ISSN 2007-9737

Propuesta de una guía de actuación forense para entornos de internet de las cosas (IoT)

H. Beatriz Parra de Gallo

Universidad Católica de Salta,
Instituto de Estudios Interdisciplinarios de Ingeniería (IEsIIng),
Facultad de Ingeniería,
Argentina

bgallo@ucasal.edu.ar

Resumen. Internet de las Cosas (IoT) se considera el entorno de comunicación del futuro, en el que se conectan componentes tecnológicos de cualquier tipo para compartir datos, haciendo posible el procesamiento y control de funcionalidades mediante un marco de trabajo integrado puesto a disposición del usuario. Este contexto, de muchísimas ventajas para la mejora de la calidad de vida de las personas, con amplio impacto en la economía, la salud y la industria, también se encuentra a disposición de quienes buscan en internet nuevos modos de delinquir. Y es desde esta óptica que se aborda el Entorno IoT, para estudiar y proponer una guía de acción que permitan realizar un análisis forense adecuado y suficiente cuando se deba buscar evidencia digital en estos contextos. El trabajo incluye la revisión de un conjunto de metodologías para el análisis forense en general —y de IoT en particular— de la cual se deriva luego una Guía de Actuación Forense para Entornos IoT (GAFIoT).

Palabras clave. Forensia digital, Internet de las Cosas, IoT.

Proposal for a Forensic Action Guide for Internet of Things (IoT) Environments

Abstract. Internet of Things (IoT) is considered the communication environment of the future, in which technological components of any kind are connected to share data, making possible the process and control of functionalities through an integrated framework available for the user. This context, with many advantages for improving the quality of life of people, with a wide impact on the economy, health and industry, is also available to those who search new ways of chime using the Internet. And it is from this perspective that the IoT environment is approached, to study and propose an action guide that allows an adequate and sufficient forensic analysis when it must search digital evidence in this context. The work includes the review of a set of methodologies for forensic analysis in general, and IoT in particular, from which a Forensic Action Guide for IoT Environments (GAFIoT) derives.

Keyword. Digital forensic, internet of things, IoT.

1. Introducción

Según la recomendación ITU Y.6060 [1] de la Unión Internacional de Telecomunicaciones (UIT) 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 particulari-dades que diferencian esta tecnología de las aplicadas hasta hoy; revelando un

ISSN 2007-9737

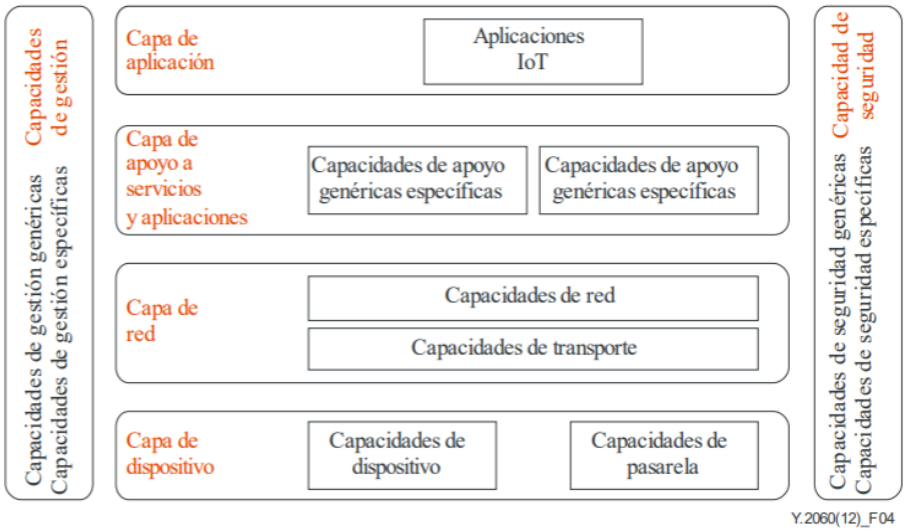

Fig. 1. Modelo de Referencia de IoT

funcionamien-to 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 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.

La DFRWS 2001 USA [2] 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.

Uno de los objetivos de la Forensia Digital, es colaborar con la justicia en la validación y presentación de evidencia digital, conforme a los principios y métodos que garanticen la confiabilidad de dicha evidencia, que se sustenta en dos elementos claves: a) la capacidad de reproducibilidad del análisis forense (basado en criterios metodológicos científicos rigurosos), y b) el registro de la *Cadena de Custodia* de la evidencia (sistema de control y registro que se aplica a la evidencia, desde su hallazgo hasta la conclusión del caso). En este sentido, las características de IoT resultan un desafío para la Forensia Digital.

El objetivo del presente trabajo es elaborar una propuesta metodológica que sirva como guía de acción para el análisis forense de la evidencia digital derivada de Entornos IoT, con atención en los aspectos técnicos y procedimentales (legales e investigativos) del análisis forense.

Este trabajo está organizado de la siguiente manera: la Sección 2 incluye una breve descripción del Entorno IoT. La Sección 3 describe los actuales desafíos que se plantean desde la Forensia Digital al abordar IoT. La Sección 4 contiene una revisión de las metodologías para el análisis forense en general y en particular, para datos provenientes de Entornos IoT, concluyendo la sección con un análisis comparativo de dichas metodologías. Por su parte, la Sección 5 detalla la

propuesta elaborada como Guía de Actuación Forense para Entornos IoT. La Sección 6 presente un plan de validación de dicha propuesta y finalmente, la Sección 7 contiene las conclusiones y futuras líneas de investigación sobre esta temática.

2. Breve descripción del entorno IoT

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 [1] que se grafica en la Figura 1, basado en cuatro capas y capacidades de gestión y de seguridad relacionadas con éstas.

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: 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. Desafíos de la Forensia Digital frente a IoT

Son varios los autores que investigaron sobre la aplicación de la Forensia Digital a Entornos IoT, destacando los problemas que se presentan frente a este nuevo contexto tecnológico.

Patel et al. [3] señalan algunos aspectos que se deberán resolver sobre IoT:

- El límite de almacenamiento de los dispositivos de IoT fijado por los fabricantes provoca la sobre escritura de los datos, impactando en la vida útil de los datos que pudieran contener;
- La reticencia de los proveedores de servicios de internet para brindar acceso voluntario a los servicios que brindan, a lo que se suma la ubicuidad de los datos, significan un esfuerzo considerable del investigador forense en la búsqueda del dato de primera fuente;
- La complejidad de las arquitecturas de procesamiento y almacenamiento de datos, basadas en tecnologías acordes a los dispositivos IoT también implican un desafío para las actuales herramientas forenses;
- La dinámica del Entorno IoT atenta contra la capacidad de mantener la integridad de los datos impactando en la Cadena de Custodia de la evidencia digital, poniendo en riesgo la admisibilidad judicial de esta evidencia.

Por su parte, Stoyanova et al. [4] marcan los problemas que el Entorno IoT presenta para la Forensia Digital, desde los distintos procesos involucrados en el análisis forense:

- Identificación de la evidencia: a veces no es posible saber dónde están almacenados exactamente los datos. A esto colaboran la dificultad de secuestro de los dispositivos

intervinientes en el acto delictivo y la factibilidad de reconstruir la escena del crimen. La tecnología de los dispositivos IoT (sensores, drones, implantes médicos, etc.) también atentan contra una correcta identificación de la evidencia.

– Adquisición de la Evidencia: la comunidad forense no cuenta con métodos estandarizados formalmente aceptados en la corte de justicia para la recolección de la evidencia en Entornos IoT, principalmente debido a la variedad y madurez tecnológica de los dispositivos IoT. A esto se suma la falta de competencias del personal forense en las nuevas tecnologías y/o dispositivos de IoT.
– Preservación y protección de la evidencia: las cuestiones relacionadas con la conservación y garantía de la integridad de los datos son de suma importancia en el contexto forense. El proceso de resguardo de la evidencia basado en la Cadena de Custodia es alta-mente exigido en el ámbito judicial, ya que garantiza la admisibilidad de la prueba. La Cadena de Custodia se complica cuando los soportes que contienen la probable evidencia no pueden "reservarse" y registrase como prueba del delito, como ocurre con los datos residen en servidores remotos de la nube.
– Análisis y correlación de la evidencia: cuando se trabaja en Entorno IoT, surgen problemas relacionados con el análisis "punta a punta" (considerando el proceso integrado desde la identificación de la evidencias hasta la presentación en la corte de justicia). La falta de metadatos en los dispositivos IoT así como las diferencias horarias de los procesos que intervienen también impactan en el análisis forense. El contexto legal en que se encuadra el delito se complica en los Entornos IoT, ya que no resulta sencillo identificar las jurisdicciones legales internacionales o regionales, y se observa además la ausencia de convenios de cooperación entre estos estamentos.
– Identificación de personas que comenten los delitos: De por sí, la Forensia Digital solo llega hasta la identificación del *usuario* asociado a la evidencia, dejando en manos de la investigación policial, la relación entre ese usuario tecnológico y una persona real. Esta situación es mucho más compleja en Entorno IoT debido a la ubicuidad de la evidencia encontrada, a los principios de uso compartido de los recursos de computación en la nube y principalmente a la funcionalidad automatizada de algunos dispositivos IoT (como la apertura de puertas o el control de sensores).
– Presentación de la Evidencia: usualmente en el ámbito judicial, los interesados no cuentan con formación tecnológica de base. Esa es la razón por la que se recurre a los profesionales peritos. En el caso del Entorno IoT, es doblemente difícil para el lego comprender como funciona esta tecnología y el impacto que la misma tiene en la comisión de delitos. Esto significa que el informe de presentación de la evidencia, debe escribirse en términos simples y comprensibles para el lector no tecnológico, siendo esta una competencia de los investigadores forenses que usualmente no se promueve.

Para el contexto tecnológico que particularmente nos preocupa —IoT— el CyBok (The Cyber Security Body of Knowledge) [5] menciona otros desafíos:

– Los procesos de *adquisición física* de los datos (volcados de memoria por ejemplo), son prácticamente inaplicables en la nube, debido a que los datos se encuentran en constante movimiento, se comparten y además surgen problemas de propiedad de los mismos. Por ello, la *adquisición lógica* de los datos (identificación a partir de los metadatos y configuraciones de las aplicaciones) debe ser el criterio normalizado para la adquisición de datos en la red, y para ello, las API de servicios en la nube deben incorporar funcionalidades de búsqueda y filtrado de los registros que informen sobre las actividades del usuario y los sistemas.
– El procesamiento distribuido es la base de los servicios de red. Se está migrando del modelo cliente/servidor en el que todo el procesamiento se realizaba en el propio dispositivo del usuario a sistemas tipo SaaS, en los que el procesamiento se distribuye en diversos espacios de la nube, a los que el

usuario accede solo para interactuar en eventos puntuales. Las herramientas forenses no están preparadas para este con-texto, se necesita otro enfoque que permita la recolección de los datos en vivo desde los servicios que consume el sistema IoT. Un párrafo aparte merece las cuestiones relacionadas a la ética forense:

– Algunos dispositivos IoT almacenan datos sobre de carácter privado (salud de las personas, por ejemplo) y a los que no se debe acceder sin la debida autorización. Desde la Forensia Digital se observa con preocupación el acceso masivo a los datos de manera involuntaria, poniendo al investigador forense en una situación delicada que debe saber manejar para no caer él mismo en la comisión de delitos por acceso indebido a datos personales. En el Entorno IoT, la protección de la privacidad de las personas es muy difícil de lograr. El proceso de recolección de datos es generalizado, a veces sin filtros de búsqueda por términos claves. Aquí toma especial interés el artículo de Vallejo et al. [6] en el que se analiza la exposición de los niños en Entornos IoT en donde pueden estar expuestos datos sensibles a través de los dispositivos de IoT (como implantes médicos o dispositivos de control de los signos vitales), así como la propuesta de Escamilla Ambrosio et al. [7] en la que se analizan los riesgos y las condiciones de seguridad informática de las aplicaciones móviles de los servicios de salud de urgencia. Por otra parte, los proveedores de servicios en la nube se enfrentan a cuestionamientos de sus clientes cuando la recolección forense no está debidamente organizada y orientada, por ello usualmente no son colaborativos con la justicia.

– Atlam et al. [8] señalan otros aspectos éticos que aplican al Entorno IoT que deben tenerse presente: a) la identificación precisa de la evidencia digital con el usuario que efectivamente generó esos datos; b) los límites de la información pública y privada que se recolecta; y c) y el impacto de los contextos de seguridad de los dispositivos IoT en la vida y/o salud de las personas.

4. Marcos metodológicos para el análisis forense en entornos 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 resolver, 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* [5]:

1. Las personas que actúan sobre la evidencia digital no deben tomar ninguna acción que comprometa la confiabilidad de la misma.
2. Quienes accedan a la evidencia digital, deben tener competencias suficientes para hacerlo.
3. 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.
4. 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 describe 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.

4.1. Marcos metodológicos de la forensia digital

Con un desarrollo de más de 25 años la Forensia Digital cuenta con técnicas ajustadas a la aplicación de principios científicos y metodológicos para el tratamiento de la evidencia digital.

Fig. 2. Fases de PURI

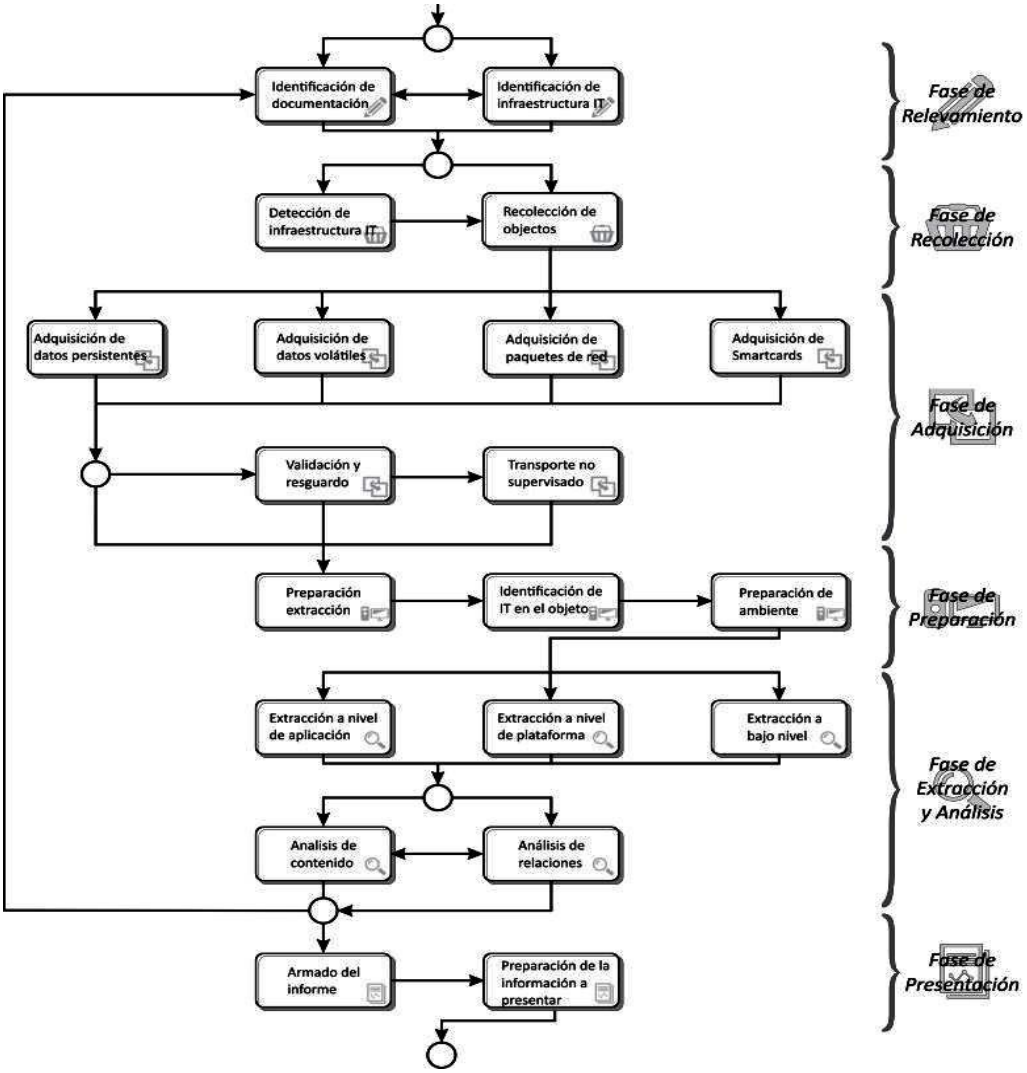

Fig. 3. Diagrama de Actividades de PURI

En sus inicios, las pericias informáticas se realizaban recurriendo a las normas y protocolos que la Informática había desarrollado para el ámbito de la Seguridad de los Sistemas de Información. Los antecedentes se remontan a la norma BS 7799 de BSI (British Standards Institution); la "RFC 3227: Guía Para Recolectar y Archivar Evidencia" elaborada por la IETF (Internet Engineering Task Force) en la que se provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones; la Norma ISO17999 que luego evoluciona en la ISO/IEC 17999:2005, hasta conformar lo que hoy se conoce como familia de normas ISO/IEC 27001:2015, algunas de ellas de competencia directa con la forensia digital como la ISO/IEC 27037:2012 para la gestión adecuada de la evidencia digital potencial; la ISO/IEC 27041:2015 para garantizar la idoneidad y adecuación de los métodos de investigación; y la ISO/IEC 27042:2015 para el análisis e interpretación de la evidencia digital.

Si bien estas propuestas resuelven —cada una en lo suyo— algún aspecto técnico del proceso forense, no lo abarcan en su totalidad, ya que son escasas las definiciones relacionadas con el proceso judicial y criminalístico. Es necesario considerar todo el entorno involucrado en un acto delictivo, sumando a los procesos técnicos los componentes del Derecho Procesal y de la investigación criminal para asegurar la integridad de la posible evidencia digital.

Por otra parte, Rashid [5] menciona que el Modelo de Análisis de Tareas Cognitivas propuesto originalmente por Pirolli [9] se adecua al proceso cognitivo que requiere el análisis forense, particularmente por la naturaleza iterativa de las distintas fases, en las que se encuentran fuentes potenciales de evidencia —que se consulta y filtra por relevancia— mediante un proceso iterativo de ajuste en espiral; y por otra parte, también está presente un bucle de construcción del caso que se nutre iterativamente a la vez que la evidencia toma sentido en el contexto del análisis que se está realizando.

Así, es posible observar la interacción entre la hipótesis de trabajo (en este caso los puntos de pericia que se deben responder) y la evidencia encontrada, ya que nueva evidencia puede requerir la redefinición de la hipótesis de trabajo, así como, la redefinición de esta última impacta en los criterios de búsqueda de la evidencia digital.

Desde el enfoque de la iteración de procesos, es de interés la metodología PURI (Proceso Unificado de Recuperación de Información) [10] en la que se incorporan elementos de la Ingeniería de Software conjugados con criterios forenses que ordenan el procedimiento. A lo que suman otros aspectos, como el enfoque ingenieril de los procesos, la definición de perfiles y funciones de los investigadores forenses, que hacen posible considerar esta metodología como base para GAFIoT.

PURI toma el modelo de Proceso Unificado para desarrollo de software, que se caracteriza por estar dirigido por casos de uso, centrado en la arquitectura y por ser iterativo e incremental. El modelo agrupa las tareas en actividades de mayor abstracción, y a éstas en fases. A su vez, el esquema se complementa con las técnicas para llevar a cabo cada una de esas tareas y las herramientas disponibles que ejecutan dichas técnicas. La Figura 2 esquematiza el proceso PURI, señalando las seis fases: Relevamiento, Recolección, Adquisición, Preparación, Extracción-Análisis y Presentación.

Es importante considerar a qué se denomina fase, entendiendo por tal a cada uno de los estados sucesivos en el que puede encontrarse un proceso de recuperación de información que se ejecute sobre el modelo. Estas fases son sucesivas debido a que llevan un orden lógico; están compuestas por actividades, y cada una de estas actividades engloba un conjunto de tareas, las que pueden o no realizarse, de acuerdo al caso y al objeto de estudio.

La Figura 3 grafica las actividades y tareas incluidas en cada fase.

PURI define los niveles de conocimiento que deben tener los expertos forenses, identificando roles propios: a) *Responsable de Identificación* de la evidencia (trabaja en la escena del delito); b) *Especialista en Recolección* (calificado para recolectar los soportes que contienen la evidencia digital); c) *Especialista en Adquisición* (experto en herramientas forenses); y d) *Especialista en Evidencia Digital* (a cargo del análisis, investigación y gestión general del proyecto forense).

4.2. Marcos metodológicos propuestos para la forensia de entornos IoT

Para el presente estudio se tomó como base la investigación de Patel et al. [1], que analiza un conjunto de metodologías para forensia de IoT, y se completó el listado con otras propuestas surgidas de la revisión bibliográfica realizada.

Kebande & Indrakshi [11] proponen DFIFIoT (Digital Forensic Investigation Framework for Internet of Things) como framework de trabajo. El modelo incluye tres módulos diferenciados: proceso proactivo, forensia de IoT y proceso reactivo. En el primer módulo se incluyen las actividades de preparación forense del Entorno IoT (detalladas como definición del Entorno IoT, identificación de las fuentes de evidencia IoT, planificación de la detección del incidente, recopilación, presentación y almacenamiento de la potencial evidencia digital), mientras que el segundo módulo aborda los métodos de extracción de la evidencia en dispositivos IoT (en particular: análisis forense de la nube, análisis forense de redes y análisis forense a nivel dispositivos), y por último, el módulo reactivo incluye las actividades que permiten identificar el incidente delictivo (inicialización, adquisición e investigación forense). A la vez, la metodología incluye un conjunto de procesos concurrentes a los módulos indicados, para abordar la autorización de acceso a los datos, la documentación técnica, el registro de la cadena de custodia, la investigación física y la interacción entre los investigadores.

Por su parte, este mismo autor [12] avanzó con una propuesta superadora de la anterior, definiendo CFIBD-IoT, una metodología centrada en la nube para el aislamiento de pruebas forenses de Big Data en Entornos IoT. Basado en el esquema clásico del análisis forense (identificación, extracción, análisis y preservación de los datos), esta propuesta recurre las normas ISO/IEC 27043: 2015 e ISO/IEC 23037: 2012 y a la ayuda de técnicas de agentes inteligentes, virtualización y estructuras complejas de almacenamiento de datos para sostener las distintas etapas de la tarea forense. Lo interesante de este trabajo es la presentación de las vistas del proceso forense, con detalle de la participación del especialista forense que hace la extracción de datos y del investigador forense, en cada una de las actividades propuestas por esta metodología. Si bien este marco de trabajo es técnicamente robusto, carece de una mención expresa de los aspectos complementarios del análisis forense (planifica-ción, realización de informes, ajuste a normas procesales y criminalísticas).

Siguiendo con esta línea, el mismo equipo de investigación liderado por Kebande [13] propone IDFIF-IoT, una extensión de la metodología DFIFIoT, en el que se introduce el concepto de *ecosistema IoT* (conjunto complejo e integrado de relaciones y dispositivos IoT y dispositivos inteligentes). Además de los módulos de gestión habituales en un Entorno IoT (gestión de los dispositivos IoT, procesos de comunicación con las redes) el marco de trabajo de IDFIF-IoT incluye varios elementos que conforman el ecosistema IoT, como por ejemplo: a) las políticas de IoT de la organización que se está estudiando, para estudiar las estrategias de seguridad, interoperabilidad, estandarización y posibles legislaciones y regulaciones de IoT comprometidas; y b) las técnicas para el análisis de la potencial evidencia digital basadas en la familia de normas ISO/IEC 27000.

Meffert et al. [14] presentan por su parte un framework denominado FSAIoT (Forensic State Acquisition from Internet of Things), con un enfoque fuertemente orientado al proceso de identificación de la evidencia digital. La propuesta consta de un *controlador centralizado,* orientado a la identificación de los *estados* del dispositivo IoT (puerta abierta o cerrada por ejemplo), así como de los servicios de la nube que consumen estos dispositivos y un tercer método dirigido al control de la interface de comunicación con el investigador forense. Lo interesante de este trabajo son las pruebas de concepto realizadas mediante la aplicación del método a un Entorno IoT de laboratorio en el que se probaron el control de estado de 5 tipos de sensores diferentes. Por último, los autores identificaron algunas limitaciones del proyecto, destacando expresamente las restricciones de acceso a datos históricos o borrados, así como los problemas de los protocolos de comunicación de los distintos tipos de sensores (wifi, Bluetooth, Zigbee y Zwave, etc.). No hay mención de cuestiones complemen-tarias del análisis forense en sí mismo, como

mecanismos de preservación de la evidencia, cadena de custodia, elaboración del informe y presentación de la evidencia en la corte de justicia, entre otros.

El framework FIF-IoT propuesto por Hossain et al. [15], recurre a la tecnología blockchain para registrar hechos en incidentes criminales en Entornos IoT. FIF-IoT recopila interacciones que tienen lugar entre varios elementos de IoT (nubes, usuarios y dispositivos) y las resguarda de modo seguro garantizando la integridad, confidencialidad, privacidad y no repudio de la evidencia digital obtenida. Los autores citan como principales contribuciones de la investigación la propuesta de un marco de investigación forense para IoT utilizando tecnología blockchain descentralizada y distribuida; la definición de un modelo confiable para la recolección, manipulación y almacenamiento de la evidencia; y las pruebas de análisis de seguridad de FIF-IoT realizadas sobre un prototipo basado en Contiki (sistema operativo de código abierto utilizado en ordenadores de 8-bit microcontroladores y sensores).

La herramienta recopila las interaccio-nes de IoT creando transacciones con los datos intercambiados en cada interacción, luego se almacenan en el ledger y se crean los bloques de interacción combinándolos, por último, se agregan a la blockchain pública, distribuida y descen-tralizada. Las interacciones pueden ser de 3 tipos: cosas-usuarios, cosas-nube y cosas-cosas. De cada transacción se registra con precisión la acción y la identidad de las partes involucradas. Si bien se destacan las ventajas de blockchain para resguardo y manipulación de la evidencia digital, la propuesta no incluye otros aspectos del proceso forense.

La propuesta de Chhabra et al. [16] recurre a la inteligencia artificial para conformar un marco de trabajo que incluye: herramientas de machine learning para la traducción, extracción y análisis de tráfico malicioso en la red; funciones de extracción-transformación-carga de datos masi-vos en tiempo real; y técnicas de aprendizaje automático para actualizar el sistema experto que se va generando. La metodología propuesta contempla 4 módulos de trabajo: 1) recolección de datos y generación de información, 2) análisis y extracción, 3) Diseño de modelos de aprendizaje automático y 4) Análisis de modelos sobre diversas matrices de eficiencia. Estos autores presentan un marco sólido para la extracción y análisis de la evidencia digital obtenida del Entorno IoT, pero no se incluyen los restantes pasos del proceso forense (planifi-cación, preservación de la evidencia, entre otros).

Al-Masri [17] propone FoBI, un marco de trabajo para el análisis forense basado en Fog Computing (computación en la niebla), una arquitectura en la que las aplicaciones se concentran en los dispositivos al borde de la red, permitiendo que los datos puedan ser procesados localmente en un dispositivo inteligente en lugar de ser procesados en la nube. FoBI está conformado por seis módulos: a) gestión y monitoreo de dispositivos; b) analizador forense; c) recuperación de evidencia; d) notificación de casos; e) comunicación; y f) almacenamiento local. El módulo de comunicación permite la conexión con los dispositivos IoT de manera automática y la generación del entorno necesario para el envío y recepción de los datos. Considerando que cada dispositivo de IoT se identifica con una dirección IP o MAC, se toma el tráfico entre ese dispositivo y las redes externas, y se procesa con herramientas de análisis de tráfico de red para identificar los datos básicos (fecha, hora, tipo de paquete, etc.) y distinguir cualquier actividad sospechosa. Al incluir computación en la niebla, la propuesta es innovadora y podría completarse con la inclusión de otras partes del proceso forense relativas al resguardo de la evidencia, elaboración del informe final, entre otras.

IoTDots es propuesta por Babun et al. [18], para el análisis forense de entornos inteligentes, como casas u oficinas inteligentes. Este marco de trabajo cuenta con dos módulos: el modificador y el analizador. El primero de ellos considera el código fuente de las aplicaciones inteligentes y detecta información de relevancia forense, sobre eventos y estados (acciones, interacciones con los usuarios, información de los dispositivos, tiempos y localizaciones), que ocurren en el entorno inteligente en tiempo de ejecución y automáticamente inserta registros de seguimiento que se almacenan en una base de datos propia. Luego, el módulo analizador aplica técnicas de aprendizaje automático para extraer datos de interés forense sobre las actividades de los

dispositivos IoT involucrados. Este marco de trabajo está centrado en los procesos de extracción y análisis de la evidencia, sin considerar expresamente las restantes etapas del proceso forense (planificación, preservación, informes y presentación de la evidencia).

Otro framework de interés para el presente trabajo es DFIM (Digital Forensics Investigation Model), propuesto por Qatawneh et al. [19], que consta de 7 pasos: 1) la pre-investigación que incluye actividades de inicialización, validación, selección y preparación del Entorno IoT que resulten de interés para el análisis forense; 2) recolección y evaluación de los datos que son posible evidencia digital; 3) conservación de la posible evidencia en términos de la integridad y manipulación requeridos por el análisis forense mediante algoritmos hash; 4) examen y análisis de la posible evidencia recolectada; 5) intercambio de información con entidades remotas para compartir evidencia entre los investigadores forenses; 6) elaboración del informe y documentación sobre el proceso forense realizado ajustándolo a los requerimientos formales exigidos por la justicia; y 7) revisión final del informe por parte del investigador líder previo a su presentación ante la corte de justicia.

Se propone un modelo para entender el Entorno IoT, a partir de las 3 zonas en las que puede encontrarse la evidencia digital: la zona de la nube (servidores de Internet con capacidades ilimitadas en términos de almacena-miento y procesamiento); zona de niebla (servidores intermedios entre los dispositivos y los servidores en la nube, más cercanos a la zona de percepción) y la zona de percepción (sensores, computadoras, teléfonos inteligentes, cámaras, humanos, vehículos, electrodomésticos, etc.). Y además identifica dos componentes muy claros en el proceso forense: la zona de datos que contiene todos los datos relevados y reunidos en distintos grupos, y la autoridad de investigación que recibe las solicitudes de investigación, las valida y finalmente seleccione los investigadores apropiados.

En el trabajo de Islam et al. [20] se observa el estudio de forensia en Entornos IoT, con énfasis en la utilización de técnicas criptográficas para reducir el riesgo de manipulación de datos y facilitar el proceso de investigación forense. La propuesta se basa en un modelo de seguridad de datos y un modelo de investigación forense. El primero de ellos incluye algoritmos de encriptación sincrónicos, asincrónicos y hash, que se proponen en los sucesivos procesos de tratamiento de los datos que se están trabajando. Mientras que el modelo de investigación forense contempla cinco módulos distintos: 1) Planificación Inicial del análisis forense (identificación del Entorno IoT, identificación de las fuentes de la potencial evidencia, planificación de la tarea forense); 2) Conformación de un repositorio protegido para la preservación segura de la posible evidencia a obtener; 3) Estudio del incidente y planificación del análisis forense a realizar; 4) Adquisición de la posible evidencia digital; y 5) Investigación Forense (análisis de la evidencia IoT, elaboración de informes y presentación de los mismos, procesos de prueba y defensa, cierre de la investigación).

Koroniotis [21] propone un marco forense basado en redes neuronales para el análisis del tráfico de red, llamado PDF (Particle Deep Framework) que permite identificar y rastrear comportamientos de ataque en redes de IoT. Se basa en tres funciones esenciales: 1) extracción del tráfico de red y verificación de su integridad; 2) uso de un algoritmo de optimización para adaptar automáticamente los parámetros de aprendizaje profundo; y 3) desarrollo de una red neuronal profunda para descubrir y rastrear eventos anormales de la red IoT. La propuesta es innovadora al utilizar las redes neuronales para el armado de un espacio de análisis inteligente de la evidencia, y debería complementarse con las restantes etapas del proceso forense (planificación, preservación, informe y presentación de la evidencia).

Por último, Costantini et al. [22] abordan la *calidad de la información* en el análisis forense de Entornos IoT, teniendo en cuenta los diferentes niveles de complejidad y factores humanos incluidos.

Los autores proponen un marco formal para evaluar la calidad de la información de los dispositivos de IoT obtenidos en el análisis forense, considerando la información desde tres estados ontológicos diferentes: "Información *como* realidad" (por ejemplo, la señal eléctrica, que se transmite independientemente del mensaje

contenido); "Información *sobre* la realidad" (aquella acerca de los fenómenos naturales que pueden ser verdaderos o falsos) e "información *para* la realidad" (que transmite instrucciones o algoritmos a uno o varios destinatarios).

En el contexto de la Forensia Digital, la calidad de la información impacta según distintos órdenes. Primeramente, la calidad es relevante para preservar la integridad de la información recopilada, siendo fundamental en la cadena de custodia. El segundo tipo de calidad se refiere a la confiabilidad de la representación de los hechos, que debe ser verificado con otras fuentes de evidencia (aquí es importante considerar el carácter de *prueba indiciaria* que habitualmente se asigna a la evidencia digital). Un tercer espacio en el que interesa la calidad de la información, es el ámbito de discusión de la evidencia entre las partes (jueces, abogados, policías, peritos forenses), en el que intervienen criterios subjetivos y de competencia de cada parte. El modelo de trabajo parte de principios sólidos de la Forensia Digital: para ser admisible en términos del análisis forense la información adquirida debe ser, al mismo tiempo, legible y comprensible como datos digitales, y adquirida y preservada respetando las mejores prácticas forenses. Así, los autores definieron un modelo matemático para la formulación de un coeficiente de evaluación de la calidad de la información basado en los siguientes conceptos:

- Estado técnico del dispositivo (funcionamiento correcto o no)
- Nivel de protección del dispositivo (en términos de la confidencialidad, integridad y disponibilidad de los datos)
- Nivel de seguridad de los servicios de la nube con los que interactúa el dispositivo
- Nivel de manipulación de datos en los servicios de la nube
- Confiabilidad de la fuente (posibilidad de que el observador posea información adicional sobre la fuente que origina los datos)
- Cumplimiento de las normativas de protección de datos (en diseño de los dispositivos y/o en el procesamiento de los datos).
- Accesibilidad técnica de los datos (en términos de la adquisición y formato)
- Avance tecnológico del analista forense (herramientas analíticas utilizadas para recopilar y procesar evidencia).
- Grado de experiencia, habilidades y destrezas del analista forense.

La aplicación de este modelo matemático, basado en una fórmula ponderada, puede indicar una estimación más certera sobre el grado de calidad de la información relevada en el análisis forense. Este aspecto es el más destacable de la propuesta, y de sumo interés para el proceso forense, aun cuando no contempla detalladamente las restantes etapas del proceso forense.

4.3. Análisis comparativo de las metodologías descriptas

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 anali-zando, incluyendo no solo los procesos técnicos relativos al tratamiento de la evidencia digital, sino también, las actividades propias de la inves-tigación 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 siguientes etapas: 1) Planificación de las actividades; 2) Identificación de la Evidencia; 3) Extracción de la Evidencia; 4) Preservación de la Evidencia; 5) Análisis y Correlación de los Datos; y 6) Informe y Presentación de la Evidencia. Todo ello con el desarrollo concurrente de las normas procesales judiciales y de investigación.

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 (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 considerador. La tabla finaliza con una

Tabla 1. Cuadro comparativo de metodologías de IoT analizadas

	DFIFIoT	CFIBD-IoT	IDFIF-IoT	FSAIoT	FIF-IoT	Chhabra	FoBI	IoTDots	DFIM	Islam	PDF	Costantini
1. Planificación	Si	No	Si	No	No	No	No	No	Si	Si	No	No
2. Identificación de la evidencia	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
3. Extracción	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
4. Preservación	Si	Si	Si	No	Si	No	No	No	Si	Si	Si	No
5. Análisis y correlación de los datos	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
6. 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%

línea que señala el *grado de completitud* o porcentaje de cumplimiento de la metodología, en relación a 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 descriptos en la sección 4.2 solo 4 (DFIFIoT [11], IDFIF-IoT [13], DFIM [19] y la propuesta de Islam et al. [20]) incluyen de manera completa las 6 etapas señaladas del proceso forense, y además, consideran las normas procesales y de investigación requeridas por la justicia. 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 [12] 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 [14] 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 metodo-logías tradicionales de análisis forense.
- FIF-IoT [15], 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. [16] incorpora herramientas que permiten procesar la evidencia digital en términos de un sistema experto; FoBI [17] presenta un modelo basado en computación en la niebla; IoTDots [18] está centrado en la extracción de datos aplicando técnicas de aprendizaje automático; mientras que PDF [21] propone un marco forense basado en redes neuronales profundas.
- La propuesta de Costantini et al. [22] 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.

5. Propuesta de una guía de actuación forense para entornos IoT (GAFIoT)

GAFIoT está basada en la metodología PURI [10] 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

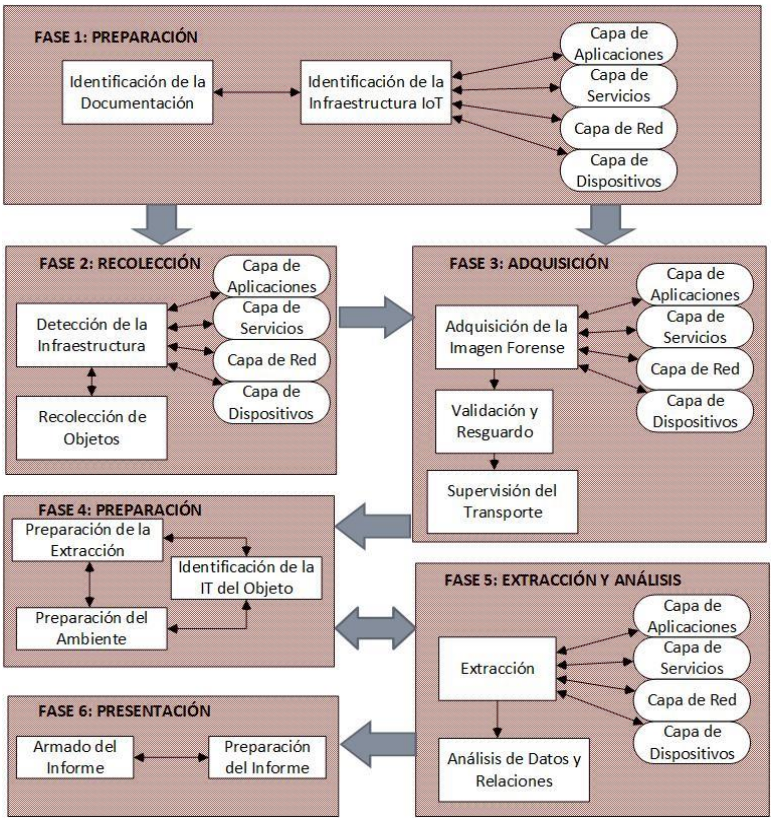

Fig. 4. Guía de actuación para forensia de entornos IoT (GAFIoT)

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 características de casos de uso, iteración y trabajo multidisciplinario definidos para PURI.

La Figura 4 describe 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 de la Documentación* 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.

Lo mismo ocurre con las actividades definidas sobre las capas del Entorno IoT, ya que es necesario considerar cada capa en particular pero sin descuidar la interacción de ésta sobre las restantes capas.

De igual forma, las Fase 4y 5 se alimentan mutuamente hasta que los resultados obtenidos se consideran satisfactorios. A continuación se describen las fases de GAFIoT.

5.1. Fase de relevamiento

Aquí PURI incluye dos actividades principales: Identificación de la Documentación e Identificación

de la Infraestructura IT, las que se adecuan y mantienen en GAFIoT.

En la *Identificación de la Documentación*, se tratan los aspectos comunes a los proyectos de análisis forense (revisión de la documentación legal, administrativa, de seguridad física y lógica del caso), que ayudan a conocer el problema en profundidad y a formular estrategias adecuadas.

La actividad de *Identificación de la Infraestructura IT* permite entender cuál es el entorno tecnológico en el que se trabajará. Es necesario identificar las características técnicas del mismo, considerando: arquitectura de procesamiento, cantidad de usuarios intervinientes, dispositivos y servicios potenciales puestos a disposición de los mismos, etc. Este paso es de suma importancia para preparar adecuadamente las siguientes fases. Cuando se trata de Entornos IoT, esta actividad se realiza en base al modelo de 4 capas antes descripto. Las técnicas aconsejadas se orientan a conocer la funcionalidad y características de la infraestructura, mediante la búsqueda en la web de documentos técnicos pertinentes o la consulta a fabricantes o expertos técnicos en componentes del Entorno IoT. Aquí puede ayudar el modelo propuesto por DFIM[19] respecto de las tres zonas fuente de evidencia digital.

Esta fase finaliza con el modelo de procesamiento propio para el caso en estudio, identifi-cando en lo posible, los componentes particulares de cada capa.

5.2. Fase de recolección

Cuando el juez requiere de la intervención de un especialista forense digital, usualmente se presentan dos escenarios:

- Los equipos de soporte de la evidencia ya fueron recolectados (en acciones de allanamiento ya ejecutadas o por entrega de alguna de las partes del juicio) y le son entregados al especialista para que continúe con las siguientes etapas del proceso; o
- Se debe realizar la recolección de los mismos con presencia del especialista forense en el lugar (en casos de allanamiento o medidas de prueba anticipada). Es en este último caso en que esta etapa es necesaria.

PURI propone un conjunto de acciones necesarias para obtener los equipos físicos, y/o las posibles fuentes de datos, sobre los cuales se deberá trabajar posteriormente definiendo dos actividades principales que interactúan entre sí y se nutren una a la otra: Detección de la Infraestructura y Recolección de Objetos.

Respecto de la *Detección de Infraestructura*, 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 puede 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 además 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 [13] 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.

La actividad de *Recolección de Objetos* como dispositivos de soporte o fuente de evidencia digital, debe respetar estrictamente la Cadena de Custodia, cuidando de realizar correctamente las tareas de secuestro, 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 juris-dicciones en las que se desarrolla la actuación.

5.3. Fase de adquisición

Para esta fase, PURI propone actividades tendientes a la adquisición de la imagen forense de la posible evidencia digital que pudiera encontrarse en todos los componentes del Entorno IoT, utilizando las técnicas y herramien-tas más adecuadas para cada caso. Siguiendo el modelo de referencia de IoT de las cuatro capas, en GAFIoT esta etapa debe incluir las siguientes actividades:

- *Adquisición de datos de las aplicaciones IoT*: como habitualmente estas aplicaciones se encuentran residentes en el dispositivo de interacción del usuario con el sistema IoT (teléfonos inteligentes, tablet, etc.), las técnicas y herramientas a utilizar son las conocidas en la forensia digital para el análisis de estos dispositivos, tales como FTK Imager[1] u otras similares.
- *Adquisición de datos de los servicios de apoyo*: en este caso se debe realizar una imagen forense realizando la recolección en caliente, es decir, con el sistema IoT en pleno funcionamiento.
- Es probable que no sea posible acceder completamente a todos los componentes de esta capa, principalmente por la reticencia de los proveedores de servicios a colaborar voluntariamente con la justicia. La adquisición de datos de esta capa consiste en obtener la imagen forense de todos los artefactos forenses (registros internos) que sea posible, en los que se registren las características de utilización de dichos servicios, así como de las memorias caché disponibles.
- *Adquisición de datos de Red*: habitualmente la imagen forense se realiza utilizando técnicas de *sniffing (*permite la captura de distintos paquetes que circulan en una red) para obtener estos datos, obteniendo información sobre las capas de protocolos, el contenido de los paquetes, datos que han sido retransmitidos, así como patrones de tráfico y situaciones anómalas. Son varias las herramientas disponibles (NetworkMiner[2], WireShark[3] entre otras).
- *Adquisición de datos de los dispositivos IoT*: la comunicación con las “cosas” se realiza mediante los sensores que toman las señales y las envían a los dispositivos de mayor nivel que hacen el procesamiento de esas señales. Si el sensor cuenta con una memoria básica tipo EEPROM (Electrically Erasable Programmable Read-Only Memory), y siempre que sea posible debería enfocarse el proceso de adquisición de datos recurriendo a herramientas tradicionales de volcado de memoria. Podría realizarse la imagen forense utilizando la técnica de *crashdump* (forzar un malfuncionamiento del sistema operativo para que él mismo genere una copia de la memoria principal) y proceder al volcado de la misma con herramientas como Volatility[4]. También puede considerarse la extracción del estado (prendido/apagado) de los dispositivos IoT, según el modelo propuesto por FSAIoT [14].

El desarrollo completo de las actividades de adquisición precitadas dependerá de la factibilidad de acceso a 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 puede depender de si fue posible secuestrar los dispositivos utilizados, mientras que el acceso a los dispositivos IoT dependerá de la factibilidad geográfica y física de acceder a las “cosas” que estos dispositivos controlan.

También puede recurrirse al *carving de archivos* (recuperación y reconstrucción del contenido del archivo directamente desde el

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

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

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

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

almacenamiento en bloque sin utilizar los metadatos del sistema de archivos), 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. Aunque debe tenerse presente las dificultades de usar estas técnicas en Entornos IoT mencionadas por Rashid [5].

Algunas de las metodologías analizadas en la sección 3.2 (CFIBD-IoT [12],Chhabra et al. [16], FoBI [17]; IoTDots [18] y PDF [21]) proponen la utilización de tecnologías de aplicación habitual en los sistemas de información pero innovadoras en el contexto de la Forensia Digital, tales como los agentes inteligentes, sistemas expertos, computación en la niebla, aprendizaje automático y redes neuronales. Estas propuestas basadas en tecnologías novedosas, se miran con mucho interés desde la Forensia Digital, a la espera de que logren un grado de madurez y confiabilidad suficientes como para que puedan incorporarse al proceso forense de manera formal, para dar respuesta al análisis forense en contextos tecnológicos complejos como el Entorno IoT.

Para PURI esta fase se completa con las actividades de *Validación y Resguardo* de la evidencia adquirida, y si corresponde, *Supervisión del Transporte*, que también son válidas para el análisis forense de Entornos IoT. La 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 [15], de usar tecnología blockchain para garantizar la integridad, confidencialidad y privacidad de la evidencia digital obtenida.

Y 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.

5.4. Fase de preparación

Esta fase es genérica cualquiera sea el tipo de evidencia que se debe analizar, así que las recomendaciones de PURI son válidas también para la forensia de Entornos IoT. Aquí se involucran las actividades técnicas previas al análisis forense en sí mismo.

GAFIoT toma las 3 actividades propuestas: *Preparación de la extracción, Identificación de la tecnología informática del objeto* y *Preparación del ambiente*, requeridas para disponer de un ambiente de trabajo que sea adecuado y suficiente (usualmente un Laboratorio Forense), en el que se realizará el análisis de las evidencias digitales obtenidas en las fases previas.

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 y la selección de las metodologías, técnicas o guías procedimentales que correspondan al caso.

5.5. Fase de extracción y análisis

PURI destaca que al llegar a esta fase, debe considerarse de manera integrada dos tareas fundamentales: *Extracción y Análisis*, puesto que ambas están muy interrelacionadas y casi resultan una sola, ya que al momento de hacer la extracción de la posible evidencia, también se la está analizando.

La extracción suele ser automa-tizada, e integrada por actividades netamente técnicas, mientras que el análisis implica un proceso de interpretación de los datos extraídos en el contexto de los puntos periciales y el interés de los investigadores.

GAFIoT propone realizar la extracción y análisis en las 4 capas del modelo IoT:

- *Extracción a nivel Capa de Aplicación*: implica acceder a la información de ejecución de las aplicaciones que se utilizan en el Entorno IoT, usualmente residen en el dispositivo que utiliza el usuario final, por lo que se procederá a extraer datos relevantes sobre el uso de la aplicación (archivos históricos, registros internos, etc.). Es común ampliar la búsqueda hacia todo aquello que indique alguna actividad en internet (URL visitadas, historial de búsquedas, archivos descargados, claves almacenadas, cookies, etc.).
- *Extracción a nivel Capa de Servicios*: aquí se obtienen los datos de ejecución de los distintos servicios (los datos históricos y en tiempo real

si fuera posible), mediante el acceso a los logs y configuración de los servicios con las herramientas de apoyo y gestión que habitualmente se encuentran en las API de los servicios en la nube.

- *Extracción a nivel Capa de Red*: en este caso, la extracción de datos se orienta a la plataforma de red del Entorno IoT. Datos sobre los sistemas operativos, sistemas de archivos, procesos en ejecución, colas de datos no entregados y configuración de las redes son de interés.
- *Extracción a nivel Capa de Dispositivos*: siempre que sea posible, se realiza el acceso a las memorias de los dispositivos IoT. Esto puede involucrar el análisis de la memoria EEPROM de los sensores que comunican las "cosas" con el sistema IoT.

Estas actividades requieren que el profesional forense tenga competencias en el Entorno IoT, y si así no fuera, se debe convocar a expertos técnicos que ayuden al entendimiento de la arquitectura de procesamiento.

La fase continúa con la actividad de *Análisis de Datos y Relaciones* que los vinculan con el fin de encontrar su peso, relevancia y significancia en el caso atendiendo fundamentalmente a los requerimientos de los puntos de pericia.

El análisis se realiza en base a las búsquedas y correlaciones de datos 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, vincularlas en pos de un mismo objetivo, recurriendo para ello al enfoque sistémico y el enfoque estratégico del Entorno IoT, que le permitirá relacionar la evidencia con el caso delictivo que se está analizando.

5.6. Fase de presentación

En esta última fase, GAFIoT toma la propuesta de PURI para la confección de los informes necesarios y la presentación del caso en el juicio. Las actividades involucradas son dos: *Armado del Informe* y *Presentación del Informe.*

La primera de estas actividades incluye la escritura del Informe Forense Final que usualmente contiene dos partes:

- *Informe Forense*, que debe contener los datos de identificación del caso, el detalle de la evidencia digital procesada, la metodología y herramientas utilizadas, más la respuesta a los puntos de pericia requeridos. Este informe está escrito en términos adecuados para la lectura por parte de los interesados no informáticos. Cuando se trata de Entorno IoT, el informe debe abundar en definiciones de conceptos de base (la arquitectura de procesamiento por ejemplo), a fin de que los profesionales no tecnológicos comprendan de mejor manera 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 *Preparación del Informe* 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 (satinización del soporte y tratamiento contra escritura, grabación y encriptación de los archivos).

6. Plan de Validación de GAFIoT

GAFIoT se formuló como una adecuación del proceso PURI enriquecido con aportes de otras investigaciones referidas a las metodologías forenses de IoT.

La propuesta 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.
- 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 diferentes *escenarios forenses*, como por ejemplo: contextos de seguridad electrónica del hogar o sistemas IoT aplicados a la salud de las personas.

Este plan de validación avanzó lentamente en el año 2020 debido a la situación de confinamiento general ocurrida por la pandemia de COVID-19, pero se espera retomarlo prontamente. Para las actividades referidas a pruebas experimentales, se cuenta con un Laboratorio Forense Digital [23] en el que está previsto la implementación de un Laboratorio de Forensia de IoT [24].

7. Conclusiones

Se considera que una vez validada, GAFIoT podría utilizarse como marco de trabajo para el analista forense presentando —entre otros beneficios— los siguientes:

- Ordena el proceso forense al identificar las actividades de cada fase según las distintas capas del modelo IoT.
- GAFIoT se ajusta al proceso general forense, respetando las actividades y criterios requeridos por las buenas prácticas de la investigación forense.
- Basada en el modelo general del análisis forense, los criterios de iteración de procesos presentes en GAFIoT permite responder a los modos propios de la gestión ingenieril de proyectos.
- GAFIoT incluye actividades lo suficientemente genéricas como para ajustar la tarea forense a diferentes Entornos IoT, conside-rando estos sistemas de manera integral, más allá de los componentes individuales y específicos que lo integren.

Las líneas de investigación que pueden derivarse de este trabajo marcan varias vías a seguir:

- Es posible extender los alcances de GAFIoT para su utilización en la forensia de incidentes de seguridad informática de interés de las empresas. Este entorno no judicial tiene características que deberán sumarse a GAFIoT, como ser: involucrar en el proceso forense al área de seguridad informática de la empresa involucrada; incorporar las políticas de seguridad y todo lo relacionado a ella como elemento de análisis de la posible evidencia digital; y particularmente si se trata de un incidente de seguridad en el Entorno IoT, se deberá sumar el área de seguridad física de las instalaciones.
- También sería de interés abordar como otra línea de investigación, la factibilidad de la propuesta Costantini et al. [22] para validar la calidad de la información de la evidencia obtenida. Un modelo matemático brinda mayor certeza, siempre que se pueda obtener la información requerida para computar el modelo y el especialista forense tenga competencias para ponderar y aplicar los datos relevados en el modelo matemático. También puede considerarse la aplicación del método propuesto por Pavón [25] para medir la calidad de los datos según sus dimensiones de exactitud, completitud y consistencia, identificando la pérdida de la calidad de los datos en contextos de interés como los métodos de encriptación.
- Otro aspecto que debe investigarse es la incorporación de procesos que permitan seleccionar adecuadamente la posible evidencia digital, separando aquellos datos

no vinculantes a la causa para asegurar la protección y privacidad de terceros ajenos al delito. La mayoría de las veces, la "separación" de los datos pertinentes a la causa queda a criterio del especialista forense, ocasionando que involuntariamente se acceda a información de terceros que no resultan de interés. En el Entorno IoT esta situación se magnifica, por la escasa aplicación de políticas de seguridad que abarquen todo el contexto de IoT, ya que habitualmente los criterios de aplicación de la seguridad en cada una de las 4 capas del modelo IoT son distintos. Es decir, la forensia de Entornos IoT con impacto directo en el cuerpo, la vida y la salud de las personas debe estudiarse particularmente para dar una respuesta adecuada, con foco en dos puntos: el supuesto acto delictivo y la protección de datos de terceros no involucrados.

Referencias

1. **Unión Internacional de Telecomunicaciones (2012)**. Descripción General de Internet de los Objetos. pp. 20.
2. **Palmer G. (2001)**. A road map for digital forensic research. First Digital Forensic Research Workshop, Utica, New York, pp. 27–30.
3. **Patel, R., Malek, Z. (2020).** Brief overview of existing challenges in IoT. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 9, No. 3.
4. **Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis E. (2020).** A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials, Vol. 22, No. 2, pp. 1191–1221.
5. **Rashid, A., Chivers, H., Danezis, G., Lupu, E., Martin, A. (2019).** The cyber security body of knowledge (CyBoK) 1.0.
6. **Vallejo, M., Muñoz, G., Rosales, J. (2018).** Kids and parents privacy exposure in the internet of things: How to protect personal information?, Computación y Sistemas, Vol. 22, No. 4. pp. 1191–1205.
7. **Escamilla-Ambrosio, P., Robles-Ramírez, D., Alsalamah, S. (2019).** Securing mHealth applications using IoTsecM security modelling: Dentify. Computación y Sistemas, Vol. 23, No. 4, pp. 1139–1158.
8. **Atlam, H., Wills, G. (2020).** IoT security, privacy, safety and ethics. Digital Twin Technologies and Smart Cities. Springer, Cham, pp. 123–149.
9. **Pirolli, P., Card, S. (2005).** The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis, Proceedings of international conference on intelligence analysis, Vol. 5, pp. 2–4.
10. **Di-Iorio, A., Castellote, M., Constanzo, B., Curti, H. (2017).** El rastro digital del delito: Aspectos técnicos, legales y estratégicos de la informática forense. Editorial UFASTA.
11. **Kebande, V., Ray, I. (2016).** A generic digital forensic investigation framework for Internet of Things (IoT). IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 356–362. DOI: 10.1109/FiCloud.2016.57.
12. **Kebande, V., Karie, N., Venter, H. (2017).** Cloud-centric framework for isolating big data as forensic evidence from IoT infrastructures. International Conference on Next Generation Computing Applications (NextComp), pp. 54–60. DOI: 10.1109/NEXTCOMP.2017.8016176.
13. **Kebande, V., Karie, N., Michael, A., Malapane, S., Kigwana, I., Venter, H., Wario, R. (2018).** Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. IEEE International Conference on Smart Internet of Things (SmartIoT), pp. 93–98. DOI: 10.1109/SmartIoT.2018.00-19.
14. **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. Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1–11.
15. **Hossain, M., Karim, Y., Hasa, R. (2018).** FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. IEEE International Congress on Internet of Things (ICIOT), pp. 33–40. DOI: 10.1109/ICIOT.2018.00012.
16. **Chhabra, G., Singh, V., Singh, M. (2020).** Cyber forensics framework for big data analytics in IoT environment using machine learning. Multimedia Tools and Applications, Vol. 79, No. 23, pp. 15881–15900.
17. **Al-Masri, E., Bai, Y., Li, J. (2018).** A fog-based digital forensics investigation framework for IoT systems. IEEE International Conference on Smart Cloud (SmartCloud), pp. 196–201. DOI: 10.1109/SmartCloud.2018.00040.

18. **Babun, L., Sikder, A., Acar, A., Selcuk-Uluagac, A. (2018).** IoTDots: A digital forensics framework for smart environments.
19. **Qatawneh, M., Almobaideen, W., Khanafseh, M., Al-Qatawneh, I., Al-Ain, P. (2019).** Dfim: A New digital forensics investigation model for internet of things. Journal of Theoretical and Applied Information Technology, Vol. 97, No. 24.
20. **Islam, J., Khatun, A., Roy, S., Kabir, S., Debnath, B. (2017).** A comprehensive data security and forensic investigation framework for cloud-iot ecosystem. *GUB* Journal of Science and Engineering, Vol. 4, No. 1.
21. **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, Vol. 110, pp. 91–106.
22. **Costantini, F., Galvan, F., De-Stefani, M., Battiato, S. (2020).** Assessing information quality in IoT forensics: Theoretical Framework and Model Implementation. *arXiv preprint arXiv: 2012.14663*.
23. **Luz-Clara, B., Aráoz-Fleming, J., Parra de Gallo, B. (2020).** Laboratorio de forensia digital: Propuesta de estructura y funcionamiento. X Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática - Ecuador.
24. **Rivetti, E., Gamarra, A., Parra de Gallo, B. (2020).** Proyecto de creación de un laboratorio de forensia de IoT. REDI. Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas UNLAM, Vol. 5 No. 1.
25. **Pavón, J., Lima, R., Dí-Pando, H. (2019).** Evaluation of data quality: A cryptographic approach. Computación y Sistemas, Vol. 23, No. 2, pp. 557–568.

Article received on 11/02/2021; accepted on 14/10/2021.
Corresponding author is H. Beatriz Parra de Gallo.