultura de la seguridad informática debe rescatar los valores básicos de cualquier cultura, tales como: respeto por la dignidad del otro, libertad, justicia, equidad, honestidad, responsabilidad.

A los que se deben sumar aquellos relacionados con el uso adecuado de los datos, que se pueden tomar de la ***Directiva 46/95 de la Unión Europea*** (Parlamento Europeo, 1995)**,** en el apartado que define los ***principios de orientación para determinar la licitud*** (Luz Clara, 2021) de los datos:

- ***La calidad de los datos***. Los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.
- ***La legitimación del tratamiento***. El tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca, o si el tratamiento es necesario para la ejecución de un contrato u obligación jurídica en el que el interesado sea parte.
- ***Las categorías especiales de tratamiento***. Deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.
- ***La información a los afectados por dicho tratamiento***. El responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernan.
- ***El derecho de acceso del interesado a los datos***. Todos los interesados deberán tener el derecho de obtener del responsable del tratamiento: la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos; así como a la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva
- ***Las excepciones y limitaciones***. Se podrá limitar el alcance de estos principios con el objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la

[6] https://dle.rae.es

represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la Unión Europea o la protección del interesado.

- ***El derecho del interesado a oponerse al tratamiento***. El interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento, y deberá ser informado antes de que los datos se comuniquen a terceros.
- ***La confidencialidad y la seguridad del tratamiento***. Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento.

  Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.
- ***La notificación del tratamiento a la autoridad de control***. El responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. Ésta realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

Así, se ha definido el marco sobre el cual debería trabajarse en la generación de una cultura de la seguridad informática.

En las empresas, y empujadas por la necesidad de incorporar la seguridad informática de sus intangibles como ventaja competitiva, existen varias propuestas para la generación de una cultura de la seguridad informática.

Como ejemplo, puede tomarse lo dicho por Schwartz (Schwartz, 2018) que propone una estrategia basada en los siguientes pasos:

- Comunique constantemente la conexión entre la seguridad y los objetivos de la misión.
- Establezca prácticas para "incorporar seguridad" y mecanismos rápidos de retroalimentación para corregir errores.
- Establecer normas de seguridad e higiene y establecer altos estándares de calidad.
- Adopte un enfoque de cero defectos conocidos.
- Examine continuamente la seguridad, tanto en el desarrollo como en la producción.

También es muy interesante considerar la propuesta de ***auto-seguridad*** de (Augusto & Moreno, 2012) que señala que: "*…la auto-seguridad aplicada a la informática es: el correcto comportamiento de los individuos frente a las TI; comportamiento que es formado por el propio individuo, y que nos debe llevar a una conducta controlada, para evitar situaciones de riesgo que pongan en peligro la conservación de la información de la organización. La auto-seguridad es, además, una actitud, que debemos como seres inteligentes asumir con compromiso, ética y responsabilidad...".*

Por su parte INCIBE en su informe sobre "Desarrollar Cultura en Seguridad" (Instituto Nacional de Ciberseguridad, 2020) aborda la formación y capacitación en el tema considerando los distintos usuarios:

- El ***usuario técnico*** debe capacitarse en función del rol que cumple en la organización:
    - Seguridad de los sistemas operativos y aplicaciones
    - Gestión y administración de elementos de seguridad perimetral (firewall, antivirus, etc.)
    - Copias de seguridad y otros mecanismos de contingencia.
    - Sistemas de seguridad de los equipos informáticos del usuario.
    - Gestión y resolución de incidentes de seguridad.
    - Políticas de seguridad sobre los soportes extraíbles.
    - Otros mecanismos de seguridad (herramientas de cifrado, mecanismos de autenticación, gestión de contraseñas, etc.).
- Mientras que el ***usuario final*** debe formarse en:
    - Aspectos técnicos, legales y organizativos de la seguridad informática. Debe conocer las implicancias de no aplicar las políticas de seguridad de la organización.
    - Situaciones de riesgo informático que puede encontrar en el contexto de su trabajo
    - Toma de conciencia sobre el correcto tratamiento de los datos personales, así como de la privacidad y confidencialidad de la información de la organización.
    - Cuestiones técnicas propias del uso de las tecnologías como, por ejemplo:
        - Aprender a reconocer un ataque de ingeniería social
        - Proteger adecuadamente su puesto de trabajo aplicando las herramientas de seguridad informática (antivirus, técnicas de doble autenticación, etc.)
        - Conocer y aplicar los controles de acceso físico a dependencias restringidas.
        - Tratamiento y manejo adecuados de los dispositivos móviles
        - Entender los riesgos que conlleva el acceso a redes públicas, páginas externas, aplicaciones de terceros o descargas de actualizaciones no autorizadas por el departamento de informática.

De lo dicho hasta aquí, es dable recalcar que es necesario aplicar estos conceptos para generar una cultura de la seguridad informática entre los usuarios finales, gestores de datos y desarrolladores de entornos IoT.

2.3 Vulnerabilidades a la que está expuesta la Tecnología IoT

Además de los beneficios de IoT para la salud y la calidad de vida de las personas, el entorno de internet también abre caminos a las ciberamenazas.

Cualquier dispositivo móvil puede ser utilizado por los ciberdelincuentes, y cuantos más dispositivos se conecten a la red, más control y acceso se dará a los atacantes. Por esa razón, la activa expansión de las redes de IoT también potencia con la misma magnitud el acceso indebido a los dispositivos y datos.

Son muchos y diversos los estudios acerca de la vulnerabilidad de la seguridad informática presente en los componentes que integran un entorno de IoT. De estas investigaciones se identifican que los tipos de ataques más habituales sobre entornos IoT son los siguientes:

- Reconocimiento Inicial
- Ataque Físico
- Ataque de Man-In-The-Middle (MITM)
- Ransomware
- Ataque de Fuerza Bruta
- Botnets
- Ataques de Denegación de Servicios Distribuidos (DDoS)
- Amenazas Persistentes Avanzadas

Un detalle de cada uno de estos tipos de ataques se describe en el Anexo I del presente trabajo.

Capítulo 3. Forensia de IoT

En este capítulo se describen las temáticas de base: IoT, Forensia Digital y la aplicación del análisis forense en entornos de IoT. Cada una de ellas se detallan en las siguientes subsecciones.

3.1 IoT

Según la recomendación ITU Y.6060 (Unión Internacional de Telecomunicaciones, 2012) se define IoT como la "*Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras*".

IoT es el entorno de comunicación del futuro, que conecta componentes tecnológicos y de automatización de diversos tipos para compartir datos, permitiendo el procesamiento y control de funcionalidades mediante un marco de trabajo integrado puesto a disposición del usuario. Es el modelo en el cual se sustentan las ciudades inteligentes y está incluido en el concepto de Industrias 4.0 que hará posible pasar a ambientes altamente tecnológicos.

Al ser un sistema que comunica cualquier objeto físico o lógico, ubicado en cualquier lugar, y en cualquier instante el entorno IoT tiene particularidades que diferencian esta tecnología de las aplicadas hasta hoy; revelando un funcionamiento muy dinámico por la escalabilidad, magnitud y heterogeneidad de los dispositivos IoT.

Este contexto, de sabidas ventajas para la mejora de la calidad de vida de las personas también está a disposición de quienes buscan en internet nuevos modos de delinquir y de quebrar la seguridad informática. Y es desde esta óptica que se aborda el entorno IoT, para proponer un marco de trabajo que permita un análisis forense suficiente y adecuado a estos contextos.

Son varios los modelos descriptivos que explican la arquitectura de los entornos IoT.

Para el presente trabajo se toma el modelo de referencia IoT de la Recomendación ITU Y.6060 que se grafica en la **Figura 1**, basado en cuatro capas y capacidades de gestión y de seguridad relacionadas con éstas.

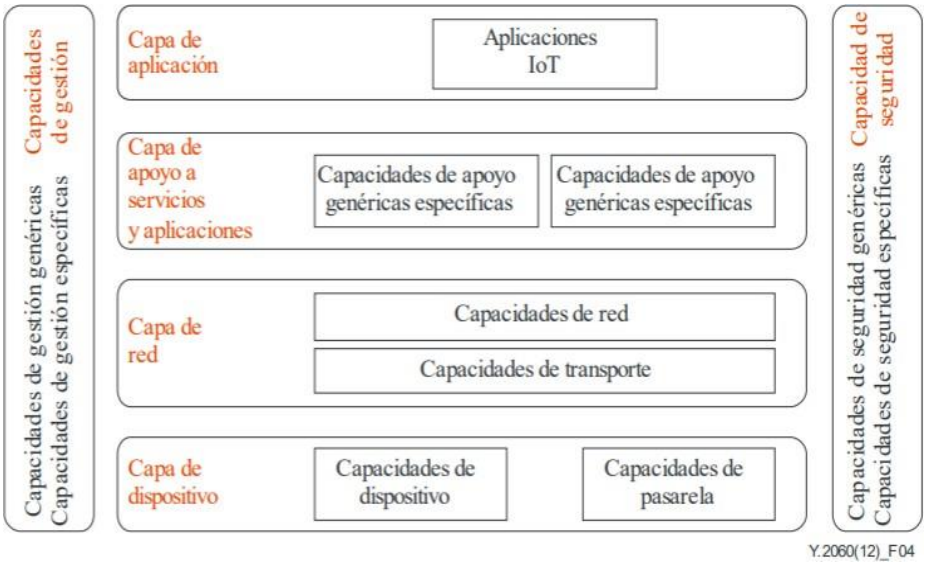

Figura 1: Modelo de Referencia de IoT

La ***capa de aplicación*** incluye las interfaces de software que permiten la interacción del usuario con el sistema IoT. Son aplicaciones que trabajan sobre los servicios de la nube, con acceso a los dispositivos del entorno IoT.

La ***capa de apoyo a servicios y aplicaciones*** identifica dos tipos de capacidades:

- Genéricas, para tareas de procesamiento o almacenamiento de datos, y
- Específicas, para funciones propias de los dispositivos IoT.

Aquí se debe identificar el modelo de servicio en la nube (usualmente SaaS o IaaS) que se aplica en el entorno IoT.

La ***capa de red*** identifica entre las capacidades propias de la red (conectividad y control de acceso) y las capacidades de transporte (tráfico de datos entre los dispositivos que conforman el entorno IoT). Algunas de las tecnologías de conectividad usuales son:

- LoRaWan (modulación de radio frecuencia para redes de área amplia de baja potencia)
- LPWAN (tecnologías diseñadas para comunicaciones inalámbricas de bajo consumo y largo alcance),
- Bluetooth Low Energy (BLE),
- ZigBee, NFC y
- RFID.

Por último, en la ***capa de dispositivos*** se encuentran diferenciadas las capacidades del dispositivo (en cuanto a su funcionamiento lógico) y las capacidades de pasarelas (referidas a las interfaces de comunicación y protocolos que vinculan el modelo de procesamiento IoT).

Hay dos ***capacidades transversales*** a todo el modelo: la de gestión y la seguridad.

- La primera hace referencia a la capacidad para administrar el sistema IoT garantizando el funcionamiento normal de la red, al congeniar las aplicaciones que actúan automáticamente con aquellas que se generan por decisión del usuario.
- Respecto de la seguridad, el modelo considera que la conexión de cualquier “cosa” al entorno IoT conlleva amenazas de seguridad, por lo que éste debe tener capacidad para integrar distintas técnicas y políticas de seguridad provenientes de los componentes IoT que lo integran.

3.2 Ciberseguridad en entornos IoT

Existen varias investigaciones acerca de la ciberseguridad en los entornos IoT. Entre los trabajos más destacados se puede citar (Bhatt & Bhushan, 2021) que describe un análisis profundo de las amenazas y vulnerabilidades de la arquitectura IoT, (Domínguez Margareto, 2020) que propone una guía de mejores prácticas para proteger un sistema IoT, (Fagan et al., 2021) autor del Informe Interno 8259 del NIST en el que proponen las actividades fundamentales de ciberseguridad que deberían tener presente los fabricantes de dispositivos de IoT.

Estas investigaciones definen un espacio para el abordaje de la ciberseguridad de entornos IoT como el que se detalla en el presente trabajo, considerando las siguientes características distintivas que se deben tener en cuenta:

- La ciberseguridad de los entornos IoT debe considerarse desde sus cuatro componentes básicos:
    - las *cosas y los dispositivos IoT,*
    - el software o aplicación que gestiona todo el sistema,
    - la plataforma de conectividad y
    - los usuarios consumidores finales del servicio.

Es necesario considerar una estrategia completa para la protección del sistema analizando cada elemento, en sus amenazas y vulnerabilidades más usuales.

- Se debe reconocer también que no hay un ***nivel homogéneo*** respecto de la incorporación de capacidades para enfrentar los riesgos y amenazas en todos los componentes que integran la arquitectura IoT. Si bien hay avances importantes en lo referente a la plataforma de comunicación, no se observa idéntica madurez en las capacidades de ciberseguridad de los dispositivos IoT (que suelen ser muy básicas) y mucho menos, en la cultura de la seguridad del usuario de IoT, sea este desarrollador o consumidor final.
- En su mayoría, las amenazas de ciberseguridad en los entornos IoT son ya conocidas (malware, denegación de servicios, acceso no autorizado, por citar algunos ejemplos), que provienen de riesgos también conocidos y suficientemente estudiados en los entornos tecnológicos tradicionales (redes, sistemas de gestión, bases de datos, etc.). Pero está faltando ***integrarlos con más fuerza*** en los entornos IoT aprovechando las experiencias exitosas de otros ambientes tecnológicos, de manera de formalizarlas en metodologías de trabajo acondicionadas específicamente para entornos IoT que aborden las particularidades de estos contextos. Aquí radica el aporte innovador del presente trabajo.

Considerando estas características se avanza en la propuesta de ciberseguridad para el caso de estudio, y se describe detalladamente en el Capítulo 5 del presente trabajo.

3.3 Forensia Digital

La DFRWS 2001 USA(Palmer, 2001) define la Forensia Digital como "*el uso de métodos científicamente probados y derivados hacia la preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital proveniente de fuentes digitales con el propósito de facilitar o promover la reconstrucción de eventos, que se consideran criminales, o ayudando a anticipar acciones no autorizadas que pueden ser perjudiciales para las operaciones planeadas*".

Cualquier evento resultante de la interacción entre el usuario y la computadora deja un rastro digital, o sea un registro que certifica la ejecución de procesos (cálculo, comunicación y/o almacenamiento de datos) ejecutados por el usuario. Este rastro digital, toma el carácter de evidencia digital cuando permite acreditar hechos en una acción judicial. Pero, además, el análisis forense permite la investigación de incidentes de seguridad informática, para tratar de averiguar qué ocurrió, como ocurrió, cuáles serían las causas que deben atenderse mediante un plan de contención de la situación.

Así, es posible considerar la Forensia digital de IoT para auditar y mejorar la infraestructura de ciberseguridad que debería tener el entorno IoT del caso de estudio que se aborda como ejemplo en el presente trabajo.

3.4 Metodologías para la Forensia Digital de IoT

En esta sección se aborda la definición del estado del arte con una búsqueda sistemática en los portales de publicaciones científicas, considerando las investigaciones relacionadas a un conjunto de palabras claves (metodologías forenses, IoT, vulnerabilidades) para el período 2019-2021.

A partir de las investigaciones encontradas, se realizó un trabajo comparativo obteniendo los aspectos destacados que luego se proponen en la Guía de Actuación Forense para Internet de las Cosas (GAFIoT), basada en la metodología PURI para el análisis forense.

Uno de los principales desafíos que deben resolverse desde la Forensia Digital, es el procedimiento por seguir para el análisis forense en contextos complejos como el descripto. Además de las cuestiones técnicas que todavía se deben solucionar, preocupa a la justicia la aplicación de procesos metodológicos y científicos para abordar la evidencia digital, toda vez que con ello se responde a los principios de integridad y admisibilidad de ésta. Si esto es una preocupación constante en la Forensia Digital tradicional, lo es más cuando se aborda IoT.

Son de interés los 4 principios básicos para el tratamiento de la evidencia digital formulados en la Guía de buenas prácticas de la ACPO (Rashid et al., 2019):

- Las personas que actúan sobre la evidencia digital no deben tomar ninguna acción que comprometa la confiabilidad de esta.
- Quienes accedan a la evidencia digital, deben tener competencias suficientes para hacerlo.
- Debe conservarse una pista de auditoría de todos los procesos aplicados a la evidencia digital, a fin de que un tercero pueda examinarlos y lograr el mismo resultado.
- El responsable de la investigación debe garantizar que estos principios se cumplan.
- Estos principios ayudan a entender que el proceso forense incluye -además de las cuestiones técnicas-, exigencias relativas a la integridad de la evidencia y al proceso de investigación.

A modo de orden, se describen a continuación algunas de las metodologías forenses de aplicación generalizada cuando se procesa evidencia digital, y un conjunto de marcos de trabajo propios para la Forensia de Entornos IoT.

Se consideraron un conjunto de 12 investigaciones que abordan diferentes metodologías para la Forensia de IoT, y se realizó un estudio comparativo a fin de identificar las fortalezas y vacancias de cada una en función de las etapas del análisis forense.

Si se tienen presente las etapas generales del proceso forense, se puede observar que las diferentes metodologías enunciadas cuentan con un grado de desarrollo y completitud variado.

Cuando se aplica la Forensia Digital en el ámbito de la justicia, se debe considerar un contexto integrado del caso delictivo que se está analizando, incluyendo no solo los procesos técnicos relativos al tratamiento de la evidencia digital, sino también, las actividades propias de la investigación criminal y del proceso judicial al que se debe ajustar la investigación.

Cualquiera fuera el marco de trabajo que se quiera aplicar, el proceso forense debe incluir las etapas señaladas en la **Figura 2**. Todo ello con el desarrollo concurrente de las normas procesales judiciales y de investigación.

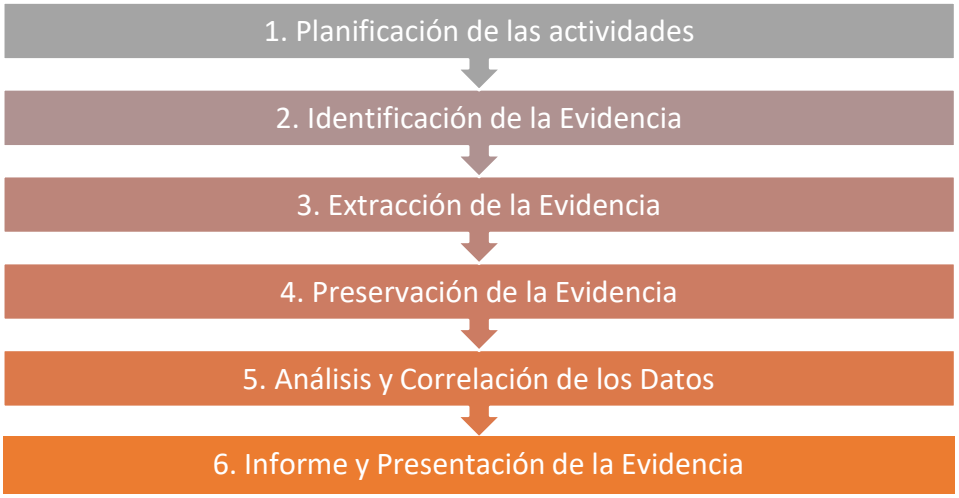

Figura 2: Pasos Generales del Análisis Forense

En base a las etapas del proceso forense y a los requerimientos nombrados, se puede establecer un cuadro comparativo de las metodologías analizadas.

La Tabla 1 muestra las 12 metodologías (en sendas columnas), comparadas en función de un conjunto de criterios señaladas en las filas (las etapas del proceso forense más los requerimientos legales y de investigación). En la intersección de cada fila/columna, se indica el cumplimiento (o no) de la metodología respecto del criterio considerado.

La tabla contiene una última fila que señala el grado de completitud o porcentaje de cumplimiento de la metodología, en relación con las etapas del proceso forense y a los requerimientos de las normas procesales de la justicia y de la investigación criminal.

De los 12 marcos de trabajo enunciados en la Tabla 1, solo 4 (DFIFIoT (Kebande & Ray, 2016), IDFIF-IoT (Kebande et al., 2018), DFIM (Qatawneh et al., 2019) y la propuesta de (Islam et al., 2017)) incluyen de manera completa las 6 etapas señaladas del proceso forense y, además, consideran las normas procesales y de investigación requeridas por la justicia.

Tabla 1: Cuadro Comparativo de Metodologías de IoT Analizadas

	DFIFIoT	CFIBD-IoT	IDFIF-IoT	FSAIoT	FIF-IoT	Chhabra	FoBI	IoTDots	DFIM	Islam	PDF	Costantini
• Planificación	Si	No	Si	No	No	No	No	No	Si	Si	No	No
• Identificación de la evidencia	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
• Extracción	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
• Preservación	Si	Si	Si	No	Si	No	No	No	Si	Si	Si	No
• Análisis y correlación de los datos	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
• Informe y presentación de la evidencia	Si	No	Si	No	No	No	No	No	Si	Si	No	No
Normas procesales y criminalísticas	Si	No	Si	No	No	No	No	No	Si	Si	No	No
Grado de Completitud	100%	57%	100%	43%	57%	43%	43%	43%	100%	100%	57%	14%

Las restantes no incluyen la etapa inicial de planificación, ni abordan explícitamente las normas procesales y de investigación del proceso forense. Aun así, presentan aportes innovadores al proceso forense que deben destacarse. Tal es el caso de:

- CFIBD-IoT (Kebande et al., 2017) propone una solución basada en agentes inteligentes para capturar los datos del entorno IoT. Y además distingue al especialista forense que interviene en las tareas de obtención de la evidencia de aquel que interviene en el análisis de los datos.
- FSAIoT (Meffert et al., 2017) está centrada en la identificación de los estados del dispositivo IoT y de los servicios de la nube que consumen éstos. Esta característica, propia de los contextos de la nube, no está presente en las metodologías tradicionales de análisis forense.
- FIF-IoT (Hossain et al., 2018) agrega tecnología Blockchain para garantizar la integridad, confidencialidad y privacidad de la evidencia digital, siendo esto de gran impacto en la admisibilidad de la evidencia como prueba judicial.
- Las restantes propuestas se distinguen por incorporar tecnologías innovadoras: (Chhabra et al., 2020) incorpora herramientas para procesar la evidencia digital en términos de un sistema experto; FoBI (Al-Masri et al., 2018) presenta un modelo basado en *Fog Computing*[7]; IoTDots (Babun et al., 2018) se enfoca en la extracción de datos con técnicas de aprendizaje automático; mientras que PDF (Koroniotis et al., 2020) propone un marco forense basado en redes neuronales profundas.
- La propuesta de (Costantini et al., 2020) se distingue expresamente por la definición de un modelo matemático para validar la calidad de la información de la evidencia obtenida, a partir de un conjunto de parámetros que representan diferentes niveles de complejidad y factores humanos incluidos en el proceso forense.

3.5 Propuesta de una Guía de Actuación Forense para entornos IoT (GAFIoT)

GAFIoT está basada en la metodología PURI con el agregado de algunos de los aspectos más destacados de los marcos de trabajo analizados en la sección anterior.

Se selecciona la metodología PURI pues conjuga aspectos informáticos y criminalísticos que ordenan el procedimiento pericial, y presenta las características necesarias para cumplir el condicionamiento de "principios científicos y técnicos" requeridos por el derecho procesal argentino a la actividad forense digital. Por otra parte, el enfoque ingenieril de esa propuesta, y la utilización del modelo de proceso unificado resultan muy interesantes para abordar el análisis forense desde una visión integrada y multidisciplinaria, considerando las cuestiones relativas al Derecho Procesal, a la Informática Forense y a la Criminalística.

GAFIoT mantiene las mismas fases definidas en PURI, y adecua las actividades y tareas de cada una para considerar las particularidades propias del entorno IoT. También se aprovecha las

[7] Fog Computing o Computación en la niebla se considera una extensión local de la nube y se refiere a una infraestructura de aplicaciones y hardware distribuida, diseñada para almacenar y procesar datos de objetos conectados. En lugar de centralizar la información que producen los sensores en la nube, la idea a través de este entorno es utilizar equipos ubicados en el borde de la red (routers, gateways, switches, dispositivos móviles, etc.) para realizar el procesamiento. Al crear esta superposición intermedia lo más cerca posible de la producción de datos, el objetivo final es optimizar los tiempos de respuesta de las aplicaciones.

características de casos de uso, iteración y trabajo multidisciplinario definidos para PURI. En la **Figura 3** se muestran las fases y actividades definidas para GAFIoT.

En GAFIoT, las actividades definidas para cada fase se consideran interactivas, ya que habitualmente resultan de acciones que se retroalimentan a medida que se avanza en el proceso.

Así, en la ***Fase 1*** (Preparación), las actividades de *Identificación del Caso* e *Identificación de la Infraestructura IoT*, se retroalimentan para definir una visión inicial del caso en estudio que se va aproximado en las sucesivas iteraciones.

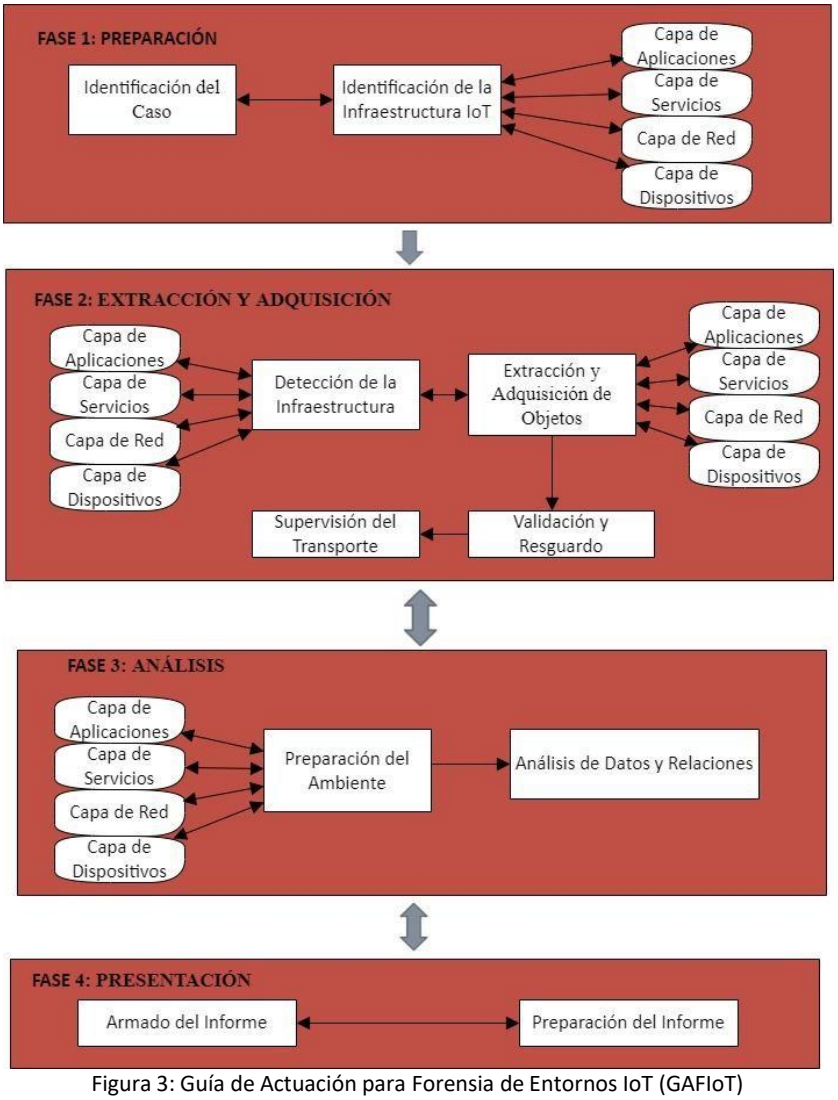

Figura 3: Guía de Actuación para Forensia de Entornos IoT (GAFIoT)

Tanto en esta fase como en las dos fases siguientes, GAFIoT enfoca las actividades sobre las capas del entorno IoT, que también tienen una retroalimentación entre ellas, ya que es necesario considerar cada capa en particular, pero sin descuidar la interacción de cada una sobre las restantes capas.

En relación con la actividad de ***Identificación del Caso*** el objetivo a lograr es el relevamiento de la situación mediante diferentes técnicas: entrevistas con usuarios, revisión de documentación técnica del sistema IoT, consulta a expertos en caso necesario, etc. Lo que se pretende es contar con un panorama lo más detallado posible que sirva para definir la estrategia o enfoque del análisis forense.

Respecto de la ***Identificación de la Infraestructura IoT***, se incluyen tareas de observación del lugar para identificar los objetos de interés. Mientras sea posible, se realizará una inspección ocular, seguida de la utilización de herramientas específicas para la detección de componentes y/o servicios no visibles a simple vista.

Aquí, la tarea debe centrarse en la detección de la infraestructura de red y de servicios utilizada para el Entorno IoT que particularmente se está analizando, atendiendo al modelo de cuatro capas ya descripto. La capa de aplicación es habitual encontrarla en el dispositivo que el usuario final utiliza para interactuar con el entorno IoT (usualmente una PC o un teléfono inteligente), y la capa de dispositivos también podría estar accesible, pues a través de ellos (sensores, cámaras, alarmas, etc.) el sistema se conecta a las "cosas". En las dos capas intermedias (de red y de servicios), es importante identificar el modelo de servicios que se está consumiendo (SaaS o IaaS), así como los tipos de servicios (aplicaciones, procesamiento, almacenamiento, recursos de networking, etc.).

También se debe identificar los recursos distribuidos que quedan bajo responsabilidad del usuario de aquellos que son brindados por el servicio propiamente. Esta actividad se completa con la identificación de los aspectos de seguridad informática necesarios. En esta etapa es de mucha utilidad el concepto de ***ecosistema IoT*** propuesto en IDFIF-IoT (Kebande et al., 2018) para identificar y conocer las políticas de IoT de la organización que se está estudiando, sus estrategias de seguridad, interoperabilidad, estandarización, posibles legislaciones y regulaciones de IoT comprometidas.

PURI señala tres fases para el contacto con la evidencia:

- Recolección: en los casos en que se debe considerar el dispositivo que contiene la evidencia, y que éste fuera recogido en la escena del hecho,
- Extracción: fase correspondiente a obtener el archivo que contiene la evidencia en sí misma, y
- Adquisición: referida a la realización de la imagen forense para proteger la evidencia extraída.

Pero en los entornos IoT, que se basan en una infraestructura distribuida, el contacto con la evidencia es on-line. Difícilmente se requiere recolectar la evidencia en el propio dispositivo que la contiene ya que muchas veces no se tiene acceso físico al mismo, sino que se accede a través de la correspondiente red de comunicación implementada.

Por otra parte, al momento de acceder al entorno IoT, por la dinámica de actualización continua de todo el sistema, la extracción de la evidencia debe realizarse en el mismo momento en que se detecta, y obviamente, se deberá preservar debidamente con las técnicas de encriptación adecuadas.

Por ello, GAFIoT propone unificar estas actividades en una única ***Fase 2*** de Extracción y Adquisición. Esta fase comprende varias actividades: *Detección de la Infraestructura, Extracción y Adquisición de Objetos, Validación y Resguardo, y Supervisión del Traslado*.

En la ***Detección de la Infraestructura,*** el objetivo es identificar con claridad todos los componentes del entorno IoT que se está analizando. Mediante la observación visual, y si fuera posible la visita a las instalaciones tecnológicas, se deberá ajustar la Identificación de la Infraestructura IoT definida en la Fase 1.

La actividad de ***Extracción y Adquisición de Objetos*** debe respetar estrictamente el protocolo de Cadena de Custodia establecido, cuidando de realizar correctamente las tareas técnicas más adecuadas para el tipo de evidencia de que se trate; así como todo lo relacionado con la

preservación, embalaje y transporte de los mismos. Es importante considerar además los procedimientos aceptados por el ámbito judicial para esta actividad, como los protocolos, guías y/o recomendaciones vigentes en las jurisdicciones en las que se desarrolla la actuación.

Se debe considerar que la extracción de la evidencia dependerá de la factibilidad de acceso a los espacios de almacenamiento volátil o permanente de los componentes que integran cada capa del Entorno IoT. Los accesos más dificultosos suelen ser a las capas de servicios y de red porque depende de terceros y puede requerir una solicitud mandataria del juez para que los proveedores permitan el acceso a su infraestructura.

El acceso a la capa de aplicación depende de la factibilidad de contar con los dispositivos utilizados por los usuarios, mientras que el acceso a los dispositivos IoT dependerá de la factibilidad geográfica y física de acceder a los sensores instalados físicamente en las "cosas" que controlan. Es decir, no resulta sencillo ingresar al entorno IoT y *llegar de manera directa* al componente de memoria física instalado en cada componente.

La actividad de ***Validación y Resguardo*** implica la realización de las imágenes forenses y su encriptación, que deberán ser debidamente registradas en la cadena de custodia. Es de utilidad la propuesta de FIF-IoT (Hossain et al., 2018), de usar tecnología Blockchain para garantizar la integridad, confidencialidad y privacidad de la evidencia digital obtenida.

La última actividad de esta fase es la ***Supervisión del Transporte.*** Se refiere a los cuidados últimos que deben tener los expertos forenses en adquisición de datos cuando deben entregar las evidencias a terceros intervinientes en la investigación, asegurándose que se cumplan estrictamente los criterios de resguardo y preservación de la evidencia digital.

La ***Fase 3*** (Análisis) comprende el trabajo de integrar en un todo coherente el conjunto de evidencias recolectadas. Se realizan dos actividades: *Preparación del Ambiente* y *Análisis de Datos y Relaciones.*

La ***Preparación del Ambiente*** se refiere a la actividad de adecuación del ambiente tecnológico para la manipulación de las evidencias encontradas, en un contexto similar al escenario delictivo, para trabajar con el conjunto de evidencias recolectadas que provienen de diferentes capas del entorno IoT.

El ***Análisis de Datos y Relaciones*** es una actividad que se realiza en base a las búsquedas y correlaciones de datos de las evidencias, recurriendo a diferentes técnicas y métodos según sea pertinente, desde el análisis de archivos con información histórica, hasta la búsqueda por cadena de caracteres.

Para esta etapa, existen herramientas forenses que presentan un árbol de navegación con toda la información extraída, y un conjunto de funcionalidades que ayudan al investigador en el análisis (líneas de tiempo, filtros por tipo de archivo, etc.), pero es probable que al utilizarse un conjunto de herramientas separadas para cada componente del entorno IoT, sea necesario conjugar y vincular los datos en un proceso manual que dependerá de la capacidad del especialista forense para identificar relaciones y vincularlas debidamente, recurriendo para ello al enfoque sistémico y el enfoque estratégico para mirar el ambiente IoT, que le permitirá relacionar la evidencia con el caso delictivo que se está analizando.

La metodología cierra con la ***Fase 4*** de Presentación, que se corresponde con las actividades ya señaladas por PURI, pero enfatizando además las explicaciones convenientes para mostrar el entorno IoT, para un mejor entendimiento de quienes no son expertos en estas tecnologías.

La primera de las actividades de esta fase, ***Armado del Informe,*** incluye la escritura del Informe Forense Final que usualmente contiene dos partes:

- *Informe Forense*, que debe contener los datos de identificación del caso, de la evidencia digital procesada, la metodología y herramientas utilizadas, y la respuesta a los puntos de pericia requeridos. El informe debe escribirse en términos adecuados para la lectura de quienes no sean expertos informáticos. Cuando se trata de entorno IoT, debe incluir definiciones técnicas básicas (la arquitectura de procesamiento, por ejemplo), a fin de que se comprenda mejor cómo actuó la evidencia digital en la comisión del delito investigado.
- *Anexos Técnicos* que apoyan las conclusiones del análisis forense. Este apartado servirá para replicar el proceso forense si fuera necesario, y debe contener todos los datos técnicos requeridos a ese efecto.

La segunda actividad de esta fase es la ***Preparación del Informe,*** que consiste en aprestar los documentos precitados y la evidencia digital que los sustentan. La presentación de la evidencia digital requiere de tareas necesarias que garantizar la admisibilidad de la evidencia (sanitización del soporte y tratamiento contra escritura, grabación y encriptación de los archivos).

Se puede concluir este capítulo indicando las razones que justifican la utilización de GAFIoT como metodología para el análisis forense del caso de estudio.

El estudio comparativo realizado permitió enriquecer la propuesta de GAFIoT con el agregado de aquellas cuestiones que resultan propias del entorno IoT, adaptando el enfoque genérico propuesto por PURI a la situación de IoT, principalmente en lo que respecta a la toma de evidencia *en caliente,* es decir, con el sistema trabajando en tiempo real.

Se considera que GAFIoT podría ser utilizado como marco de trabajo por el analista forense presentando –entre otros beneficios- los siguientes:

- Se ajusta al proceso general forense, respetando las actividades y criterios requeridos por las buenas prácticas de la investigación forense.
- Basada en el modelo PURI, toma de ésta la versatilidad de las actividades y tareas, propuestas en un ciclo de interacción entre las fases -y de iteración entre los procesos- que enriquece la actividad forense, permitiendo responder a los modos propios de la gestión ingenieril de proyectos.
- Ordena el proceso forense al identificar las actividades de cada fase según las distintas capas del modelo IoT.
- Incluye actividades lo suficientemente genéricas como para ajustar la tarea forense a diferentes entornos IoT, considerando estos sistemas de manera integral, más allá de los componentes individuales y específicos que lo integren.

Por último, el caso de estudio que se presenta propone un espacio para la validación de la propuesta, que lógicamente, redundará en la maduración de GAFIoT, tanto por la revisión y ajuste de los procesos definidos, como por las cuestiones propias de la seguridad informática del entorno IoT.

Capítulo 4. Caso de Estudio Captura de datos de Medidores de Energía Eléctrica

Para este caso particular, el demandante es una PYME que se dedica a la fabricación y producción de componentes electromecánicos variados, que propone desarrollar un sistema de control de medidores de energía eléctrica domiciliaria, a fin de captar los datos de consumo de manera automática, sin intervención humana.

El proyecto, pensado desde la aplicación de las tecnologías existentes más adecuadas a la idea, se basa en un modelo que nuclea componentes de IoT, sistemas embebidos, inteligencia artificial y una plataforma de comunicación wifi.

4.1 La Red de Distribución Eléctrica y el consumo domiciliario

La esencia del sistema considerado como caso de uso es un dispositivo inteligente denominado ***Smart Meter*** que cuenta con la capacidad de capturar información sobre el consumo de un medidor domiciliario de energía eléctrica. Este dispositivo se monta sobre una infraestructura tecnológica suficiente y adecuada para responder de manera eficiente a la recolección automática de esos datos, que impactan positivamente en la gestión de las compañías prestadoras de electricidad domiciliaria.

Para ahondar con más detalle se resume las características de una ***Smart Grid,*** definida en (Casellas Beneyto et al., 2010).

La red eléctrica que alimenta una ciudad o espacio geográfico determinado está compuesta por un conjunto de elementos (generadores de energía, redes de transporte, estaciones transformadoras y líneas de distribución), que confluyen -cada uno con su función particular- para que la electricidad llegue a los hogares.

La búsqueda de una mayor eficacia en el consumo, así como la tendencia de la cultura del ahorro energético, ha promovido la incorporación de las tecnologías de la información y de la comunicación (TICs) a este esquema.

Así la tendencia actual es lo que se denomina *Smart Grid* entendiéndose como un sistema de gestión, información y comunicaciones aplicado a la red eléctrica, es un concepto cuyo objeto es aumentar conectividad, automatización y coordinación entre productores, proveedores y consumidores en la red de distribución, lo que implica que se tienen dos redes en paralelo, una de energía y otra de información. En la **Figura 4** se esquematiza este concepto:

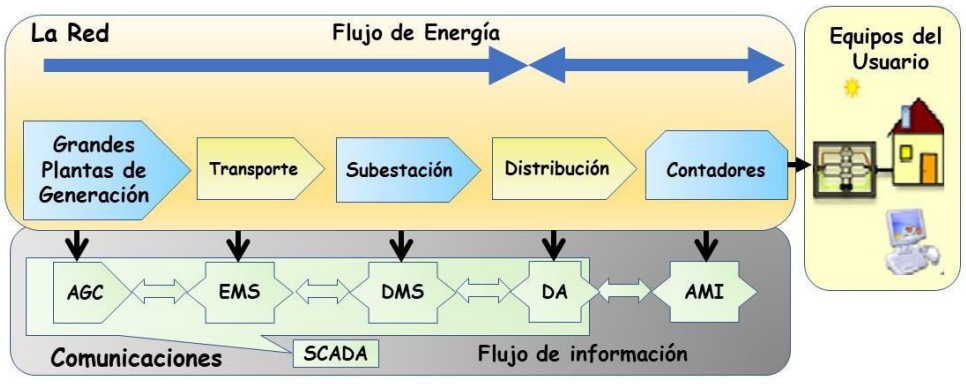

Figura 4: Flujo de Energía de una Red Eléctrica (Fte: Casellas Beneyto et alt. (Casellas Beneyto et al., 2010))

Las siglas señaladas en la parte inferior de la **Figura 4** indican los distintos ***sistemas de información*** requeridos en cada etapa de la red energética:

- AGC: Automatic Generation Control
- EMS: Energy Management System
- SCADA: Supervisory Control and Data Acquisition
- DMS: Distribution Management System
- DA: Distribution Automation
- AMI: Advanced Meter Infrastructure

A los fines del presente trabajo, solo se abordará este último sistema de información: el que conecta a la empresa de distribución con el domicilio del consumidor final de la energía.

Particularmente interesa el ***meter o contador de energía,*** que los autores del texto citado describen claramente en la **Figura 5**:

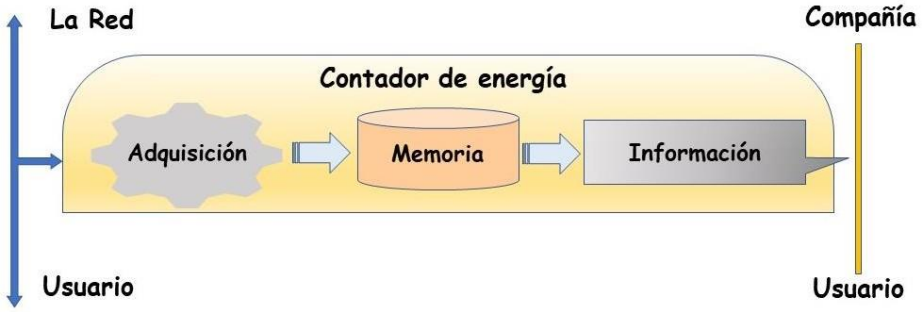

Figura 5: Estructura de un Contador de Energía (Fte. Casellas Beneyto et alt. [31])

De los diferentes tipos de contadores de energía, interesa el *Smart Meter*, estos equipos proporcionan al centro de gestión, la información y el control de los parámetros de calidad y de programación del servicio junto con la actualización del software de medición de forma telemática.

Sobre la base de estos primeros conceptos, se presenta el caso de estudio que se abordará: ***Sistema Inteligente para la Captura de Datos de Medidores de Energía Eléctrica (SICaMEe)[8].***

4.2 Descripción de la Arquitectura de Procesamiento

El modelo tecnológico del SICaMEe incluye la aplicación de herramientas de captura de imágenes y algoritmos de Inteligencia Artificial que hagan posible una solución más rápida y económica que las actuales del mercado.

Se propone reemplazar la medición manual del consumo de forma automática y remota, incorporando un ***smart meter*** con la capacidad de capturar una imagen del medidor y reconocer a

[8] Se tomará como caso de estudio el proyecto de "Sistema Inteligente para la Captura de Datos de Medidores de Energía Eléctrica" que resulta de una aplicación directa del Trabajo Final denominado "Sistema de Telemedición de servicios públicos basado en Inteligencia Artificial", de autoría del Ing. Santiago Salamandri, en el marco de la Maestría en Internet de las Cosas del Laboratorio de Sistemas Embebidos de la Universidad Nacional de Buenos Aires. El citado trabajo se encuentra en su etapa final de desarrollo y en resumen consiste en generar un entorno IoT basado en sistemas embebidos e inteligencia artificial, para el monitoreo y captura de datos que servirán de insumo de los consumos de servicios públicos

través de técnicas de Inteligencia Artificial el consumo actual, para luego transmitir esa lectura al servidor a través de una red inalámbrica.

De este modo sería posible obtener la siguiente información sobre el consumo energético:

- Consumo de energía
- Fecha y hora de la medición
- Identificación del domicilio

Considerando estos datos recabados masivamente desde cada uno de los puntos de consumo de energía, sería posible implementar herramientas de analítica de datos y Big Data para que las empresas distribuidoras de energía estudien sus estrategias de gestión:

- Análisis de las demandas de energía según zona y variables estacionales (valores históricos de consumo, clientes de algo/bajo consumo, etc.).
- Análisis de los consumos por período y zona geográfica para programar más ajustadamente las tareas de mantenimiento, cortes de energía, etc.
- Análisis tarifario de los servicios que brinda según distintas tipificaciones (consumo domiciliario/industrial, zonificación urbana/rural, etc.)

El sistema proveerá distintos niveles de usuarios: Administrador del Sistema; Gestor de Datos (personal perteneciente a la empresa distribuidora); Instalador y Consumidor o Usuario final.

Y contará con los componentes de IT necesarios para la captura, transmisión, procesamiento y almacenamiento de los datos capturados. En la **Figura 6** se muestra el modelo conceptual:

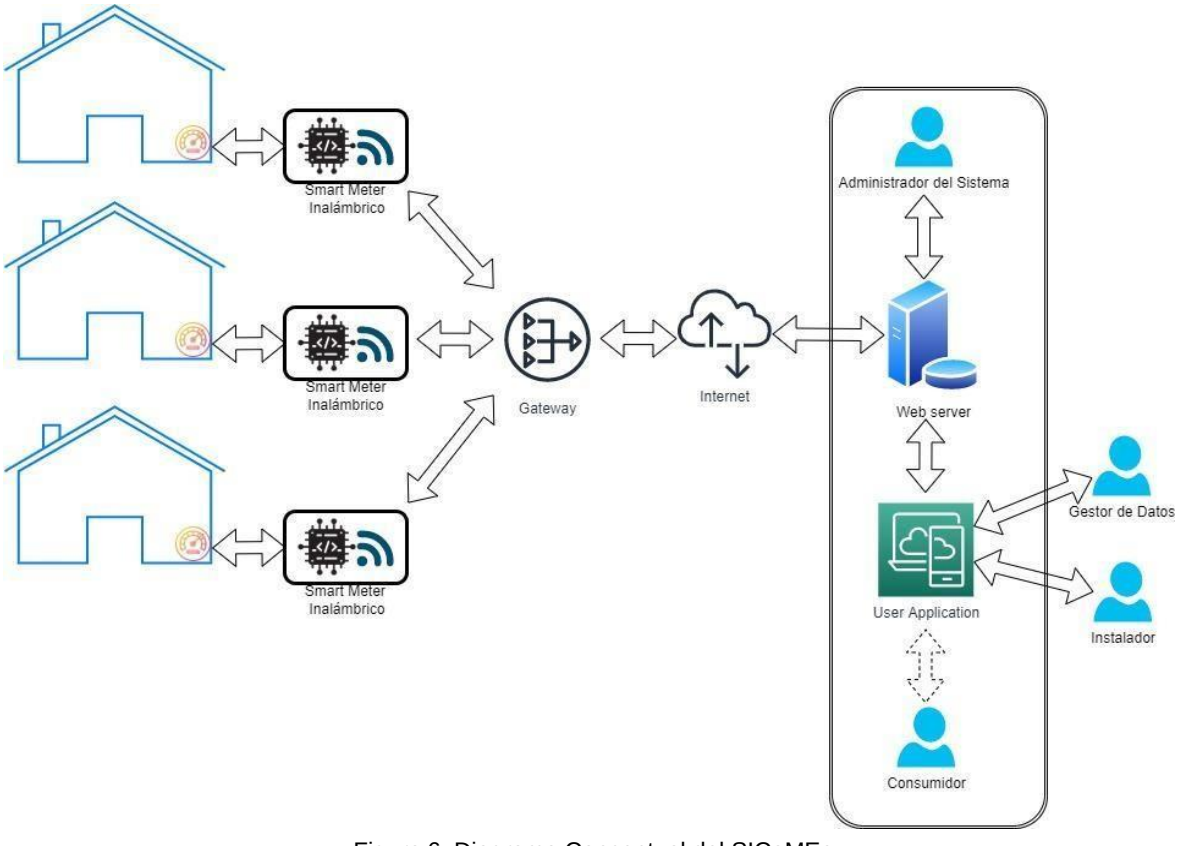

Figura 6: Diagrama Conceptual del SICaMEe

Con otro nivel de detalle, en la **Figura 7** se señala la arquitectura de procesamiento que requerirá el sistema, identificando los componentes de nivel superior, funcionalidades, tecnologías y frameworks requeridos, a la vez que transversalmente se visualizan las capas de: a) captura de datos, b) transmisión y c) procesamiento de estos.

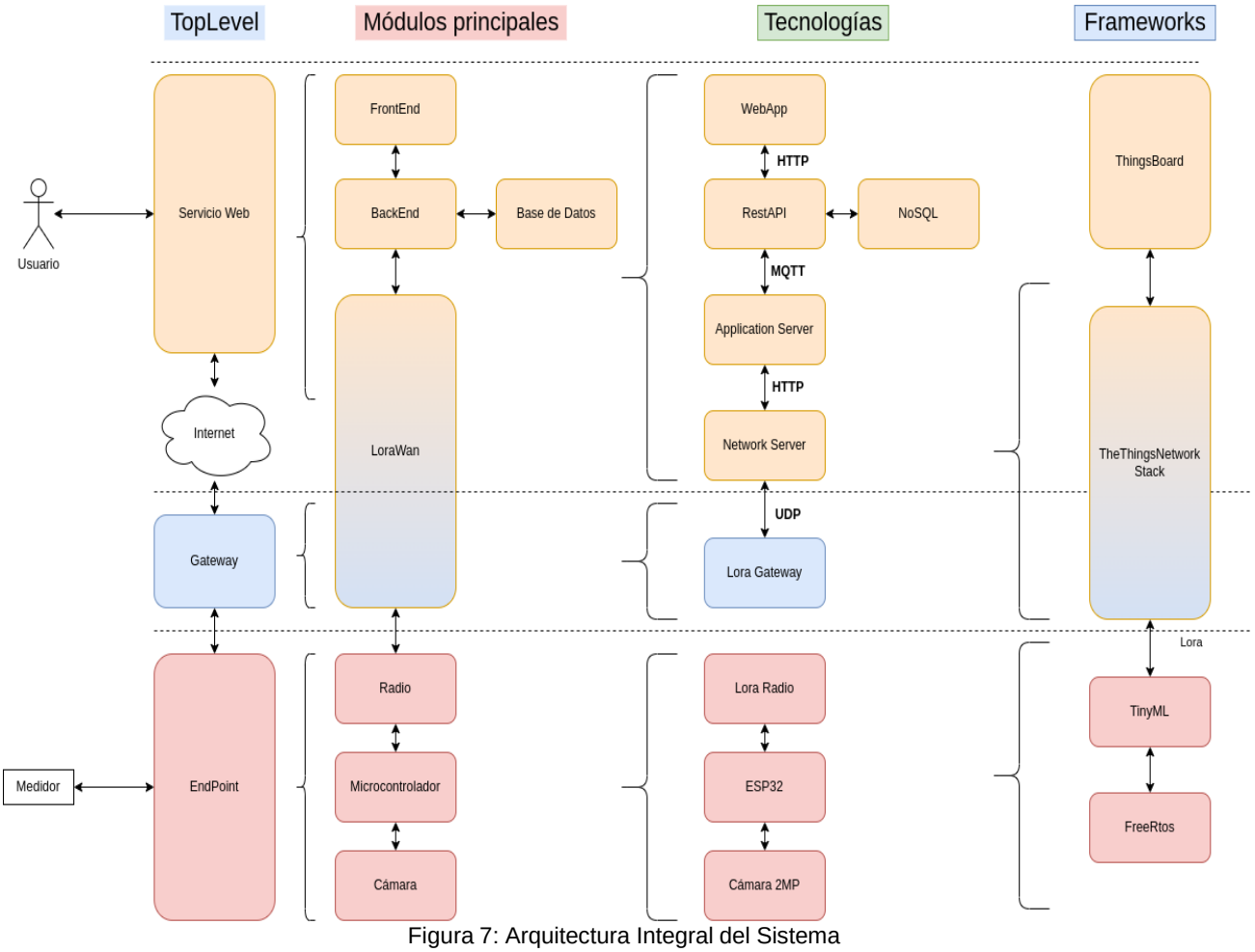

Figura 7: Arquitectura Integral del Sistema

A) Capa de Captura de los Datos

Aquí se incluyen los elementos que generan y procesan los datos que alimentan el sistema.

El ***Medidor*** es el componente primario de emisión de los datos. Es el contador de energía que informa sobre el consumo que se está realizando desde un domicilio. Este medidor interactúa con un sistema ***EndPoint,*** que integra los siguientes componentes:

- La ***cámara*** que actuará como un transductor[9] que capturará las imágenes de los medidores y las enviará al sistema embebido para detectar las mediciones.

[9] Un transductor define como un dispositivo fundamental en el sistema de control de medidores eléctricos. Actualmente, son muy utilizados en los sistemas de automatización y control para registrar grandes magnitudes. Este dispositivo transforma una magnitud física en una señal eléctrica. https://www.aeisa.com.mx/transductor-que-es-y-para-que-sirve/

Se propone utilizar una cámara ultra pequeña modelo OV2640[10] que se encuentra asociada al sistema embebido ESP32. Esta cámara capta las variaciones luz que tiene en frente y las convierte a un formato digital que puede representar la imagen final.

- Un ***microcontrolador*** que será la unidad de procesamiento encargada de recibir las imágenes de la cámara y procesar esos datos mediante un algoritmo de inteligencia artificial que identificará los valores numéricos de consumo de la imagen capturada, y posteriormente los transmitirá por internet.

  Se propone el microcontrolador ***ESP32*** [11] que puede interactuar con otros sistemas para proporcionar funcionalidad Wifi y Bluetooth a través de sus interfases propias, implementando el sistema operativo en tiempo real open source *FreeRTOS*[12], el cual incluye un kernel y un conjunto creciente de bibliotecas de IoT.

  Para el algoritmo de inteligencia artificial se propone utilizar *TinyML*[13] que integra aplicaciones de Machine Learning reducidas y optimizadas para soluciones integradas (hardware, software de base y aplicaciones), y que es posible implementar en sistemas de baja energía como sensores o microcontroladores para realizar tareas automatizadas.

- Una ***radio*** que se utilizará para enviar/recibir paquetes de datos a través de la red inalámbrica, recurriendo para ello al protocolo *LoRa* [14] . Particularmente con los componentes *Lora Transceiver* para transmitir la telemetría hasta Gateway.

  Todo ello complementado con el sistema de alimentación de todos los componentes y el soporte mecánico correspondiente.

B) Capa de Transmisión de Datos

Esta segunda capa se basa en un ***Gateway*** o antena cuya función básica es establecer comunicación entre múltiples entornos.

Este tipo de componente hace posible la conexión entre equipos ubicados en diferentes redes y que se comunican a través de diferentes estándares.

En este modelo, el Gateway actúa como dispositivo encargado de tomar los datos capturados y transportarlos por Internet.

[10] La cámara OV2640 capta las variaciones de luz que tiene enfrente mediante un sensor CCD que convierte cada pixel de la imagen en datos digitales binarios, por lo que se interpreta que la cámara funciona como un transductor. https://www.uctronics.com/download/cam_module/OV2640DS.pdf

[11] El módulo ESP32 es una solución de Wi-Fi/Bluetooth todo en uno, integrada y certificada que proporciona no solo la radio inalámbrica, sino también un procesador integrado con interfaces para conectarse con varios periféricos. Es programable en PHP, JAVA, C, C++.

[12] https://www.freertos.org/

[13] https://www.tinyml.org/

[14] *LoRa* es una tecnología de modulación de radio frecuencia para redes de área amplia de baja potencia. Al ejecutarse en frecuencias no licenciadas, esta conectividad es específicamente una referencia a los casos de uso de IoT que requieren energía ultra baja para enlaces de datos de rango extremadamente largo. Por ejemplo: hasta tres millas (cinco kilómetros) en áreas urbanas y hasta 10 millas (15 kilómetros) o más en áreas rurales (línea de visión). https://lora-alliance.org/

Para el caso de uso considerado se propone implementar tecnología ***LoRaWAN***[15], que mediante una topología de estrella vincula los dispositivos de un extremo de la red, con los servidores de la red central, para la transmisión de los mensajes entre ambos extremos.

De esta forma se conformaría una red de IoT integrada a *TheThingsNetwork*[16], red de comunidades que construye una red global a través de tecnología *LoRa*.

C) Capa de Procesamiento de Datos

El centro de esta capa será el ***Servicio Web*** que se encargará de la gestión de los datos, tanto como del ingreso de los datos capturados por el EndPoint como de las interfaces de comunicación de los distintos usuarios del sistema.

El ***BackEnd*** de este servicio estará integrado por la aplicación informática que responderá a las reglas del negocio, definidas de acuerdo con las funcionalidades que el sistema le entregará a cada tipo de usuario.

Por otra parte, el ***FrontEnd*** constará de las interfases de comunicación necesarias para los usuarios del sistema, y contará con todas las funcionalidades aportadas por ***WebApp,*** aplicaciones híbridas que conjugan la operatividad de las aplicaciones web nativas y de las aplicaciones para dispositivos móviles. Más los componentes ***Application Server*** y ***Network Server*** requeridos para la interconexión con la tecnología LoRa y ***API Rest,*** necesarios para acotar las solicitudes HTTP a los requerimientos de la arquitectura.

Para completar esta capa, se incluye una base de datos bajo el modelo ***NoSQL*** que brinda como ventajas que se ejecutan en máquinas de bajos recursos de procesamiento, tienen una escalabilidad horizontal que mejora el rendimiento mediante el agregado de nodos y manejan grandes volúmenes de datos.

Todos estos componentes se pueden implementar desde la plataforma *ThingsBoard* [17], servicio open source para la gestión de dispositivos, recopilación, procesamiento y visualización de datos para soluciones de IoT.

4.3 Grado de Avance del Proyecto

A la fecha, el proyecto descripto en este caso de estudio se encuentra en etapa de diseño preliminar. Se está a la espera de las instancias de prototipación o pruebas de concepto necesarias, que ayudarán en el ajuste de las ideas inicialmente formuladas, tanto en la definición de las funcionalidades del sistema en general, como en la factibilidad de utilización de las tecnologías y frameworks señalados.

[15] *LoRaWAN* es un protocolo de red de área amplia de baja potencia, construido sobre la red inalámbrica LoRa, que admite penetración interior profunda de largo alcance, bajo costo, móvil, de bajo consumo energético y comunicación bidireccional segura de extremo a extremo para aplicaciones de Internet de las cosas (IoT) y máquina a máquina (M2M). https://lora-alliance.org/

[16] https://www.thethingsnetwork.org/

[17] https://thingsboard.io/

Capítulo 5. Propuesta de Análisis Forense del Caso de Estudio

En breve síntesis, esta sección compendia la *Guía para el Análisis Forense de Entornos IoT* descripta en el Capítulo 3, con el caso de estudio sobre *SICaMEe* descripto en el Capítulo 4Capítulo 3, sobre el cual se supone que actúa alguno de los ataques mencionados en el Capítulo 2.

5.1 Aplicación de GAFIoT al Caso de Estudio

Considerando las fases de GAFIoT definidas en la sección 3.5 se describen a continuación como se aplicarían en el caso de estudio de SICaMEe. Es importante considerar que, a los fines del presente trabajo, se ***propone un escenario supuesto*** en el que el proyecto estuviera ya desarrollado e implementado, y hubiera sufrido un ataque a la seguridad del sistema.

Conviene recordar las fases de GAFIoT a partir del gráfico que se muestra en **Figura 8**:

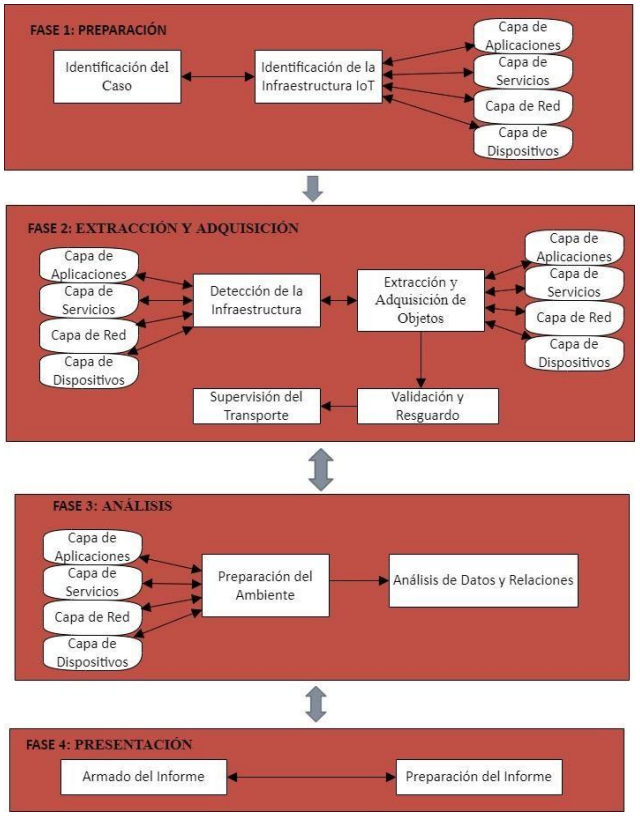

Figura 8: Fases de la Metodología GAFIoT

5.1.1 Fase de Relevamiento

Esta fase comprende dos actividades principales: Identificación del Caso e Identificación de la Infraestructura IoT.

- ***Identificación del Caso***

Supuesto un ataque al SICaMEe y que el propietario de este convoca a un analista forense para identificar el incidente ocurrido, se definen los siguientes aspectos:

  - Entrevista con los usuarios responsable del sistema para revisar la documentación legal, administrativa, de seguridad física y lógica del caso

- Definición de la narrativa general del ataque en la que se señala cómo se identificó, cual es el perjuicio generado y el grado de compromiso del sistema.
- Definición de una estrategia inicial para enfrentar el caso, con énfasis en el objetivo final del análisis forense

Como resultado de estas acciones se obtienen la siguiente información:

1) El SICaMEe fue atacado externamente por técnicas que en un primer momento no se pueden establecer, serán motivo de identificación.
2) De una primera revisión del sistema y de las entrevistas a los usuarios, se han encontrado aplicaciones sospechosas con metadatos indicativos de que se instalaron en fechas coincidentes a la aparición de otras anomalías:
    a. Se observó un funcionamiento de la red más lento que lo normal, es decir, habría una merma notoria en la velocidad de transmisión de los datos en la red IoT.
    b. Al reiniciarse el servicio web, se observa una demora también superior a la normal, como si hubiera procesos inusuales que demora la iniciación del servicio.
    c. En los sistemas de comunicación interna (correo electrónico y mensajería instantánea), los usuarios detectaron un incremento en la cantidad de mensajes de spam y anuncios publicitarios que habitualmente no aparecían.
3) El SICaMEe cuenta con un sistema básico de seguridad informática sostenido en lineamientos muy generales (acceso restringido por roles de usuario, mantiene las políticas de seguridad preexistentes de fábrica para los componentes, no cuenta con un responsable dedicado a la gestión de la seguridad informática).
4) El SICaMEe permaneció inactivo por un determinado tiempo, y se debió resetear todo el sistema y los dispositivos IoT para reiniciar su funcionamiento.
5) La pérdida de datos ocurrió, pero se estima como mínima debido a la periodicidad de los backups que mantienen resguardadas las bases de datos cada 24 hs.
6) El usuario propone como objetivos del análisis forense:
    a. Identificar el tipo de ataque ocurrido
    b. Identificar las vulnerabilidades técnicas y operativas del SICaMEe que posibilitaron el ingreso del atacante
    c. Orientar el análisis forense al estudio del ataque y no a una demanda judicial, ya que no se promoverán acciones legales contra el atacante.
    d. Obtener un conjunto de recomendaciones orientativas para mejorar la seguridad de todo el sistema

- ***Identificación de la Infraestructura IT***

La actividad de Identificación de la Infraestructura IT permite entender cuál es el entorno tecnológico en el que se trabajará.

Cuando se trata de entornos IoT, esta actividad se realiza en base al modelo de 4 capas antes descripto, y que se describen a continuación para el sistema SICaMEe:

a) **Capa de aplicación**: conformada por un servicio web que permite la interacción de todo el sistema con los diferentes roles de usuarios: administrador de los datos, gestor de datos, instalador y consumidor final. Cuenta con la funcionalidad necesaria para:

   - Administración de usuarios: altas, bajas, modificaciones y listadores de datos de usuarios y asignación de permisos de acceso
   - Administración de medidores: altas, bajas, modificaciones y listadores de datos del medidor y su ubicación geolocalizada
   - Administración de consumidores finales: altas, bajas, modificaciones y listadores de datos de los propietarios a quienes se brinda el servicio de electricidad domiciliaria
   - Acceso a herramientas analíticas basadas en cubos multidimensionales ad-hoc que genera el usuario autorizado según el rol que cumple (administrador de datos, gestor de datos o consumidor final).

   Se trata de una plataforma híbrida tipo WebApp, con acceso desde una PC o dispositivos móviles, desarrollada mediante *Thingsboard* [18] que permite definir las funcionalidades de backend y frontend del sistema.

b) **Capa de apoyo a servicios y aplicaciones:** el sistema cuenta con:

   - El sistema embebido inteligente para el procesamiento de los datos, fue desarrollado en C++, utilizando la plataforma de prototipado *Arduino*[19], y utilizando *MongoDB*[20] para el almacenamiento de los datos que se procesan. Más los componentes *Application Server* y *Network Server* requeridos para la interconexión con la tecnología IoT.
   - Para el desarrollo del software se utiliza el servicio SaaS de *GitHub*[21].
   - Se debe considerar además los servicios y aplicaciones residentes en los equipos del usuario final (PC y dispositivos móviles).

c) **Capa de Red:** basada en un Gateway, se arma una red de IoT de topología de estrella utilizando la tecnología *LoRaWan,* con la intervención de otros módulos de la tecnología LoRa para vincular los dispositivos IoT con el Gateway y éstos con el servidor de procesamiento mediante LoRa NetServer.

d) **Capa de dispositivos:** es el *Smart Meter* que en este caso está diseñado como un sistema ***EndPoint*** que integra un microcontrolador ESP32, con una cámara ultra pequeña modelo OV2640, y con protocolos de comunicación del módulo de LoRa radio, para comunicarse con el Gateway.

Tambien se identificó:

[18] https://thingsboard.io/

[19] https://www.arduino.cc/

[20] https://www.mongodb.com/

[21] https://github.com/

- ***Capacidad de gestión:*** se trata de las funcionalidades para congeniar la actuación de todos los componentes IoT con los usuarios, y se encuentran descriptas en el servicio web descripto como capa de aplicación.
- ***Capa de seguridad:*** en este sentido, el sistema solo mantiene las instancias de seguridad heredadas de los propios dispositivos IoT, y las configuraciones de las tecnologías LoRa muy básicas definidas por el administrador de los datos.

5.1.2 Fase de Extracción y Adquisición

Por las características del SICaMEe, se decidió visitar las instalaciones del comitente del servicio forense y desde allí acceder a los diversos componentes del sistema en la búsqueda de evidencia del supuesto ataque perpetrado.

Las tareas recomendadas por la metodología GAFIoT son las siguientes: Detección de la Infraestructura, Extracción y Adquisición de Objetos, Validación y Resguardo, y Supervisión del Transporte.

- ***Detección de la Infraestructura***

Se procede a observar las instalaciones, e identificar los elementos de interés:

  - Sobre la capa de aplicación: consola de comando del sistema; componentes tecnológicos físicamente ubicados en ese lugar; distribución del cableado estructurado de los componentes remotos, etc. Servicio web accedido por los restantes usuarios con identificación de las funcionalidades habilitadas a cada rol.
  - Sobre la capa de dispositivos: observación visual in situ en el domicilio de alguno de los consumidores del servicio.
  - Sobre las capas de red y de servicio: identificación del servicio SaaS consumido y recursos distribuidos que quedan bajo responsabilidad del usuario y los que quedan bajo responsabilidad del servicio SaaS contratado.
  - Sobre las capacidades de gestión y seguridad: se toma nota de la documentación que formaliza las políticas de seguridad; procedimientos de asignación de usuarios, accesos y roles; procedimientos de resguardo y recuperación de datos.

- ***Extracción y Adquisición***

En este punto del caso de estudio, y bajo el escenario supuesto de que el SICaMEe ya se encuentra implementado y en pleno funcionamiento, la extracción de la evidencia debe realizarse “en caliente”, con el sistema en pleno funcionamiento, ya sea accediendo al propio espacio web de la aplicación y/o a los propios dispositivos IoT que se utilizan. Y a la vez que, al recolectarla, se deben aplicar las actividades de preservación necesarias mediante la generación de imágenes forenses de los archivos encontrados.

En base al diagnóstico inicial, en la que se identificaron situaciones que hacen sospechar como se realizó el ataque y cuáles son los componentes que estuvieron involucrados, se genera una

estrategia para proceder a la extracción y adquisición de la evidencia, considerando el modelo de referencia de IoT de las cuatro capas, y las actividades que en ese sentido se proponen en GAFIoT:

a) ***Capa de aplicación:*** será necesario analizar el dispositivo en el que se encontró la aplicación sospechosa, así como el resto de los componentes que cuenten con discos y/o memorias persistentes: servidores de correo, servidores de gestión documental, computadoras de escritorio, notebooks y dispositivos móviles de los usuarios.

   El análisis de memorias persistentes puede realizarse con un conjunto de herramientas forense conocidas. Para este tipo de evidencia, el catálogo de NIST[22] incluye 10 herramientas registradas a la fecha, algunas de uso libre, y las identifica según diferentes variables (tipo de sistema operativo, de estructura de archivos, etc.). Se citan algunas:

   - *FTK Imager*[23]: es una herramienta de visualización y vista previa de datos que permite evaluar rápidamente el contenido de una memoria persistente (discos, pen drive, etc.) para determinar si se justifica un análisis adicional.
   - *Smart* [24] : permite detectar todos los dispositivos de almacenamiento conectados a un computador, su estructura lógica (particionamiento) y demás características (marca, modelo, capacidad y serial).
   - *ILook* [25] : permite extraer y analizar imágenes digitales de medios de almacenamiento, analizar cabeceras de archivos para validación real de tipo de archivos y cuenta con un editor hexadecimal integrado.
   - También puede recurrirse al *carving de archivos*[26], para reconstruir el objeto lógico a partir de una captura de datos masiva obtenida de una copia imagen del dispositivo o un volcado de memoria RAM.

   Es posible que sea necesario utilizar una o varias de estas herramientas, dependiendo de las evidencias que se vayan encontrando durante la revisión de la capa de aplicación.

b) ***Capa de apoyo a servicios y aplicaciones*****:** se debe analizar el espacio destinado a esta capa, en la que se utilizan distintos espacios y componentes: GitHub y MongoDB para las aplicaciones; y Windows y Android para los equipos del usuario final.

   Aunque no se encontraron herramientas específicas para el análisis forense del servicio de GitHub, NIST tiene registros de 8 herramientas para el abordaje de espacios como Dropbox, Flickr, Google Drive / Google Docs, Amazon S3, entre otros. Se puede trabajar con el contenido de GitHub analizando los metadatos y los timestamp de los archivos contenidos en este espacio.

[22] https://toolcatalog.nist.gov/search/index.php

[23] https://accessdata.com/product-download/ftk-imager-version-4-2-1

[24] http://www.asrdata.com/forensic-software/our-software/

[25] http://www.ilook.com/

[26] Técnica de recuperación y reconstrucción del contenido de archivos accediendo directamente al almacenamiento en bloque de memoria, salteando la utilización de los metadatos del sistema de archivos.

Particularmente, para el análisis de las bases de datos MongoDB no existen todavía herramientas específicas que aborden las estructuras de datos NoSQL, pero como el acceso a la base de datos de SICaMEe está asegurada ya que el propietario es el interesado en averiguar hasta donde impactó el ataque, es posible utilizar las estrategias de Forensia de Bases de Datos propuestas por Gioia (Gioia, 2019): utilizar las herramientas de auditoría que provee el propio motor, definir triggers y código de consultas que permitan filtrar y obtener datos que puedan resultar espurios.

Respecto de los equipos PC utilizados por los usuarios, son de mucha ayuda los *registros internos* de los servicios, así como las memorias caché disponibles. Es posible utilizar herramientas forenses como *Volatility*[27] muy útil para analizar memorias volátiles, o revisar los registros internos con *Windows Registry Recovery* [28] . El catálogo de NIST incluye 17 herramientas registradas para el análisis y captura de datos en memorias volátiles.

Por último, los dispositivos móviles pueden revisarse mediante dos técnicas habituales: extracción lógica y extracción física. Pero en este caso particular, no se necesita el análisis forense que regularmente se realiza sobre los dispositivos móviles para obtención de contactos, llamadas, mensajes de textos, etc. Por el tipo de ataque que se estima ocurrió, el análisis se debe dirigir a la memoria persistente y volátil de estos dispositivos, recurriendo a las herramientas previamente citadas mediante la conexión del aparato a una PC u otro dispositivo que permita acceder al mismo para revisar los espacios de memoria persistente y volátil.

No obstante, si fuera necesario acceder al contenido de los datos vinculados a las distintas aplicaciones particularmente las redes sociales (¿por allí entró el malware?), hay muchas herramientas forenses disponibles. Si bien NIST tiene registradas 35 herramientas destinadas a la extracción de datos y revisión de dispositivos móviles, la mayoría son propietarias, pero existe un conjunto de herramientas de uso libre -con mayor/menor potencialidad- que se pueden utilizar para este caso. La propuesta de (Martínez, 2016) incluye algunas de ellas:

- *Android Data Extractor Lite (ADEL)*[29] es una herramienta desarrollada en Python que permite obtener un flujograma forense a partir de las bases de datos del dispositivo móvil.
- *AFLogical OSE - Open source Android Forensics app and framework* es una aplicación en formato APK que debe ser previamente instalada en el terminal Android. Permite extraer información variada a la tarjeta SD (registro de llamadas, listado de contactos y de aplicaciones instaladas, mensajes de texto y multimedia).

c) ***Capa de Red***: en esta capa el análisis forense debería centrarse en el Gateway y en la infraestructura de red utilizada para la transmisión, es decir, los protocolos LoRa y LoRaWan.

Aquí se recurre a técnicas de *Sniffing*[30] para acceder a la red e identificar eventos anómalos. Entre las herramientas disponibles para esta técnica podemos citar *NetworkMiner* [31] o

[27] https://www.volatilityfoundation.org/

[28] http://qwww.mitec.cz/wrr.html

[29] https://forensics.spreitzenbarth.de/adel/

[30] Técnica que permite supervisar el tráfico de red en tiempo real y capturar los paquetes de datos que entran y salen del equipo.

[31] https://www.netresec.com/?page=networkminer

WireShark[32]. Para el análisis de la comunicación WiFi, se puede recurrir a herramientas como *WiFi Pineapple*[33].

Si la infraestructura de comunicación tuviera cierta complejidad, se puede recurrir a herramientas *Triage*[34], tales como: *AD TRIAGE*[35], *TRIAGE INVESTIGATOR*[36], *W4*[37] o *SPECTOR*[38].

d) ***Capa de dispositivos IoT:*** en particular, el sistema SICaMEe utiliza un EndPoint basado en el microcontrolador ESP32-S Wi-Fi+BT SoC Module. El datasheet[39] de ese dispositivo menciona que cuenta con tres memorias:

- *Memoria ROM*: que almacena los códigos que manejan la pila Bluetooth, el control de la capa física de la Wifi, algunas rutinas de propósito general y el cargador de arranque (bootloader) para iniciar el código de la memoria externa.
- *Memoria SRAM*[40]: esta memoria, de 520 Kb en este modelo, es utilizada por el procesador para almacenar tanto datos como instrucciones. Su ventaja es que, para el procesador, es mucho más fácil acceder a esta que a la SRAM externa.
- *Memoria SPI Flash*: memoria externa tipo utilizada para almacenar el código de la aplicación.

Siempre que sea posible, el proceso de adquisición de datos debería enfocarse recurriendo a herramientas tradicionales de volcado de memoria. Podría realizarse la imagen forense utilizando la técnica de *CrashDump*[41] y proceder al volcado de la misma con herramientas como Volatility.

El microcontrolador ESP32-S Wi-Fi+BT SoC Module utiliza la memoria SPI Flash para almacenar la aplicación, la cual se ejecuta utilizando también la memoria SRAM. Cuenta con un módulo OTP[42] donde se almacenan las claves de cifrado del contenido de la SPI Flash o los certificados digitales con sus claves privadas. Bajo esta tecnología, realizar un volcado de memoria no generaría resultados legibles. Para acceder a la memoria SPI Flash es necesario tener acceso físico al chip, conectar los pines correspondientes y aplicar los comandos SPI necesarios para obtener el contenido de toda la memoria.

---

[32] https://www.wireshark.org/

[33] https://shop.hak5.org/products/wifi-pineapple. En realidad, son equipos para realizar auditorías de redes WiFi.

[34] Desde la Ciberseguridad, se define *Triage* como el proceso para categorizar las amenazas durante la respuesta a incidentes e identificar qué eventos deben tratarse primero en función de su gravedad y los recursos disponibles.

[35] https://digitalforensicsdubai.com/product/ad-triage/

[36] https://www.adfsolutions.com/triage-investigator

[37] https://www.vound-software.com/

[38] https://www.cclsolutionsgroup.com/products/spektor

[39] https://modtronix.com/mx-m/esp32/esp32-s-ai_datasheet.pdf

[40] SRAM: memoria de acceso aleatorio estático. Proporciona baja latencia y acceso a datos de alta velocidad. Es una tecnología de memoria volátil, lo que significa que sus datos se pierden cuando se apaga la energía

[41] CrashDump: Forzar un malfuncionamiento del sistema operativo para que él mismo genere una copia de la memoria principal

[42] OTP (On Time Password) es una contraseña que pierde su validez después de su uso, de ahí su denominación. Por lo general, se emplea como parte de una autenticación de doble factor y para trabajar con claves sensibles de forma segura.

Respecto de la ***Adquisición***, en todos los casos en que se recolecta una evidencia conviene resguardarla debidamente haciendo una copia forense de la misma. Para esto se puede utilizar las funciones que en tal sentido ya vienen incorporadas en algunas de las herramientas nombradas o bien, se puede recurrir a alguna de las 31 herramientas registradas en el catálogo de NIST, que abarcan dispositivos con diversos sistemas operativos (Windows, Linux, standalone, etc.), diferentes estructuras internas (discos SATA/SCI/IDE, dispositivos USB, tarjetas SD, etc.) y mediante algoritmos de encriptación habituales (MD5, SHA1, SHA2-256, SHA2-512, SHA3-256, SHA3-512).

- ***Validación y Resguardo***

El caso que nos ocupa no requiere del registro en una cadena de custodia, pero sí se debe documentar de manera ordenada la evidencia recolectada, a fin de que el antecedente del incidente de seguridad se pueda analizar y comparar si hubiera otros ataques futuros.

Será necesario identificar debidamente cada evidencia señalando el conjunto de datos que la diferencie: id de identificación, descripción, componente/dispositivo en el que se encontró, metadatos de la evidencia, fecha y hora de la extracción y adquisición, código hash de la imagen forense, entre otros datos de interés.

- ***Supervisión del transporte***

En este caso la evidencia recolectada será entregada al comitente, por lo que no será necesario definir ningún aspecto particular referida a esta actividad.

5.1.3 Fase de Análisis

GAFIoT propone dos actividades en esta tercera fase: Preparación del Ambiente y Análisis de Datos y Relaciones.

- ***Preparación del Ambiente***

Esta fase es genérica para cualquier tipo de evidencia que se debe analizar y se refiere a la preparación del laboratorio forense en el cual se procederá a revisar las evidencias recolectadas.

Las tareas requeridas incluyen la restauración y validación de las imágenes forenses obtenidas, la selección de las herramientas más adecuadas para el tipo de evidencia, así como la elección de las metodologías, técnicas o guías procedimentales correspondientes.

Para el caso de estudio del SICaMEe, esta fase no se requiere específicamente, salvo que hubiera necesidad de simular un contexto idéntico al del sistema para realizar pruebas e identificar con mayor precisión la mecánica de desarrollo del ataque a las instalaciones.

- ***Análisis de Datos y Relaciones***

Se deben desarrollar las actividades relacionadas con el ***Análisis de las evidencias*** encontradas, a fin de responder a los requerimientos del cliente.

Recordemos que entre los objetivos planteados por el comitente al solicitar el servicio de análisis forense pidió "*Identificar el tipo de ataque ocurrido*". Para dar una respuesta apropiada, el analista forense se enfoca en el análisis integrado y conjunto de todas las evidencias recolectadas, para llegar una estimación de los hechos ocurridos.

Durante la fase de adquisición se observó que los usuarios habían encontrado "*aplicaciones sospechosas con metadatos indicativos de que se instalaron en fechas coincidentes a la aparición de otras anomalías".* Y durante la recolección de evidencias en las distintas memorias volátiles se encontraron archivos coincidentes con la estructura y contenido de bots tipo *Mirai*[43].

La botnet Mirai es considerada la botnet más grande de la historia, que contiene una gran cantidad de dispositivos IoT comprometidos. Para obtener acceso al dispositivo, Mirai emplea más de 60 combinaciones diferentes de credenciales de usuario predeterminadas, que se divulgan públicamente. Utilizando este diccionario aplica técnicas de fuerza bruta hasta que logra ingresar al dispositivo. Una vez que captura un dispositivo IoT, lo integra a su red botnet y avanza sobre el espacio de direcciones IPv4 del primer dispositivo capturado, y escanea todo el especto encontrando nuevos dispositivos vulnerables para sumarlos a su botnet.

Debido a que este bots inicia el ataque en la comunicación TELNET establecida entre los dispositivos IoT y su sistema IoT, se aprovecha de la escasa seguridad en la definición de las credenciales de acceso originales de fábrica de estos dispositivos, que en muchos casos los usuarios no las modifican durante la integración de estos dispositivos a su sistema IoT.

Podemos sumar esta característica al escenario supuesto de implementación del sistema SICaMEe, asumiendo que, al implementarlo, se mantuvieron las credenciales de fábrica de los dispositivos EST32, con lo cual éstos sirvieron de boca de entrada para el bots.

Habiendo identificado esta supuesta primera boca de acceso del atacante, se debe analizar los restantes componentes para identificar el impacto del ataque en todo el sistema IoT. De esta forma se podría encontrar que:

- El análisis forense de todo el sistema SICaMEe, en cuanto a las memorias persistentes y volátiles, han generado evidencia que podría indicar hasta donde avanzó el bots en su búsqueda de componentes vulnerables para sumar a su botnet.
- Estableciendo líneas de tiempo con los metadatos de las evidencias encontradas podría identificarse el recorrido realizado por el bots.

5.1.4 Fase de Presentación

En esta última fase, GAFIoT incluye dos actividades: Armado del Informe y Presentación del Informe.

- ***Armado del Informe***

Por sí mismo, el Informe debe dar respuesta a los objetivos planteados por el comitente:

a) Identificar el tipo de ataque ocurrido

[43] El código fuente de Mirai fue liberado en un foro e incluso está publicado en GitHub, y de él se derivaron otros bots más agresivos como Reaper, Okiru, Satori, Masuta, etc. Consultado en https://empresas.blogthinkbig.com/darlloz-mirai-botnets-iot-ciberseguridad/

b) Identificar las vulnerabilidades técnicas y operativas del SICaMEe que posibilitaron el ingreso del atacante

c) Orientar el análisis forense al estudio del ataque y no a una demanda judicial, ya que no se promoverán acciones legales contra el atacante.

En el caso que nos ocupa el informe debe enfocarse de manera integral, considerando todos los componentes del entorno IoT:

- ***Software:*** debe incluir el impacto del ataque en el código de los sistemas de aplicación de SICaMEe, en los sistemas operativos de los dispositivos involucrados, sean éstos los utilizados por el usuario final, como los que integran la arquitectura de procesamiento (servidores varios), de conectividad (Gateway) y los propios dispositivos IoT (Smart Meter en este caso).
- ***Hardware:*** toda la infraestructura tecnológica afectada por el ataque debe identificarse con claridad, incluso con mención de cada componente y el grado de impacto recibido.
- ***Estructuras de datos:*** se deben señalar la/s base/s de datos que fueron comprometidas, así como los reservorios de archivos documentales de los usuarios de SICaMEe que pudieran haber sido contaminados.
- ***Conectividad:*** la infraestructura de comunicaciones debe mostrarse particularmente en cuanto al *camino recorrido* por el bots para expandir la captura de dispositivos, a fin de identificar las rutas débiles que fueron aprovechadas para la contaminación del sistema.
- ***Comunicación con el usuario:*** en este apartado se debe enunciar el comportamiento del usuario, en términos de la cultura de la seguridad que tuvo, y las responsabilidades frente al hecho.
- ***Seguridad Informática:*** usualmente aquí es en donde se pueden encontrar las causas finales del acceso indebido a SICaMEe, y es importante destacar las técnicas y elementos de seguridad vigentes al momento del ataque para medir el grado de defensa de todo el sistema en esa situación inicial.

Los seis componentes precitados permitirán ordenar el Informe para concluir en la respuesta a los objetivos planteados para el análisis forense.

- ***Preparación del Informe***

Esta actividad será la conclusión del análisis forense, mediante la entrega de los soportes digitales y documentales de toda la actividad realizada en torno a SICaMEe: entrevistas con los usuarios, relevamientos documentados, evidencia recolectada, técnicas y herramientas forenses utilizadas, anexos técnicos y cualquier otra documentación que sostenga las conclusiones arribadas por el analista forense.

Para el caso de estudio, es importante incluir también diagramas, esquemas o modelos técnicos necesarios para explicar cómo ocurrió el incidente de seguridad en SICaMEe.

Capítulo 6. Recomendaciones de Seguridad para SICaMEe

En el caso de estudio analizado en este trabajo, uno de los objetivos propuestos por el comitente al analista forense es "*Obtener un conjunto de recomendaciones orientativas para mejorar la seguridad de todo el sistema*".

Si se consideran las 4 capas del modelo IoT, se pueden efectuar las siguientes recomendaciones de seguridad:

a) Recomendaciones sobre la CAPA DE APLICACIONES:

Siendo que SICaMEe utiliza una aplicación WebApp para comunicación de los usuarios, allí se encuentra el primer punto de entrada que será vulnerable a los ataques según el grado de protección establecida para la interfase de comunicación con los usuarios**.**

Desde este punto de vista, es recomendable implementar un ***Estándar de Verificación de Seguridad de Aplicaciones (ASVS).*** Una de las más utilizadas es la propuesta por OWASP[44], que brinda una base para probar los controles técnicos de seguridad de las aplicaciones web y también proporciona a los desarrolladores una lista de requisitos para un desarrollo seguro.

La verificación de seguridad de aplicaciones no aborda solamente el código mismo de la aplicación, sino todo el espacio de interacción del usuario: la comunicación, los datos y el área de almacenamiento. De ello da prueba el TOP TEN 2021 de OWASP que señala el ranking 2021 de las principales vulnerabilidades de las aplicaciones web:

- A01:2021 – Control de Acceso Vulnerado
- A03:2021 – Inyección de Código
- A04:2021 – Diseño Inseguro
- A05:2021 – Configuración Incorrecta de Seguridad
- A06:2021 – Componentes Vulnerables y Obsoletos
- A07:2021 – Fallas de Identificación y Autenticación
- A08:2021 – Fallas de Integridad de Software y Datos
- A09:2021 – Registros de Seguridad y Fallas de Monitoreo
- A10:2021 – Falsificación de Solicitud del lado del Servidor

b) Recomendaciones sobre la CAPA DE SERVICIOS Y APLICACIONES:

Aquí se debe poner énfasis en la seguridad de los servicios en la nube. Al respecto, el trabajo de (Sailakshmi, 2021) define los *principios de control* que se deben establecer para este tipo de entornos:

1. Los controles deben garantizar que todas las transacciones se procesen y completen de principio a fin;
2. El control necesita asegurar que los datos correctos son procesados dentro de las aplicaciones;

[44] https://owasp.org/www-project-application-security-verification-standard/

3. El control necesita verificar bajo autenticación que los usuarios correctos tienen acceso al sistema apropiado bajo las aplicaciones;
4. Controles que necesitan verificar la autorización de estos usuarios autentificados y los derechos que tienen sobre estos objetos;
5. Controles que validan la integridad de los datos que vienen de la fuente a la aplicación y los datos que se envían de la aplicación a los consumidores de datos posteriores; y
6. Controles que registran las transacciones y los procesos ocurridos durante estas actividades para garantizar que haya suficientes datos para auditar las reclamaciones y también en caso de incidente.

El trabajo del autor citado define además 5 dominios (Usuario de la nube, Aplicación de la nube, Integración de la nube, Datos de la nube y Procesos de la nube) con 20 controles implementados en plataformas AWS, Azure y Google Cloud. Seguramente esta propuesta se puede tomar como modelo para estudiar el alcance de la misma respecto de los servicios en la nube que consume el sistema SICaMEe.

Por otra parte, sería importante establecer un procedimiento ad-hoc para revisar y limpiar todos los dispositivos que cuenten con memorias permanentes, especialmente aquellos utilizados por los usuarios (discos externos, pen drive, espacios compartidos de workflow, etc.).

También sería recomendable revisar los resguardos realizados durante el último tiempo, a fin de evitar el vuelco de datos contaminados sobre el sistema, una vez que este sea depurado totalmente.

c) Recomendaciones sobre la CAPA DE RED:

El modelo de comunicación de SICaMEe utiliza una LoRaWAN como capa de red. Esta tecnología tiene características de seguridad que no comprometerían el sistema con tanta facilidad. En el trabajo de (Buitrago Marquez et al., 2020) se define con todo detalle.

En la **Figura 9** se describe la relación entre los dispositivos IoT, los Gateway, el servidor y las aplicaciones que integran el sistema IoT.

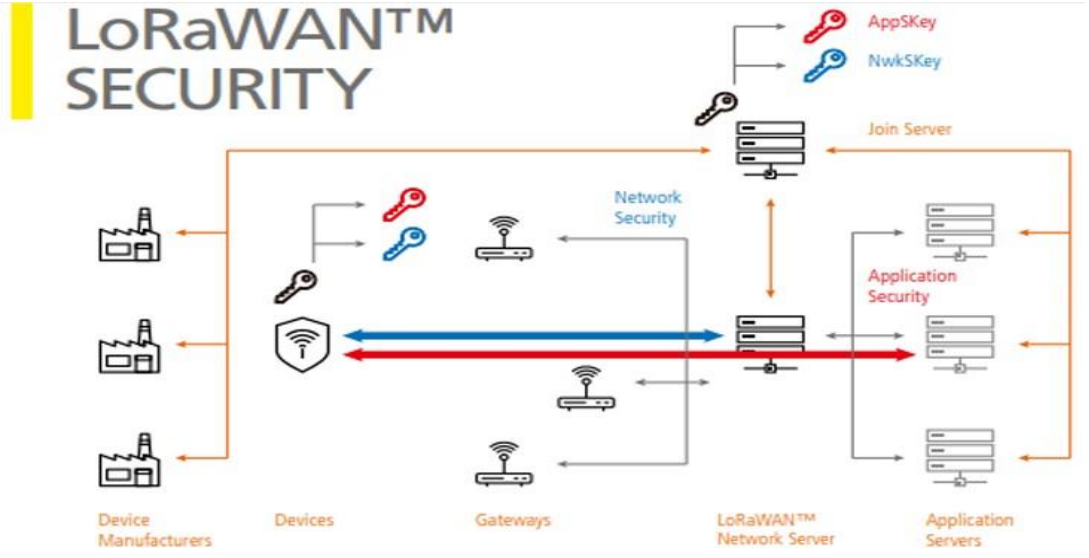

Figura 9: Estructura de Seguridad de una red LoRaWAN (Fte: (Buitrago Marquez et al., 2020))

LoRaWAN utiliza cifrado AES de 128 bits y tiene varias capas independientes de seguridad:

- una clave de sesión de red (NwkSKey),
- una clave de sesión de aplicación (AppSKey),
- una clave de autenticación del dispositivo final (AppKey) más un identificador único global (DevEUI).

Este esquema de seguridad permite acciones de contención y prevención de ataques como las siguientes:

- Cifrado de extremo a extremo: se utiliza una clave de sesión de la aplicación (AppSKey) para cifrar y descifrar la carga útil de la aplicación.
- Distribución de claves de sesión: se generan dos claves de sesión a partir de AppKey, que son AppSKey y NwkSKey. Estas claves se utilizarán para proteger todo el tráfico LoRaWAN.
- Integridad y confidencialidad de los datos: el tráfico de LoRaWAN se protege mediante las dos claves de sesión derivadas. Cada carga útil se cifra mediante AES-CTR y se calcula un código de integridad de mensaje (MIC) con AES-CMAC (para evitar la manipulación de paquetes). La clave de sesión de red (NwkSKey) se utiliza para verificar la autenticidad e integridad de los paquetes y para cifrar los comandos MAC de LoRaWAN y la carga útil de la aplicación.
- DevNonce: el servidor de red registra el DevNonce recibido en el mensaje de "solicitud de unión" para evitar ataques de repetición. Entonces, cuando un atacante transmite la misma "solicitud de unión" una y otra vez que la enviada por el dispositivo final, el servidor se dará cuenta de que el DevNonce ya está en uso y el mensaje proviene de un atacante.
- Contadores de tramas: debido a que se trabaja con un protocolo de radio, cualquiera podrá capturar y recoger los mensajes. No es posible leer estos mensajes sin AppSKey, porque están encriptados. Tampoco es posible manipularlos sin la NwkSKey, porque esto hará que la verificación del MIC falle. Sin embargo, es posible retransmitirlos. Estos llamados ataques de repetición se pueden detectar y bloquear mediante contadores de tramas.
- Cuando se activa un dispositivo, estos contadores de tramas (FCntUp y FCntDown) se establecen en 0. Cada vez que el dispositivo transmite un mensaje de enlace ascendente, el FCntUp se incrementa y cada vez que la red envía un mensaje de enlace descendente, el FCntDown se incrementa. Si el dispositivo o la red reciben un mensaje con un contador de tramas inferior al anterior, el mensaje se ignora.

(Paul Pickering, 2017) menciona dos métodos para implementar las claves en una LoRaWAN:

- Activación mediante personalización (ABP): Aquí, los dispositivos finales LoRaWAN pueden ser programados en fábrica con la información de autenticación para una determinada red LoRaWAN.
- Activación inalámbrica (OTAA): Este utiliza un ID de aplicación, un único ID de dispositivo, y una red de dispositivo asignado para obtener la dirección y NwkSKey AppSKey. Este es el método preferido porque las teclas no están predeterminadas y pueden ser regeneradas.

Obviamente estas funcionalidades serán provechos para la red IoT siempre que se atienda debidamente la asignación de credenciales y accesos de los dispositivos IoT.

d) Recomendaciones sobre la CAPA DE DISPOSITIVOS:

Para esta capa se pueden tomar las recomendaciones señaladas por (Bhatt & Bhushan, 2021):

- Aplicar métodos de control de acceso, derogando las credenciales de fábrica por otras más seguras, ajustadas a los protocolos que en tal sentido se definan desde las políticas de seguridad informática.
- Aplicar técnicas de cifrado ligero El algoritmo de cifrado ligero (también conocido como LEA) es un cifrado de bloques de 128 bits para proporcionar confidencialidad en entornos de alta velocidad como los requeridos por los dispositivos IoT. LEA tiene tres longitudes de clave diferentes: 128, 192 y 256 bits y es más rápido que AES.
- Aplicar técnicas de autenticación de nodos, para garantizar que el servidor de gestión y los recopiladores de datos se comunican entre sí de forma segura.

e) Recomendaciones sobre la CAPACIDAD DE SEGURIDAD:

Por último, como recomendación prioritaria, se sugiere trabajar fuertemente la ***capacidad de seguridad transversal*** del sistema SICaMEe.

Esta cuestión se puede abordar desde la ***Gestión de Riesgos en Ciberseguridad,*** y aplicar alguna de las técnicas o guías de reconocimiento internacional como, por ejemplo:

- La familia de normas ISO/IEC 27000[45] propone un conjunto de herramientas muy apropiadas para mejorar la seguridad informática de entornos IoT, trabajando las siguientes normas:
    - ISO/IEC 27001:2015 Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información, apunta a la conformación de SGSI (Sistema de Gestión de la Seguridad de la Información).
    - ISO/IEC 27002:2017 Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, apunta a la protección de los datos.
    - ISO/IEC 27017:2015 Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.
    - ISO/IEC 27032:2012 Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP).
- El marco de seguridad definido por el NIST, denominado ***Ciber Security Framework (CSF)*** (OEA, 2019)***,*** que consta de tres componentes, siendo el más destacado el ***Framework Core,*** conjunto de actividades y resultados de ciberseguridad deseados, diseñado para permitir la comunicación entre equipos multidisciplinarios mediante el uso de lenguaje simplista y no técnico.

[45] https://www.iso27000.es/iso27000.html

También será importante avanzar en el desarrollo de una ***Cultura de la Seguridad*** entre la comunidad de usuarios que interactúan con SICaMEe, tanto quienes cumplen tareas técnicas como aquellos que actúan como usuarios finales. Para ello son útiles las recomendaciones señaladas en la sección 2.2 La Cultura de la Seguridad Informática.

Capítulo 7. Conclusiones

En términos de los objetivos inicialmente planteados para este Trabajo Final Integrador, se puede concluir que:

- Se mostró la factibilidad de aplicación de la propuesta de Forensia de entornos IoT, para el caso SICaMEe.
- Se analizaron los ataques más comunes a entornos IoT, y se identificaron las vulnerabilidades del sistema SICaMEe, bajo el supuesto de un ataque de botnets.
- Dado que el SICaMEe se encuentra actualmente en etapa de diseño experimental, las recomendaciones propuestas para la mejora de seguridad informática del sistema son atinentes y oportunas, y se dejaron a consideración del equipo de trabajo del proyecto SICaMEe.

Respecto de la metodología GAFIoT, lo realizado hasta aquí marca un camino de crecimiento y fortalecimiento de esta propuesta, ya que la validación con un caso experimental es enriquecedora, aun cuando no se haya llegado a la instancia de implementación en un trabajo de campo.
GAFIoT debe ser validada y aceptada por la comunidad forense, mediante un plan que incluya, entre otras actividades, las siguientes:

- Convocatoria a usuarios expertos para la discusión abierta de la propuesta mediante un esquema colaborativo sistemático y riguroso, que permita recabar las distintas opiniones y enriquecer GAFIoT con críticas constructivas provenientes de quienes serán usuarios finales de la misma. A la fecha, fue presentada en un evento de la comunidad forense (Info-Conf 2021), y se encuentra publicada en una revista internacional (https://cys.cic.ipn.mx/ojs/index.php/CyS/article/view/3898). De estas primeras experiencias ya se recabaron críticas y ajustes a la propuesta original que se ven reflejadas en este Trabajo Final Integrador.
- Aplicación de GAFIoT en casos de usos ya resueltos, para identificar ajustes que podrían mejorarla. Esta actividad también requiere de una planificación formal y sistemática que garantice un proceso de control riguroso.
- Validar con pruebas experimentales de laboratorio las tareas de adquisición y extracción de la evidencia digital de entornos IoT, con herramientas forenses adecuadas al tipo de evidencia y soporte.
- Si bien puede considerarse que la propuesta es abarcativa de los diferentes componentes que pueden encontrarse en un sistema IoT, deberá validarse en otros escenarios forenses más exigentes como, por ejemplo: contextos de seguridad electrónica del hogar o sistemas IoT aplicados a la salud de las personas.

Tanto la propuesta de GAFIoT como el estudio sobre la aplicación de la metodología PURI para realizar el análisis forense de entornos IoT no se agota con el presente trabajo. Es posible generar líneas de continuidad de la investigación, mediante el estudio de:

- Las herramientas forenses para entornos IoT, ya sea que se tomen las existentes y se realicen pruebas de concepto lo suficientemente robustas como para aplicarlas en estos nuevos ambientes, o bien, se propongan nuevas herramientas forenses.

- Las técnicas de recolección y adquisición de probable evidencia digital en los distintos espacios del entorno IoT, con más fuerza en los procesos forenses “en caliente” requeridos para estos casos.
- El estudio de áreas comunes con otras disciplinas como por ejemplo el ecosistema IoT, los sistemas ciberfísicos, la automatización de procesos, que pueden considerarse desde la electrónica y la ingeniería industrial en conjunto con los profesionales de la Informática Forense, sean estos informáticos, abogados o criminalísticos.

Para las cuales puede recurrirse a los espacios de investigación de las instituciones abocadas al desarrollo de la Informática Forense, tales como:

- la Red UNIF (Red Universitaria de Informática Forenses),
- la Red CIIDDI (Red Iberoamericana de Investigadores y Docentes de Derecho e Informática), y
- la propia carrera de Especialización en Informática Forense de UFASTA
- los grupos de I+D+i de los institutos universitarios interesados en estas temáticas.

Por último, vale expresar los beneficios que este trabajo han aportado a la autora, visto desde la propia carrera de Especialización en Informática Forense, entre los que se mencionan:

- El desarrollo de un marco formal, de carácter teórico-práctico, como sostén del análisis forense de la evidencia digital.
- La integración de las experiencias y saberes previos en dicho marco de trabajo, logrando el ordenamiento necesario para un desempeño profesional más adecuado como Especialista en Informática Forense.
- El análisis forense digital como marco de referencia útil para el desarrollo profesional en el ámbito judicial y en los contextos de incidentes de ciberseguridad.

Anexo I. Tipos de Ataques a Entornos IoT

A modo de orden, se toma el trabajo de (Bhatt & Bhushan, 2021), en el que analizan los tipos de ataques a dispositivos IoT más usuales, complementando la descripción con los trabajos de (Humayun et al., 2021), (Angrishi, 2017), (Márquez Díaz, 2019) y (Pandya, 2021). De estas investigaciones se consideran los siguientes tipos de ataques:

- Reconocimiento Inicial
- Ataque Físico
- Ataque de Man-In-The-Middle (MITM)
- Ransomware
- Ataque de Fuerza Bruta
- Botnets
- Ataques de Denegación de Servicios Distribuidos (DDoS)
- Amenazas Persistentes Avanzadas

A continuación, se describen las principales características de cada uno de ellos.

1. Reconocimiento Inicial

Antes de atacar un dispositivo, los ciber atacantes lo investigan, intentando trazar una huella del objetivo y comprender el alcance y profundidad de la seguridad del dispositivo.

Habitualmente el atacante compra el dispositivo IoT en el mercado tecnológico e intenta aplicar ingeniería inversa para que hacer un ataque de prueba del dispositivo.

También es posible que examine el hardware interno y manipule el microcontrolador para vulnerarlo y encontrar información de interés.

El ataque de prueba le permite dimensionar la probabilidad de éxito del ataque.

Cualquier información que se pueda obtener es importante, ya que podría identificar un punto de entrada a la red. Aquí, en el hardware y el software embebido del dispositivo es en donde es posible encontrar las primeras vulnerabilidades del sistema.

2. Ataque Físico

En este tipo de ataque, el intruso obtiene acceso físico al dispositivo IoT propio del sistema. Son dos las técnicas que se pueden utilizar en este tipo de ataque:

- ***Ataques de interrupción***, en los que se apaga la red a la que están conectados los dispositivos y cesan la función o se produce algún daño físico en el dispositivo.
- ***Ataque por inyección de código malicioso, el atacante utiliza inhibidores para bloquear o manipular las señales generadas o utilizadas por el dispositivo.***

Los ataques físicos se utilizan a menudo para identificar las vulnerabilidades del dispositivo en el entorno IoT particular que es de interés de los atacantes.

3. Ataque de Man-In-The-Middle (MITM)

En este tipo de ataque, el intruso se posiciona entre el usuario y una aplicación. El atacante hace esto para espiar o para hacerse pasar por una de las partes.

Esta técnica de ataque es muy utilizada en la capa de red de la arquitectura IoT, y el atacante puede posicionarse entre muchas conexiones diferentes como un servidor o un cliente.

Como habitualmente los dispositivos IoT no tienen implementaciones de seguridad estándar para resistir cualquier tipo de ataque, son más vulnerables a los ataques MITM.

Entre las características distintivas de este tipo de ataque se puede indicar:

- El ataque ocurre "en el medio" de la transmisión, o sea, durante el tráfico que conecta a dos dispositivos, o un dispositivo y un servidor.
- El intruso intercepta los datos que circulan y suplanta la identidad de una de las partes (o ambas) antes de enviarlo al destinatario correspondiente.
- Usualmente los dispositivos de ambos extremos de la comunicación no identifican que están siendo atacados y confían en que se realiza una comunicación normal.

Comúnmente este tipo de ataques sigue esta secuencia de acciones:

1. Se procede a interceptar el tráfico de datos, y para ello pueden utilizarse diversos métodos:
    a. Suplantación de dirección IP: el atacante falsifica la dirección del equipo destino para que el dispositivo que remite lo identifique como destino válido.
    b. Envenenamiento de la caché ARP[46]: El atacante envía mensajes falsificados ARP a la red y consigue vincular su dirección MAC con la dirección IP del dispositivo destino. A partir de ese momento, recibe todo el tráfico que circula desde esa dirección IP.
    c. Suplantación de DNS[47]: por una cuestión de rendimiento, usualmente los servidores y algunos dispositivos guardan en su caché los DNS, si el atacante accede a esa memoria, puede redirigir al usuario a una dirección IP diferente.
2. Luego se descifra los datos interceptados. También hay varios métodos que se pueden aplicar:
    a. Suplantación de certificados HTTPS, para que el navegador interprete un certificado falso como válido y proporcione el acceso.
    b. Vulnerar el navegador en SSL, rompiendo el cifrado por bloques del protocolo SSL.
    c. Secuestrar SSL: consiste en sustituir los enlaces https por http, para que la comunicación entre el dispositivo origen y el atacante sea por http y la comunicación entre el atacante y el dispositivo destino sea por https.

[46] ARP (Address Resolution Protocol) es el Protocolo de Resolución de Dirección, cuya función esencial es encontrar la identificación MAC de un equipo que corresponde a una dirección IP. Los paquetes de datos que se envía a través de TCP/IP necesitan conocer la máscara de subred, la dirección IP y la dirección MAC del dispositivo destino.

[47] DNS (Domain Name System) es un sistema que traduce los nombres de dominios aptos para lectura humana (por ejemplo, www.amazon.com) a direcciones IP aptas para lectura por parte de máquinas (por ejemplo, 192.0.2.44).

d. SSL Stripping: cuando el atacante ya se posicionó como intermediario con alguna de las técnicas ya señaladas, y luego cambia la versión de seguridad de la aplicación (HTTPS) por una versión no segura (HTTP), y recibe los datos descifrados.

También es posible encontrar otros contextos en los que se aplican las mismas técnicas de intercepción de tráfico, tales como:

- ***Ataque Man in the Middle por Wifi***: dirigido principalmente a los usuarios de telefonía móvil, el atacante simula un punto de acceso inalámbrico en una red pública, para que el usuario se conecte al dispositivo del atacante y así entrar como intermediario en su red.
- ***Ataque Man in the Browser:*** en este caso el atacante utiliza un malware que instala en el navegador del usuario, para interceptar toda la información que el usuario intercambia con sitios y servicios web. Generalmente este tipo de ataque tiene mucho éxito cuando los dispositivos no tienen parches de actualización de seguridad.

4. Ransomware

En breve síntesis, se puede decir que un ransomware es un tipo de ataque de malware que se dirige a la información de la computadora de la víctima y encripta o bloquea esta información.

La víctima debe pagar el rescate exigido para recuperar o acceder a sus datos.

Hay dos tipos de ataques:

- *Ransomware bloqueado*: se cifra o bloquea toda la computadora del objetivo y luego exige un rescate por la clave de descifrado. La víctima no puede usar el dispositivo capturado a menos que pague el rescate solicitado, usualmente con criptomonedas para evitar el rastreo de la transacción. En la **Figura 10** se describe el proceso general:

Figura 10: Cómo trabaja el Ransomware Bloqueado (Fte: (Humayun et al., 2021))

- *Crypto ransomware*: el malware cifra algunos de los archivos importantes del usuario (**Figura 11**). En este caso, no se ataca todo el disco duro, sino que se eligen algunos archivos importantes basados en extensiones de archivo. Este ataque suele utilizar un esquema de cifrado de 24 bits que es casi imposible descifrar sin desbloquear la clave.

Figura 11: Cómo trabaja el Crypto ransomware (Fte: (Humayun et al., 2021))

En entornos IoT el ataque por ransomware no se dirige a los dispositivos, debido a que no le resulta fácil al atacante identificar un usuario o un correo electrónico para enviar sus demandas. Estos ataques generalmente ocurren en la capa superior o de aplicación del sistema IoT.

5. Ataque de Fuerza Bruta

Esta técnica se basa en realizar una serie de intentos para vulnerar las credenciales de acceso. Mediante algoritmos que prueban múltiples combinaciones de caracteres, se intenta encontrar la clave de acceso al dispositivo. Por supuesto que el nivel de complejidad de la contraseña incide en los tiempos de ejecución del ataque, cuanto más compleja y extensa es la contraseña, más tiempo requerirá el ataque. En entornos IoT estos ataques también suelen ocurrir en la capa de aplicación, más que en el acceso a los dispositivos.

Hay varios tipos de ataques de fuerza bruta:

- ***Relleno de credenciales***: cuando el atacante recurre a una combinación conocida de nombre de usuario y contraseña que funcionó para otra aplicación (una página web, por ejemplo), a la espera de que, por comodidad el usuario utilice las mismas credenciales en el sistema IoT.
- ***Fuerza bruta simple***: en este caso el atacante intenta adivinar la clave de acceso utilizando su propia lógica, sin ninguna ayuda de un algoritmo computacional.
- ***Fuerza bruta inversa***: se trata de ataques en lo que se busca no es la contraseña sino el nombre de usuario.
- ***Ataques por diccionarios***: el atacante recurre a un diccionario o registro de contraseñas habituales, palabras o caracteres especiales posibles, del cual obtienen insumos para los algoritmos de combinación de caracteres.
- ***Fuerza bruta híbrida***: es una combinación de cualquiera de los métodos anteriores, principalmente la utilización de diccionarios para relleno de credenciales o para ataques de fuerza bruta inversa.

6. Botnets

Se denomina *botnet*, o red de robots, al conjunto de computadoras conectadas entre sí e infectadas por un malware que las deja bajo el control de un único dispositivo: el pastor de *bots*. De este modo, un conjunto de equipos es *secuestrado* por el malware y puesto a disposición de un atacante que ejerce el control sobre todo el parque de dispositivos conectados en esa red.

Estos esquemas de ataque se utilizan para distintos fines delictivos: ataques DoS distribuidos, robo de datos y expansión de virus, entre otros. Además de MITM, los ataques de botnet también son comunes en dispositivos IoT.

Los dispositivos IoT son de fácil acceso para este tipo de ataque debido principalmente a que las actualizaciones de seguridad de estos dispositivos se demoran o incluso no están previstas para aquellos componentes que se fabrican masivamente y pierden actualidad rápidamente. Muchos dispositivos IoT cuentan con un sistema operativo basado en una versión reducida de Linux, y ello facilita la compilación de un software malicioso en el propio sistema operativo.

Para analizar cómo actúan los botnets en entornos de IoT tomemos la *Anatomía de un ataque Botnet a IoT* (Angrishi, 2017), que se grafica en la **Figura 12**:

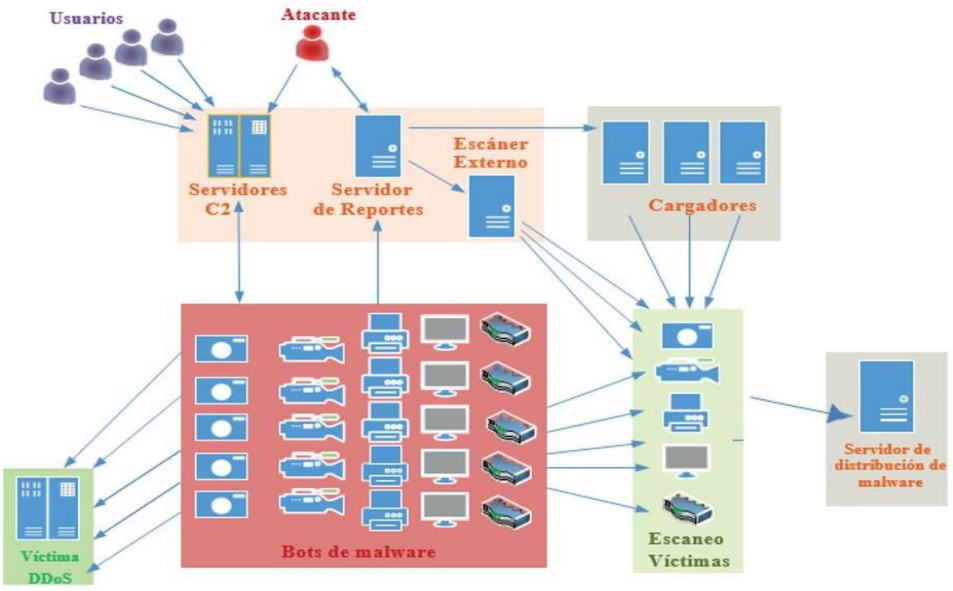

Figura 12: Estructura Genérica de una botnet de IoT (Fte: Angrishi [28])

Las botnets de IoT consisten principalmente en dos componentes básicos y cuatro adicionales, a saber:

1. Malware de Bots de los dispositivos IoT finales. Del tipo *Aidra* [48] realizan ataques DDoS[49]. El código del malware IoT está escrito principalmente en lenguaje C, C++ o Python. El código fuente para los bots se compila de forma cruzada para múltiples arquitecturas que ejecutan Linux, por ser éste un sistema operativo común entre la mayoría de los dispositivos IoT.

[48] Botnet que ataca dispositivos móviles como smartphones y tablets, routers domésticos, sistemas de vigilancia IP y equipos con sistema operativo Linux. A la fecha existen diferentes variantes y evoluciones cada vez más sofisticados.

[49] DDoS (Distributed Denial of Service): ataque de denegación de servicios distribuido, es un ataque a una red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos comprometiendo a varias o a todas las computadoras de la red.

2. Servidores de Comando y Control (C2s) se utilizan para controlar los bots.
3. Los escáneres se utilizan para buscar dispositivos IoT vulnerables.
4. Servidor de informes: utilizado para recopilar los resultados o analizar informes de bots o analizadores externos. Recibe tráfico unidireccional con información sobre las direcciones IP y las credenciales de los dispositivos IoT vulnerables o de los bots según van actuando.
5. Cargadores: son aplicaciones utilizadas para iniciar sesión en dispositivos IoT vulnerables e indicarles que descarguen el malware.
6. Servidor de Distribución de malware: es la ubicación donde se almacena el código malware para ser descargado por dispositivos IoT infectados.

Las funciones de uno u otro componente enumerados anteriormente se pueden combinar y su función puede ser realizada por otro componente, dependiendo de la estructura de funcionamiento establecida por el fabricante del botnet.

Pero en su mayoría los botnets cuentan con funciones de escaneo, ya sea que forme parte de las tareas del Servidor C2s o cuenten con algoritmos de escaneo externo. Para la búsqueda de dispositivos potenciales se pueden utilizar motores de búsqueda especializados en dispositivos conectados a internet como *Shodan*[50] y *Censys*[51].

Es importante destacar que no se observan esfuerzos serios por proteger a los dispositivos IoT de base. La mayoría de ellos tienen acceso vía telnet y con interfaz web habilitadas con credenciales predeterminadas para facilitar el acceso de los usuarios finales, quienes usualmente no cambian las credenciales predeterminadas de los dispositivos IoT.

Así, estos servicios con contraseñas predeterminadas son el primer punto de acceso para los malwares de IoT.

En resumen, el modo de operación común para la mayoría de las botnets de IoT es el siguiente:

1. El malware (escáner externo o bots o C2s) escanea continuamente Internet en busca de dispositivos IoT vulnerables, generalmente en busca de puertos Telnet u otros servicios abiertos accesibles a través de Internet.
2. Una vez que se encuentra un dispositivo IoT vulnerable, el malware accede a él utilizando la fuerza bruta con una lista de credenciales predeterminadas conocidas.
3. La dirección IP del dispositivo junto con la clave correcta se almacenan en un servidor de informes para ser utilizado por el malware cuando quiera acceder al dispositivo más tarde.
4. El malware accede al dispositivo IoT analizado con las credenciales almacenadas en el servidor de informes. Explota las debilidades de seguridad conocidas en los servicios disponibles en los dispositivos IoT, para descargar datos útiles de malware adicional en el servidor de distribución de malware.
5. El malware protege los dispositivos IoT para que ningún malware ajeno pueda acceder al dispositivo.

[50] https://www.shodan.io/

[51] https://censys.io/

6. El malware se activa mediante la ejecución del binario de malware descargado. Con se ello se aumentan los privilegios al explotar las debilidades de seguridad conocidas en los dispositivos IoT vulnerados y se acondiciona debidamente para ningún otro malware pueda acceder al mismo dispositivo IoT.
7. Si se encontrara malware de la competencia en los dispositivos IoT vulnerados, éste es erradicado utilizando diferentes técnicas como el raspado de memoria, entre otras.
8. El malware reconfigura el dispositivo para que forme parte de la botnet
9. Los bots se comunican regularmente con sus C2 utilizando el protocolo basado en IRC para indicar su existencia al operador de la botnet
10. El malware puede afectar hábilmente el rendimiento o el funcionamiento del dispositivo IoT, hasta que un usuario o propietario de botnets les indique que realicen un ataque DDoS.

Los malwares de IoT se están volviendo cada vez más adaptables y sofisticados con muchas características nuevas como el soporte de IPv6, los métodos de comunicación sofisticados entre bots y C2s. Por otra parte, también se observa un lucha aguerrida y continua en el mercado de fabricantes de botnets por dominar el mercado de ataques a entornos de IoT.

7. Ataques de Denegación de Servicios Distribuidos (DDoS)

Un ataque de denegación de servicio o DoS es un ataque en el que los recursos de un sitio web son atacados para que los usuarios no puedan acceder al mismo, básicamente inundan los servicios web o los bloquean.

La lógica de funcionamiento de este tipo de ataques consiste en bombardear el dispositivo con gran cantidad de peticiones de diferentes tipos y siempre a un mismo punto, de manera que el servidor o la red no soporten la cantidad de paquetes recibidos, y se produzca la interrupción del servicio. Su objetivo es inhabilitar el uso de un sistema informático. Pueden dirigirse a cualquier tipo de dispositivo o servidor (webs, de aplicaciones, de servicios, etc.).

Los dispositivos IoT se dañan con mucha facilidad por este tipo de ataques. Cuando el ataque es permanente (PDoS) tienen un efecto importante en los dispositivos IoT, ya que los inutiliza porque bloquea o destruye el firmware de este.

Los ataques de denegación de servicio distribuidos (DDoS), son un tipo particular de ataques de DoS en el cual el envío de peticiones está realizado por varios atacantes, utilizando mayormente botnets para controlar el ataque a distancia.

Los ataques DDoS siguen siendo un problema crítico de la seguridad de la información en los entornos IoT ya que, según el tipo de ataque, se afecta no solo el ancho de banda, sino también la latencia y las tablas conmutadas de flujo de datos.

Gran parte del hardware de los dispositivos IoT se arma con componentes reutilizados o de bajísimo costo, con escasa atención a las protecciones de seguridad necesarias, principalmente debido a que los procesos de fabricación permiten la producción masiva de componentes descartables, que se dejan a disposición del mercado tecnológico con escaso o nulo soporte postventa. Trend Micro[52] menciona “la responsabilidad compartida” que tienen los fabricantes de dispositivos para IoT, en relación con la

[52] https://www.trendmicro.com/es_es/business.html

entrega de actualizaciones de firmware y la publicación del fin del soporte para los productos más antiguos.

En un sistema IoT los dispositivos están encendidos e interconectados entre sí de forma continua, haciéndolos muy visibles en internet, con lo cual son atacados permanentemente por malware que abre camino para que el atacante genere un DDoS.

(Márquez Díaz, 2019) caracteriza en detalle este tipo de ataque. Si bien la técnica del DDoS no es nueva, lo innovador es el uso de diversos dispositivos del entorno IoT para que actúen como puente de conexión y usarlos como armas digitales de ataque y/o espionaje, lo que en conjunto con el malware potencian el nivel de petición a los servidores objetivos del ataque, a miles o millones de veces lo usual.

Dado el crecimiento continuo de los sistemas basados en IoT, es primordial proteger debidamente tanto el firmware como el hardware de los componentes IoT como, por ejemplo: termostatos conectados a cámaras de seguridad y televisores inteligentes, sensores de jardín, puertas de garajes inteligentes, cubos de basura inteligentes, wareables para humanos y mascotas, equipos médicos de alta tecnología, etc. Todos estos sistemas se convierten en potenciales armas de espionaje y/o ataque.

Si de las Smart Cities se trata, es importante reconocer que la seguridad metropolitana mediada por cámaras, robots y drones, emplean conexión a dispositivos de IoT, principalmente sensores.

(Pandya, 2021) describe los distintos tipos de ataques DDoS y se resumen a continuación:

- ***Ataque directo***: cuando las peticiones ilegítimas se envían directamente contra el objetivo sin enmascarar las direcciones IP de los atacantes.
- ***Ataque indirecto***: se redistribuye el tráfico de las peticiones a través de intermediarios antes de atacar al host objetivo. De esta manera se ocultan las direcciones IP atacantes, y son más difíciles de localizar. Además, el ataque indirecto permite llevar a cabo la técnica de amplificación, mediante la cual los propios dispositivos que actúan como intermediarios multiplican los paquetes, incrementando así la potencia del ataque.
- ***Ataque dirigido al ancho de banda***: tienen por objetivo consumir todo el ancho de banda de la red y evitar el tráfico legítimo de sus usuarios. Puede utilizarse distintas técnicas:
    - Desborde por UDP (User Datagram Protocol): Este tipo de ataque trata de “inundar” el host objetivo enviando una multitud de paquetes UDP a puertos aleatorios.
    - Desborde por ICMP (Internet Control Message Protocol): El planteamiento de este ataque es muy similar al anterior, con la excepción de que en lugar de paquetes UDP se utilizan paquetes ICMP, también llamados “ping”.
    - LOIC (Low Orbit Ion Cannon): es una herramienta escrita en el lenguaje de programación C#, que permite realizar un ataque DoS sobre una IP o URL de destino. Una vez configurada, esta herramienta genera un envío masivo de paquetes al destino establecido por el atacante.
- ***Ataque dirigido a la memoria:*** realizado con el fin de consumir la memoria del servidor objetivo provocando con ello su inhabilitación. Las técnicas más usuales son:

- Desborde SYN: aprovechándose del protocolo TCP, el atacante manipula la negociación del protocolo TCP, y en lugar de negociar una conexión entre el cliente y el servidor, como está previsto, se crean en el servidos muchas conexiones semiabiertas. Es decir, no se cumple el ciclo de la negociación TCP, y se ocupan recursos del servidor que dejan de estar disponibles para el usuario autorizado.
- Desborde Slowloris: Es muy parecido al anterior, pero consume la memoria de su objetivo mediante peticiones HTTP (Hypertext Transfer Protocol) sin completar.
- Desborde HOIC (High Orbit Ion Cannon): es el predecesor del LOIC. En este caso el ataque se realiza enviando peticiones HTTP "GET" y "POST" al host objetivo hasta que este no pueda aguantar la cantidad de peticiones que tiene por resolver.

- ***Ataque dirigido al ciclo de CPU:*** se centran en consumir todo el uso del CPU del servidor atacado. Las técnicas habituales son:
  - Christmas tree: Este tipo de ataque consiste en enviar un paquete TCP específico aprovechando la configuración de los "flags" que se encuentran en la cabecera de los paquetes TCP. En este ataque se activan 3 flags específicos, "Urgent, Push, Fin" y, si el servidor no entiende el paquete, su CPU se consumirá hasta que termine por apagarse.

8. Amenazas Persistentes Avanzadas

Las ***Amenazas Persistentes Avanzadas (APT)*** son aplicaciones de malware especialmente diseñadas para atacar un objetivo específico. Utilizando técnicas de ataque continuo y persistente se vigilan las infraestructuras corporativas hasta encontrar vulnerabilidades que permitan el acceso indebido al sistema.

Los entornos IoT no son la excepción en los ataques APT ya que el malware puede filtrarse desde cualquier dispositivo con escasa seguridad de base, y de allí escalar el sistema hasta cubrirlo por completo.

(Cano, 2011) señala que las APT han introducido técnicas de espionaje del pasado en el contexto digital, actuando de manera persistente para acceder y mantenerse en la red de la empresa atacada sin ser detectado. Este tipo de ataques se enfoca en atacar a los usuarios y no a los componentes tecnológicos. Mediante un estudio sobre el comportamiento y perfiles de los usuarios, los transforma en "víctimas útiles" para ingresar a través de ellos a la infraestructura empresarial.

Bibliografía

Al-Masri, E., Bai, Y., & Li, J. (2018). A fog-based digital forensics investigation framework for IoT systems. *Proceedings - 3rd IEEE International Conference on Smart Cloud, SmartCloud 2018*, 196–201. https://doi.org/10.1109/SmartCloud.2018.00040

Ameijide García, L. (2016). *Gestión de proyectos según el PMI*.

Angrishi, K. (2017). *Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets*. http://arxiv.org/abs/1702.03681

Augusto, D., & Moreno, P. (2012). *GESTIÓN DEL RIESGO EN LA SEGURIDAD INFORMÁTICA: "CULTURA DE LA AUTO-SEGURIDAD INFORMÁTICA."*

Babun, L., Sikder, A. K., Acar, A., & Selcuk Uluagac, A. (2018). IoTDots: A digital forensics framework for smart environments. *ArXiv*.

Bhatt, S., & Bhushan, B. (2021). Cyberattacks and Risk Management Strategy in Internet of Things Architecture. In *Artificial Intelligence and Cybersecurity* (pp. 51–68). CRC Press. https://doi.org/10.1201/9781003097518-4

Buitrago Marquez, L. M., Manrique Latorre, M. A., & Hernandez Gutierrez, J. (2020). *Redes LoRaWAN. Revisión de componentes funcionales en aplicaciones IoT*.

Cano, J. (2011). Amenazas persistentes avanzadas, inteligencia y contrainteligencia en un contexto digital. *Revista Sistemas*, *119*. https://acis.org.co/portal/Revista/119/Dos.pdf

Casellas Beneyto, F., Velasco Quesada, G., Guinjoan Gispert, F., & Piqué López, R. (2010). El concepto de Smart Metering en el nuevo escenario de distribución eléctrica. *XVII Seminario Anual de Automática, Electrónica Industrial e Instrumentación*, 752–757.

Chhabra, G. S., Singh, V. P., & Singh, M. (2020). Cyber forensics framework for big data analytics in IoT environment using machine learning. *Multimedia Tools and Applications*, *79*(23–24), 15881–15900. https://doi.org/10.1007/s11042-018-6338-1

Costantini, F., Galvan, F., de Stefani, M. A., & Battiato, S. (2020). *Assessing Information Quality in IoT Forensics: Theoretical Framework and Model Implementation*. 1–3. http://arxiv.org/abs/2012.14663

di Iorio, A. H., Castellote, A. M., Constanzo, B., Curti, H., Waimann, J., Alberdi, J. I., Cistoldi, P., Giacaglia, M. F., & Lamperti, S. (2017). El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense. In *Universidad FASTA*. Esitorial UFASTA. http://info-lab.org.ar/images/pdf/Libro.pdf

Domínguez Margareto, D. (2020). *CIBERSEGURIDAD EN INTERNET OF THINGS*.

Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2021). *Actividades fundamentales de ciberseguridad para los fabricantes de dispositivos de IoT*. https://doi.org/10.6028/NIST.IR.8259es

Gioia, C. (2019). *Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos*.

Hossain, M., Karim, Y., & Hasan, R. (2018). FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. *Proceedings - 2018 IEEE International Congress on Internet of Things, ICIOT 2018 - Part of the 2018 IEEE World Congress on Services*, 33–40. https://doi.org/10.1109/ICIOT.2018.00012

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. In *Egyptian Informatics Journal* (Vol. 22, Issue 1, pp. 105–117). Elsevier B.V. https://doi.org/10.1016/j.eij.2020.05.003

Instituto Nacional de Ciberseguridad. (2020). *PROTEGE TU EMPRESA Colección DESARROLLAR CULTURA EN SEGURIDAD*. https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad

Islam, J., Khatun, A., Roy, S., Kabir, S., & Debnath, B. C. (2017). *A Comprehensive Data Security and Forensic Investigation Framework for Cloud-Iot Ecosystem*. *4*(1).

Kebande, V. R., Karie, N. M., Michael, A., Malapane, S., Kigwana, I., Venter, H. S., & Wario, R. D. (2018). Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. *Proceedings - 2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018*, 93–98. https://doi.org/10.1109/SmartIoT.2018.00-19

Kebande, V. R., Karie, N. M., & Venter, H. S. (2017). Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures. *2017 1st International Conference on Next Generation Computing Applications, NextComp 2017*, 54–60. https://doi.org/10.1109/NEXTCOMP.2017.8016176

Kebande, V. R., & Ray, I. (2016). A generic digital forensic investigation framework for Internet of Things (IoT). *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 356–362. https://doi.org/10.1109/FiCloud.2016.57

Koroniotis, N., Moustafa, N., & Sitnikova, E. (2020). A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Future Generation Computer Systems*, *110*, 91–106. https://doi.org/10.1016/j.future.2020.03.042

Luz Clara, B. (2021). *Seminario de Derecho Informático, módulo de la carrera de Especialización en Informática Forense, UFASTA*.

Márquez Díaz, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. *Revista de Bioética y Derecho Perspectivas Bioéticas*, *46*, 85–100. www.bioeticayderecho.ub.edu

Martínez, A. (2016, February 23). *Herramientas para realizar análisis forenses a dispositivos móviles _ INCIBE-CERT*. https://www.incibe-cert.es/blog/herramientas-forense-moviles

McCauley, D., & Lara, V. (2018). *What the Internet of Things means for consumer privacy*. https://impact.economist.com/perspectives/sites/default/files/EIU_ForgeRock%20-%20What%20the%20Internet%20of%20Things%20means%20for%20consumer%20privacy.pdf

Meffert, C., Clark, D., Baggili, I., & Breitinger, F. (2017). Forensic state acquisition from internet of things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. *ACM International Conference Proceeding Series*, *Part F1305*. https://doi.org/10.1145/3098954.3104053

OEA. (2019). MARCO NIST CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad. *White Paper Serie*, *5*.

Palmer, G. (2001). A road map for digital forensic research. *Proceedings of the Digital Forensic Research Conference, DFRWS 2001 USA*, iii–42.

Pandya, G. (2021). *Preparing to withstand a DDoS Attack Preparing to withstand a DDoS Attack*.

Parlamento Europeo. (1995). *DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO (EUR-Lex - 31995L0046 - ES)*. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=ES

Paul Pickering, P. (2017). *Desarrollar con LoRa para aplicaciones IoT de baja tasa y largo alcance*. https://www.digikey.com/es/articles/develop-lora-for-low-rate-long-range-iot-applications

Qatawneh, M., Almobaideen, W., Khanafseh, M., Qatawneh, I. al, & al Ain, P. (2019). Dfim: a New Digital Forensics Investigation Model for Internet of Things. *Journal of Theoretical and Applied Information Technology*, *31*(February 2020), 24. www.jatit.org

Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. (2019). *The Cyber Security Body of Knowledge (CyBoK) 1.0*. https://www.nationalarchives.gov.uk/%0Ahttps://www.cybok.org/

Sailakshmi, V. (2021). *Analysis of Cloud Security Controls in AWS, Azure, and Google Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud Cloud*. https://repository.stcloudstate.edu/msia_etds/112

Schwartz, M. (2018). *5 Steps to Building a Culture of Security*. https://aws.amazon.com/es/blogs/enterprise-strategy/5

Steward, J. (2022). La lista definitiva de estadísticas de Internet de las cosas para 2022. *FindStack Blog*. https://findstack.com/es/internet-of-things-statistics/

Unión Internacional de Telecomunicaciones, I. (2012). *Descripción General de Internet de los Objetos*. 20. http://handle.itu.int/11.1002/1000/11559