Análisis Forense de Entornos IoT

Beatriz Gallo [1][0000-0002-3230-3108], Santiago Salamandri[2][0000-0002-7837-7137], Miguel Solinas [2][0000-0002-7550-1067]

[1] I.Es.I.Ing. /Facultad de Ingeniería, Universidad Católica de Salta
Campo Castañares S/N, Salta, Argentina
bgallo@ucasal.edu.ar
https://www.ucasal.edu.ar
[2] LARYC, Facultad de Ciencias Exactas, Físicas y Naturales,
Universidad Nacional de Córdoba, Córdoba, Argentina
miguel.solinas@unc.edu.ar
https://fcefyn.unc.edu.ar/

Abstract. Internet de las Cosas (IoT) es un entorno de comunicación que conecta componentes tecnológicos diversos en una arquitectura integrada para el procesamiento y control de funcionalidades del mundo físico y digital. Este contexto, de amplio impacto social, también está a disposición de la delincuencia virtual. En este contexto se propone una guía de acción para el análisis forense cuando se deba buscar evidencia digital en entornos IoT. El trabajo aborda la aplicación de una Guía de Actuación Forense para Entornos IoT en un caso ejemplo que analiza vulnerabilidades y el proceso de recolección de la evidencia digital necesaria, para finalizar con un conjunto de recomendaciones con impacto en la mejora de la calidad de la arquitectura de seguridad del modelo IoT.

Keywords: Forensia Digital, IoT, debilidades IoT.

1 Introducción

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" [1]. Al enlazar objetos físicos y lógicos, el entorno IoT tiene características que lo diferencian de otros, mostrando un funcionamiento muy dinámico por la escalabilidad, magnitud y heterogeneidad de los dispositivos IoT. Este contexto, de sabido impacto en la calidad de vida de las personas también está accesible para quienes buscan delinquir y quebrar la Seguridad Informática (SI). Y es desde esta óptica que se propone un marco de trabajo para el análisis forense de estos contextos.

La Forensia Digital se define 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" [2]. Cualquier evento virtual deja un rastro, que se toma como evidencia digital cuando acredita hechos, además el análisis forense investiga los incidentes de SI, indaga las técnicas e impactos del ataque.

El trabajo aborda una metodología 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 se encuentra en etapa de diseño experimental. Se toma ese ejemplo para identificar las debilidades de IoT presentes en un escenario de acceso indebido, finalizando con recomendaciones para la mejora de la arquitectura de SI del caso de uso. Para analizar el escenario propuesto, se aplica la Guía de Actuación Forense para IoT (GAFIoT) [3], que surgió del estudio comparativo de 12 metodologías propias para el análisis forense de IoT, donde se identificaron fortalezas y vacancias de cada una en función de las etapas del análisis forense.

La organización del trabajo es la siguiente: la sección 2 trata sobre la SI en IoT. La sección 3 aborda la Forensia de IoT. La sección 4 describe el caso de estudio que luego en la sección 5 se toma como ejemplo para aplicar la metodología GAFIoT. En la sección 6 se describen las recomendaciones de seguridad para el caso de estudio y en la sección 7 se presentan algunas conclusiones y trabajos a futuro.

2 La Seguridad Informática en los Entornos IoT

La SI es un aspecto crítico a partir del cambio cultural y tecnológico devenido luego del año 2020, que intensificó el uso de un espacio virtual de comunicación entre las personas que todavía no se encuentra debidamente protegido ante la ciberdelincuencia. Los dos ámbitos crecen por igual: la tecnología y el delito virtual.

Abordando los principales aspectos de la SI en entornos IoT el informe [4] destaca el incremento constante en la instalación de dispositivos IoT, el volumen de datos generados que crece notablemente, los problemas de las empresas para detectar las brechas de SI de IoT en su red, y la identificación de los enrutadores como el principal componente atacado en estos entornos. La mayoría de las acciones intrusivas (malware, ransomware, etc.) tienen dos rasgos comunes: a) la falta de una cultura de la SI en los usuarios (desarrolladores, gestores de datos o usuarios); y b) la explotación de las debilidades del software, hardware, estructuras de datos o redes de transmisión de datos.

Como trabajos notorios sobre la SI en entornos IoT se puede citar a [5] que describe un análisis profundo de las amenazas y debilidades de la arquitectura IoT, [6] que propone una guía de mejores prácticas para proteger un sistema IoT y el Informe Interno 8259 del NIST [7] que señala las actividades fundamentales de SI que deberían tener presente los fabricantes de dispositivos de IoT. Estos trabajos definen un espacio para el abordaje de la SI de entornos IoT considerando entre otros aspectos:

- La SI de los entornos IoT debe tratarse desde sus *cuatro componentes básicos*: las cosas y los dispositivos IoT, el software que gestiona el sistema, la plataforma de conectividad y los usuarios; basada en una estrategia integral para la protección de cada componente que tome los ataques y vulnerabilidades más usuales.
- *No hay un nivel homogéneo* en las capacidades para enfrentar los riesgos y amenazas en todos los componentes de la arquitectura IoT. Hay avances importantes en las plataformas de redes, pero no se observa idéntica madurez en las capacidades de SI de los dispositivos IoT y en la cultura de la seguridad del usuario de IoT.
- Las amenazas de SI en los entornos IoT son conocidas (malware, denegación de servicios, acceso no autorizado, etc.), y provienen de riesgos suficientemente estudiados en los entornos tecnológicos tradicionales. Pero está faltando *integrarlos con más fuerza* a los entornos IoT aprovechando las experiencias exitosas logradas, y aplicando metodologías de trabajo específicamente acondicionadas.

2.1 La Cultura de la Seguridad Informática

Llevadas por la necesidad de incorporar la SI en sus intangibles como ventaja competitiva, las empresas agregan este componente a su cultura organizacional. Al respecto, Schwartz [8] propone una estrategia basada en los factores críticos de la SI (los usuarios y la comunicación con ellos) y es útil la propuesta de auto-seguridad de [9] sobre el comportamiento de las personas frente a las tecnologías basado en la conducta controlada, la ética y la responsabilidad para evitar situaciones de riesgo. INCIBE [10] aborda la formación y capacitación de los distintos usuarios distinguiendo el usuario técnico que debe capacitarse en función del rol que cumple (SI de los sistemas operativos y aplicaciones, gestión de la seguridad perimetral, incidentes de SI, etc.); mientras que el usuario final debe formarse en la responsabilidad con el cuidado de un entorno seguro de trabajo (aspectos legales de la SI; situaciones de riesgo informático; tratamiento de los datos personales, etc.). Por otra parte, la SI debe rescatar los valores sociales básicos: respeto por la dignidad del otro, libertad, justicia, equidad. A los que se suman los relacionados con la protección de datos personales ([11]–[12])**.**

2.2 Vulnerabilidades de las Tecnologías IoT

Cualquier dispositivo móvil puede ser utilizado para delinquir, y cuantos más dispositivos se conecten a la red, mayor superficie de ataque se brinda y 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. Son muchos y diversos los estudios acerca de amenazas a la SI en los componentes que integran un entorno de IoT: en [5] se analizan los tipos de ataques a dispositivos IoT más usuales (ataques de denegación de servicios, de tipo Man in the Middle, ransomware, ataques de fuerza bruta y botnets), complementando la descripción con los trabajos [13]–[16].

Interesa detallar el ataque de *denegación de servicio* (DoS), que consiste en bombardear un dispositivo con gran cantidad de peticiones de diferentes tipos de modo que el servidor o la red no lo soporten y se produzca la interrupción del servicio para los usuarios autorizados. Los dispositivos IoT se dañan con mucha facilidad con estos ataques. Un tipo particular de ataque es la denegación de servicio distribuida (DDoS), en el cual el envío de peticiones es realizado por varios atacantes, utilizando botnets para controlar el ataque a distancia. Si bien esta técnica no es nueva, lo innovador es el uso de dispositivos IoT como armas de ataque, lo que junto con el malware elevan en gran volumen la cantidad de peticiones sobre los servidores objetivos bajo ataque.

Es primordial proteger debidamente tanto el firmware como el hardware de los componentes IoT. 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 el camino para que un atacante genere una DDoS. Gran parte del hardware de los dispositivos IoT se arma con componentes reutilizados o de bajísimo costo, con escasa atención a las protecciones de SI, debido a que los procesos de fabricación permiten la producción masiva de partes descartables, que quedan a disposición del mercado tecnológico con escaso soporte técnico, extendiéndose la responsabilidad del ataque a los fabricantes de dispositivos IoT.

3 Forensia de IoT

En esta sección se describen las temáticas de base: arquitectura de entornos IoT, características de la SI en estos ambientes y Forensia Digital de IoT.

3.1 Arquitectura de Entornos IoT

La Recomendación ITU Y.6060 [1] propone un modelo IoT basado en cuatro capas y capacidades de gestión y de seguridad relacionadas con éstas. La *capa de aplicación* incluye el software que trabaja sobre los servicios en la nube, para la interacción del usuario con el sistema IoT. La *capa de apoyo a servicios y aplicaciones* tiene dos capacidades: a) genéricas, para el procesamiento y/o almacenamiento de datos; y b) específicas, para funciones propias de los dispositivos IoT. La *capa de red* distingue las capacidades propias de la red (conectividad y control de acceso) y las de transporte (tráfico de datos entre los dispositivos que conforman el entorno IoT). Por último, en la *capa de dispositivos* están diferenciadas las capacidades del dispositivo (en cuanto a su funcionamiento lógico) y las de pasarelas (interfaces de comunicación y protocolos que vinculan el modelo de procesamiento IoT). Hay dos capacidades transversales: *la de gestión y la seguridad*. La primera hace referencia a la capacidad para administrar el sistema IoT garantizando el funcionamiento de la red, congeniando las aplicaciones de acción automática con las generadas por el usuario. Desde la SI, se considera que la conexión de un dispositivo al entorno IoT conlleva

amenazas, por lo que es necesario integrar las distintas políticas de SI de los componentes IoT.

3.2 Metodologías para el Análisis Forense de IoT

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

El proceso forense incluye seis etapas: a) Planificación de las Actividades; b) Identificación de la Evidencia; c) Extracción de la Evidencia; d) Preservación de la Evidencia; e) Análisis y Correlación de los Datos; y f) Informe y Presentación de la Evidencia. Cualquiera sea el marco de trabajo a aplicar, el proceso forense debe incluir estas etapas con el desarrollo concurrente de las normas técnicas que correspondan.

La propuesta inicial para GAFIoT en [3] fue ajustada en una segunda versión, que aquí se presenta (ver Fig. 1), producto de una primera experiencia de aplicación de esta metodología en un escenario de ataque que luego se explica en la sección 5. Las actividades de cada fase son interactivas, ya que resultan de la retroalimentación natural del proceso. En todas sus fases, las actividades se enfocan en las capas del entorno IoT, que también tienen una retroalimentación entre ellas, siendo necesario analizar cada capa en particular, pero sin descuidar la interacción de cada una sobre las restantes.

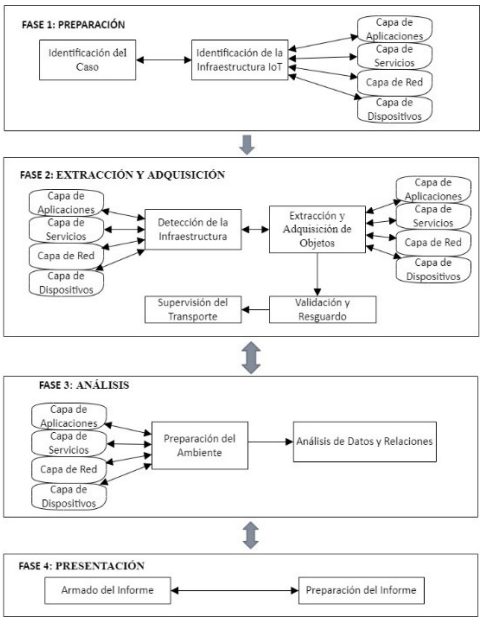

Fig. 1: Guía de Actuación Forense para Entornos IoT (GAFIoT)

En la **Fase 1(Preparación)** se realizan dos actividades. La **Identificación del Caso,** cuyo objetivo es el relevamiento de la situación mediante técnicas adecuadas (entrevistas a usuarios, revisión de documentación técnica, consulta a expertos, etc.) para definir la estrategia del análisis forense. En la **Identificación de la Infraestructura IoT** se incluyen tareas de observación del lugar para identificar los objetos de interés, centrándose en la detección de la infraestructura de red y de servicios atendiendo al modelo de cuatro capas ya descripto. La *capa de aplicación* es habitual encontrarla en el dispositivo inteligente del usuario final, 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 cloud 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 los brindados por el proveedor. Esta actividad se completa con la identificación de los aspectos de la SI necesarios.

En la **Fase 2 (Extracción y Adquisición)** se desarrollan 4 actividades. En la **Detección de la Infraestructura** se identifica con claridad todos los componentes del entorno IoT que se está analizando mediante la observación visual (si fuera posible la visita a las instalaciones) para ajustar la primera idea de la Infraestructura IoT lograda en la Fase 1. La **Extracción y Adquisición de Objetos** debe respetar estrictamente el protocolo que asegure la trazabilidad de la evidencia, cuidando de realizar las tareas técnicas adecuadas según el tipo de evidencia, así como lo relacionado con la preservación, embalaje y transporte de éstas. 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. 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 de acceder a los sensores instalados físicamente en las "cosas" que controlan. Los accesos más dificultosos suelen ser a las capas de servicios y de red que depende de terceros. La **Validación y Resguardo** implica realizar las imágenes forenses, su encriptación y registro seguro, y la **Supervisión del Transporte** se refiere a los cuidados cuando se deben entregar las evidencias a terceros intervinientes en la investigación, garantizando que se cumplan 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. En la actividad de **Preparación del Ambiente** se adecua el ambiente tecnológico para la manipulación de las evidencias encontradas, en un contexto similar al escenario delictivo. La actividad de **Análisis de Datos y Relaciones** consiste en realizar búsquedas y correlaciones de las evidencias, con las técnicas y métodos pertinentes (análisis de información histórica, búsqueda por cadena de caracteres, etc.). Para esta última etapa las herramientas forenses presentan un árbol de navegación con toda la información extraída, y un conjunto de funcionalidades que ayudan al investigador (líneas de tiempo, filtros por tipo de archivo, etc.). Pero es probable que al usar herramientas separadas para cada componente del entorno IoT, sea necesario vincular manualmente los datos, lo que dependerá de la capacidad del especialista forense para identificar relaciones y vincularlas debidamente.

La **Fase 4 (Presentación**) se enfoca en mostrar los resultados logrados para 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 contiene dos partes: a) la explicación general del caso en un lenguaje acorde a los usuarios no tecnológicos incluyendo un diccionario de definiciones técnicas sobre IoT, a fin de que se comprenda mejor cómo actuó la evidencia digital en el hecho investigado; y b) los Anexos Técnicos que apoyan las conclusiones del análisis forense. Estos últimos sirven para replicar el proceso forense si fuera necesario. Luego sigue la **Preparación del Informe**, que consiste en aprestar los documentos precitados y la evidencia digital que los sustentan, garantizando la admisibilidad de esta (sanitización del soporte y tratamiento contra escritura, grabación y encriptación de los archivos).

GAFIoT presenta entre otros beneficios, los siguientes: a) se ajusta al proceso general forense, respetando las actividades y criterios de las buenas prácticas de la investigación forense; b) ordena el proceso forense al identificar las actividades de cada fase según las capas del modelo IoT; y c) incluye actividades lo suficientemente genéricas como para ajustar la tarea forense a diferentes entornos IoT, considerando a éstos de manera integral, más allá de los componentes individuales y específicos que lo integren.

4 Caso de Estudio: Captura de datos de Medidores de Energía Eléctrica

El caso de estudio denominado *Sistema Inteligente para la Captura de Datos de Medidores de Energía Eléctrica (SICaMEe)*, es producto del Trabajo Final para la Maestría en Internet de las Cosas de la Universidad de Buenos Aires, del Ing. Santiago Salamandri, titulado ”Sistema de Telemedición de servicios públicos basado en Inteligencia Artificial”. Tiene como objetivo generar un entorno IoT basado en sistemas embebidos e Inteligencia Artificial (IA) para el monitoreo y captura de datos que servirán de insumo de los consumos de servicios públicos. Al momento de presentar este informe dicho trabajo se encuentra en su etapa final de desarrollo.

El modelo tecnológico del SICaMEe incluye herramientas de captura de imágenes e IA que hacen posible una solución más rápida y económica que las actuales del mercado, reemplazando la medición manual del consumo incorporando un *smart meter* con la capacidad de capturar una imagen del medidor y reconocer a través de la IA el consumo actual, y transmitir esa lectura al servidor a través de una red inalámbrica. Así es posible obtener datos sobre el consumo energético (kw consumidos, fecha y hora de la medición, domicilio, etc.), para procesarla con herramientas de analítica de datos, a fin de que las empresas distribuidoras de energía tengan oportunidad de estudiar estrategias de gestión como por ejemplo: análisis de las demandas de energía según zona y variables estacionales; programación más ajustada de las tareas de mantenimiento y cortes de energía y análisis tarifario de los servicios que brinda según distintas tipificaciones (consumo domiciliario/industrial, zonificación urbana/rural, etc.). En la Fig. 2 se muestra la arquitectura del sistema, identificando los componentes de nivel superior, funcionalidades, tecnologías y frameworks requeridos, a la vez que transversalmente se visualizan las capas de: captura de datos, transmisión y procesamiento.

La **Capa de Captura de datos** incluye los elementos que generan y procesan los datos que alimentan el sistema. El *Medidor* es el componente primario proveedor de datos de consumo eléctrico e interactúa con un sistema *EndPoint* (cámara que actúa como un transductor y un microcontrolador que es la unidad de procesamiento encargada de recibir las imágenes y procesarlas mediante un algoritmo de IA que identifica los valores numéricos de consumo de la imagen capturada). Posteriormente estos datos se envían por la red inalámbrica. Todo ello complementado con el sistema de alimentación y el soporte mecánico de los componentes. La **Capa de Transmisión de Datos** se basa en un Gateway que comunica los equipos ubicados en diferentes redes y que utilizan estándares propios, actuando como dispositivo encargado de tomar los datos capturados y transportarlos por la red inalámbrica. La **Capa de Procesamiento de Datos** está centrada en el *Servicio Web* que permite la gestión del sistema. Bajo la modalidad de una WebAPP, la aplicación responde a las reglas del negocio y a la comunicación entre los componentes IoT como BackEnd, más las interfases necesarias en el FrontEnt. Esta capa se completa con una base de datos no SQL, de uso ventajoso en equipos de bajos recursos de procesamiento.

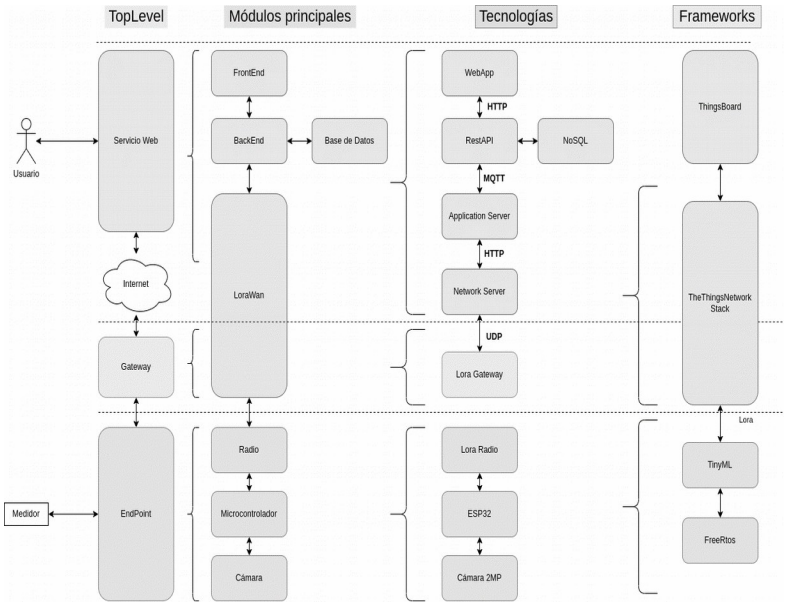

Fig. 2: Arquitectura Integral del Sistema SICaMEe

5 Aplicación de GAFIoT al Caso de Estudio

A los fines del presente trabajo, se propone un escenario de ataque en el que SICaMEe tuvo un acceso indebido. Considerando las fases y actividades de GAFIoT definidas en la Sección 4 se describe su aplicación en el escenario indicado.

El analista forense inicia su tarea con la actividad de **Identificación del caso** mediante entrevistas con los usuarios responsables del sistema, para armar la narrativa general del ataque y definir la estrategia inicial para enfrentar el caso. Como resultado de estas acciones se obtienen la siguiente información: a) El SICaMEe fue atacado externamente con técnicas que en un primer momento no se pueden establecer y serán motivo de identificación; b) de una primera revisión general 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 (lentitud en funcionamiento de la red, demoras al reiniciarse el servicio web, e incremento de tráfico SPAM en el correo electrónico y mensajería instantánea). También se obtuvo información acerca de las instancias de SI existentes, la inactividad del sistema y pérdida de datos. De esta revisión inicial se proponen los objetivos del análisis forense: a) Identificar el tipo de ataque ocurrido; b) Identificar las debilidades técnicas y operativas del SICaMEe que posibilitaron el ingreso del atacante; y c) Obtener un conjunto de recomendaciones orientativas para mejorar la seguridad del sistema.

En la **Identificación de la Infraestructura IT** se define cada uno de los componentes de SICaMEe en base al modelo de 4 capas descripto. En la *capa de aplicación* se presta especial atención a la administración de las credenciales de

acceso de los usuarios. En la *Capa de apoyo a servicios y aplicaciones* se observa el software embebido desarrollado mediante ESP-ID (herramienta propietaria del componente ESP32), *CassandraDB*, más los componentes *Application Server* y *Network Server* para la interconexión con la tecnología IoT. Se utiliza además el servicio SaaS de *GitHub*, además de los servicios y aplicaciones residentes en los dispositivos móviles del usuario final. La *Capa de Red* utiliza LoRaWan como Gateway y los componentes adicionales de esta tecnología que resulten necesarios. Por último, en la *Capa de Dispositivos* se mira el *Smart Meter* diseñado como un sistema EndPoint que integra un microcontrolador ESP32, la cámara ultra pequeña OV2640, y protocolos de comunicación del módulo de LoRa radio.

En la **Fase de Extracción y Adquisición**, se visitan las instalaciones del comitente para acceder a los diversos componentes en la búsqueda de evidencia del ataque perpetrado. Las tareas recomendadas por la metodología GAFIoT se realizan adecuadamente. En la **Detección de la Infraestructura** se procede a observar las instalaciones e identificar los elementos de interés (consola de comandos, dispositivos locales, servicios web accedidos, etc.). La **Extracción y Adquisición de Objetos** es realizada *en caliente* cuidando de preservar la evidencia recolectada mediante la generación de las imágenes forenses correspondientes. En esta fase se identifican situaciones que hacen sospechar cómo se realizó el ataque y cuáles son los componentes involucrados, generando una estrategia para proceder a la extracción y adquisición de la evidencia de cada capa. En la *Capa de aplicación* se busca evidencia en 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), mediante las herramientas forenses apropiadas. La evidencia que se busca en la *Capa de apoyo a servicios y aplicaciones* está en los espacios destinado a GitHub y MongoDB para las aplicaciones; y Windows/Android para los dispositivos del usuario final, usando herramientas forenses acordes. De GitHub se pueden obtener metadatos y timestamp de los archivos contenidos, para MongoDB se aplican herramientas de auditoría del propio motor para filtrar los datos necesarios, y para los dispositivos de los usuarios, son muy útiles los registros internos de los servicios, las memorias caché y el contenido general disponible que puede obtenerse mediante herramientas para la extracción lógica y física. Si la infraestructura presenta complejidades, se puede recurrir a herramientas triage. En cuanto a la *Capa de Red*, la extracción debe centrarse en el Gateway y en la infraestructura de transmisión. Son útiles las técnicas de *Sniffing* para identificar eventos anómalos. Y, por último, en la *Capa de Dispositivo IoT* la evidencia se encuentra en las memorias del microcontrolador, por lo que son útiles las técnicas de volcado de memoria para la recolección. Las restantes actividades de esta fase requieren documentar ordenadamente el caso como antecedente para ataques futuros.

En la **Fase de Análisis** se aborda la actividad de *Análisis de Datos y Relaciones*. Entre los objetivos inicialmente planteados está el de "*Identificar el tipo de ataque ocurrido*". Para responder, el experto forense se enfoca en el análisis integrado de todas las evidencias recolectadas y llega a identificar 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.* Para obtener acceso a los dispositivos IoT, Mirai emplea un diccionario basado en más de 60 combinaciones diferentes de credenciales de usuario de divulgación pública, que luego utiliza en los ataques de fuerza bruta hasta lograr el ingreso al dispositivo IoT. Una vez que lo captura, lo integra a su red botnet y avanza sobre el espacio de direcciones IP del dispositivo, y escanea todo el espectro encontrando nuevos dispositivos vulnerables para sumarlos a su botnet. El atacante aprovecha la escasa seguridad en las credenciales de acceso originales de fábrica de estos dispositivos, y que usualmente los usuarios no modifican al integrarlos a su sistema IoT. Habiendo identificado esta boca de acceso del ataque, se debe analizar los restantes componentes para conocer el impacto en todo el sistema IoT. De esta forma, el análisis forense de las memorias persistentes y volátiles del sistema SICaMEe, genera evidencia que podría indicar hasta donde avanzó el bots en su búsqueda de componentes vulnerables para sumar a su botnet. También se pueden armar líneas de tiempo con los metadatos de las evidencias para identificar el recorrido realizado por el bots.

En la **Fase de Presentación** se responde a los objetivos inicialmente planteados sobre el incidente, con el grado de detalle suficiente para entender el impacto del ataque en los seis componentes de un sistema de información: hardware, software, conectividad, estructura de datos, comunicación con el usuario y SI.

6 Recomendaciones de Seguridad para SICaMEe

Para cumplir con el objetivo propuesto de “*Obtener un conjunto de recomendaciones orientativas para mejorar la seguridad de todo el sistema*” se formulan las siguientes recomendaciones para cada capa del modelo IoT. En la *Capa de Aplicaciones* las recomendaciones se enfocan en la aplicación WebAPP utilizada por los usuarios, pues allí está el primer punto de entrada de ataques según el grado de protección establecida en las credenciales de acceso. Es aconsejable considerar las recomendaciones OWASP [17] para mejorar la seguridad de las aplicaciones. En la *Capa de Servicios y Aplicaciones* se debe enfatizar la seguridad de los servicios en la nube. Al respecto, el trabajo [18] define 5 dominios y 20 controles asociados para el monitoreo de las plataformas de cloud computing. Además, se requieren procedimientos de revisión y limpieza de los dispositivos que tengan memorias permanentes, así como los resguardos de datos previos al ataque, para evitar el contaminado del sistema una vez curado. La *Capa de Red* de SICaMEe se basa en tecnología LoRaWAN que tiene características fuertes en SI [19], que obviamente serán provechosas siempre que se atienda la asignación de credenciales y accesos de los dispositivos IoT. Para la *Capa de Dispositivos IoT* son válidas las recomendaciones [20] respecto de aplicar métodos de control de acceso, derogando las credenciales de fábrica, así como técnicas de cifrado y autenticación de nodos que garanticen la comunicación entre todos los componentes de la red IoT. Y en cuanto a la *Capa de Seguridad*, cabe una recomendación prioritaria: trabajar fuertemente sobre

la capacidad de seguridad transversal del sistema IoT, abordado desde la gestión de riesgos en SI, según guías de reconocimiento internacional como *Ciber Security Framework* (CSF) [21], junto con el desarrollo de una cultura de la SI entre los usuarios que interactúan con SICaMEe desde todos los roles que cumplen.

7 Conclusiones

De acuerdo a los objetivos planteados se puede concluir que: a) se mostró la factibilidad de aplicación de la propuesta de Forensia de entornos IoT para el caso SICaMEe; b) se analizaron e identificaron las posibles debilidades del sistema SICaMEe bajo el supuesto de un ataque de botnets; y c) dado que el SICaMEe se encuentra en etapa de diseño experimental, las recomendaciones propuestas sobre la SI son atinentes y oportunas, y están a consideración del equipo de trabajo del proyecto SICaMEe.

Lo realizado hasta aquí con GAFIoT marca un camino de fortalecimiento de esta propuesta, ya que la validación con un caso experimental es enriquecedora, aun cuando no se haya llegado a la implementación en un trabajo de campo. GAFIoT debe ser validada y aceptada por la comunidad forense, mediante un plan que incluya: a) convocatoria a usuarios expertos para una crítica constructiva mediante un esquema colaborativo sistemático y riguroso; b) validación de los procesos de adquisición y extracción de evidencia, con pruebas de laboratorio que usen herramientas forenses adecuadas al tipo de evidencia y soporte; y c) validación en otros escenarios forenses más exigentes como sistemas IoT aplicados a la salud de las personas. La investigación puede continuar con el estudio de las herramientas forenses para entornos IoT, ya sea tomando las existentes y realizando pruebas robustas en estos ambientes, o bien, se propongan nuevas herramientas forenses. Por último, sería provechoso mejorar las técnicas de recolección y adquisición de evidencia “en caliente”.

Referencias

1. Unión Internacional de Telecomunicaciones, “Descripción General de Internet de los Objetos,” p. 20, 2012, [Online]. Available: http://handle.itu.int/11.1002/1000/11559
2. G. Palmer, “A road map for digital forensic research,” Proceedings of the Digital Forensic Research Conference, DFRWS 2001 USA, pp. iii–42, 2001
3. H. B. Parra De Gallo, “Proposal for a Forensic Action Guide for Internet of Things (IoT) Environments,” Computación y Sistemas, vol. 26, no. 1, Mar. 2022, Accessed: May 21, 2022. [Online]. Available: https://cys.cic.ipn.mx/ojs/index.php/CyS/article/view/3898
4. J. Steward, “La lista definitiva de estadísticas de Internet de las cosas para 2022,” FindStack Blog, 2022. Accessed: Mar. 18, 2022. [Online]. Available: https://findstack.com/es/internet-of-things-statistics/
5. S. Bhatt and B. Bhushan, “Cyberattacks and Risk Management Strategy in Internet of Things Architecture,” in Artificial Intelligence and Cybersecurity, CRC Press, 2021, pp. 51–68. doi: 10.1201/9781003097518-4.

6. D. Domínguez Margareto, “CIBERSEGURIDAD EN INTERNET OF THINGS,” Jun. 2020.
7. M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, “Actividades fundamentales de ciberseguridad para los fabricantes de dispositivos de IoT,” Gaithersburg, MD, Mar. 2021. doi: 10.6028/NIST.IR.8259es
8. M. Schwartz, “5 Steps to Building a Culture of Security,” 2018. [Online]. Available: https://aws.amazon.com/es/blogs/enterprise-strategy/5
9. D. Augusto and P. Moreno, “GESTIÓN DEL RIESGO EN LA SEGURIDAD INFORMÁTICA: ‘CULTURA DE LA AUTO-SEGURIDAD INFORMÁTICA,’” 2012.
10. Instituto Nacional de Ciberseguridad, “PROTEGE TU EMPRESA Colección DESARROLLAR CULTURA EN SEGURIDAD,” 2020. Accessed: Mar. 11, 2022. [Online]. Available: https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad
11. Parlamento Europeo, “DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO (EUR-Lex - 31995L0046 - ES),” 1995. Accessed: Mar. 11, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=ES
12. D. Ce, D. E. L. Parlamento, and E. Y. Del, “DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre PROTECCIÓN DE DATOS,” vol. 39, pp. 1–22, 2008.
13. M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, “Internet of things and ransomware: Evolution, mitigation and prevention,” Egyptian Informatics Journal, vol. 22, no. 1. Elsevier B.V., pp. 105–117, Mar. 01, 2021. doi: 10.1016/j.eij.2020.05.003.
14. K. Angrishi, “Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets,” Feb. 2017, [Online]. Available: http://arxiv.org/abs/1702.03681
15. G. Pandya, “Preparing to withstand a DDoS Attack Preparing to withstand a DDoS Attack,” 2021.
16. J. Márquez Díaz, “Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas,” Revista de Bioética y Derecho Perspectivas Bioéticas, vol. 46, pp. 85–100, 2019, [Online]. Available: www.bioeticayderecho.ub.edu
17. V. Sailakshmi, “Analysis of Cloud Security Controls in AWS, Azure, and Google Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud Cloud,” 2021. [Online]. Available: https://repository.stcloudstate.edu/msia_etds/112
18. “OWASP Top 10-2017,” 2017. [Online]. Available: https://github.com/OWASP/Top10/issues
19. L. M. Buitrago Marquez, M. A. Manrique Latorre, and J. Hernandez Gutierrez, “Redes LoRaWAN. Revisión de componentes funcionales en aplicaciones IoT,” 2020.
20. S. Bhatt and B. Bhushan, “Cyberattacks and Risk Management Strategy in Internet of Things Architecture,” in Artificial Intelligence and Cybersecurity, CRC Press, 2021, pp. 51–68. doi: 10.1201/9781003097518-4.
21. OEA, “MARCO NIST CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad,” White Paper Serie, vol. 5, 2019.