De un Proceso Unificado de Recuperación de la Información a un Protocolo de Actuación en Informática Forense

Ana Haydee Di Iorio[1], Pablo Cistoldi [2],
Sabrina Lamperti [3], Fernanda Giaccaglia[4], Bruno Constanzo[5]

[1] Ingeniera en Informática, Directora del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense: InFo-Lab, Instructor Informático en el Ministerio Público de la Provincia de Buenos Aires, Docente e Investigador en Universidad FASTA, diana@ufasta.edu.ar

[2] Abogado, Especialista en Derecho Penal, Agente Fiscal de la Unidad Funcional de Delitos Culposos del Ministerio Público de la Provincia de Buenos Aires, Investigador del InFo-Lab, pcistoldi@mpba.gov.ar

[3] Abogada, Especialista en Criminalidad Económica, Integrante de la Unidad Fiscal en Delitos Económicos del Ministerio Público de la Provincia de Buenos Aires, Investigador en InFo-Lab, slamperti@mpba.gov.ar

[4] Abogada, Investigador en InFo-Lab, Docente e Investigador en Universidad FASTA, fernandag@ufasta.edu.ar

[5] Ingeniero en Informática, Investigador en InFo-Lab, Docente e Investigador en Universidad FASTA, bconstanzo@ufasta.edu.ar

Sumario

I. Introducción

La Recuperación de Información contenida en medios digitales constituye en la actualidad uno de los mayores desafíos de las investigaciones criminales. Por un lado, las empresas desarrolladoras de tecnología buscan cada vez más proteger la privacidad de sus clientes, brindando opciones para impedir los accesos no deseados a software y dispositivos; y, por otro lado, la masificación del Cloud Computing facilita que una gran parte de la información sea almacenada en grandes servidores alojados con frecuencia en otros países. Sumado a esta realidad, existen otros aspectos técnicos y jurídicos que influyen sobre la labor de obtención de evidencia digital válida y con fuerza probatoria.

PURI[1]**:** El Grupo de Investigación de Informática Forense y Sistemas Operativos de la Facultad de Ingeniería de la Universidad FASTA define un Proyecto de Investigación con el fin de desarrollar un Proceso Unificado de Recuperación de Información (PURI), que sirva como guía técnica válida tanto para informáticos forenses como para los organismos de justicia.

PURI nace en el seno científico, con una visión amplia, considerando cuestiones legales generales de los principios forenses pero sin ajustarse a una normativa en particular.

InFo-Lab: La Procuración del Ministerio Público de la Provincia de Buenos Aires, Argentina, reconociendo la necesidad de un actuar acorde a la garantía del debido proceso en el ámbito de la informática Forense, convoca a la Universidad FASTA -creadora de PURI- y a la Municipalidad de General Pueyrredon con el objeto de fundar un Laboratorio de Investigación y Desarrollo de soluciones de Tecnología en Informática Forense ("InFo-Lab"), formalizándose mediante Convenio 5/14 de la Procuración General.

Los resultados de las investigaciones y desarrollos tecnológicos logrados por el Laboratorio podrán extenderse a la totalidad de los Ministerios Públicos de la República Argentina a través del Consejo de Procuradores y del Consejo Federal de Política Criminal, dando un alcance nacional al trabajo del equipo técnico marplatense.

Desde otra perspectiva, la iniciativa se inscribe en el impulso dado por el Municipio al desarrollo de una industria basada en la innovación y la sociedad del conocimiento. Asimismo la Secretaría de Seguridad, Justicia Municipal y Control de la Municipalidad de General Pueyrredón cuenta con un Centro de análisis estratégico del

1 Libro Colectivo: DI IORIO, A., SANSEVERO, R., CASTELLOTE, M., GRECO, F., CONSTANZO, B., WAIMANN, T. & PODESTÁ, A. "Determinación de aspectos carentes en un Proceso Unificado de Recuperación de Información digital"*, Anales de las 42 JAIIO.* 2013, pp. 1-13.

delito y la violencia, cuya misión es gestionar el conocimiento en materia de seguridad pública, mediante la producción, planificación, coordinación y evaluación de la información referida a la situación del delito y la violencia en el ámbito municipal, con la finalidad de contribuir a la toma de decisiones y de coordinar acciones con las autoridades de las diferentes instituciones e instancias que intervienen en la política de seguridad. Dicho centro cuenta con un equipo interdisciplinario de profesionales especializados en el análisis del delito.

PAIF: Uno de los objetivos del InFo-Lab es el desarrollo de un Protocolo de Actuación en Informática Forense (PAIF) para ser adoptado y promovido por el Ministerio Público de la Provincia de Buenos Aires como estándar oficial de trabajo, en base a lo establecido por el Proceso Unificado de Recuperación de Información (PURI).

II. El Proceso PURI: características.

El Proceso Unificado de Recuperación de Información es el resultado de años de investigación en la Universidad FASTA por el grupo de Investigación en Informática Forense que depende de la cátedra de Sistemas Operativos de la Facultad de Ingeniería. En el año 2011 comenzó el primer proyecto de investigación orientado a la creación de PURI. Se buscaron, estudiaron, compararon y evaluaron las guías de recomendaciones, guías de buenas prácticas, normas, y protocolos de actuación existentes hasta ese momento; para establecer un proceso general aplicable a la informática forense. Además de las guías propiamente dichas, fue necesario el estudio de diversos trabajos académicos para comprender las problemáticas con las que puede enfrentarse un informático forense[2].

El trabajo de investigación se prolongó hasta entrado el año 2012, en el que se propuso un modelo inicial de PURI. Durante el año 2012 se realizó una validación

2 Revista: PICCIRILLI, D. "La forensia como herramienta en la pericia informática". *Revista Latinoamericana de Ingeniería de Software*, 2013, Vol 1, núm. 6, pp. 237-240.

técnica de lo propuesto, evaluando el proceso sugerido y su aplicabilidad a distintos escenarios. La primer versión de PURI© adaptada a Equipos de Escritorio se finaliza en el año 2013. Posteriormente se detecta la necesidad de adaptar el proceso a Equipos Móviles, especialmente Smartphones y a Entornos Distribuidos[3]. Surgen así dos proyectos de investigación que aún están en curso.

En su concepción original, PURI es un proceso netamente técnico que cubre, desde el punto de vista del especialista informático, las tareas que deben llevarse a cabo para recuperar la información almacenada en un sistema informático, agrupando dichas tareas en etapas y fases de un proceso, recomendando las técnicas y herramientas más adecuadas para este fin. Además hay que tener en cuenta que la recuperación de información en la informática forense es tanto una cuestión de cantidad como de calidad. Debe recuperarse toda la información posible, pero también es necesario presentarla de forma adecuada para no saturar a los destinatarios con datos que, aunque necesarios para el armado del informe, pueden resultar excesivamente técnicos para algunos interlocutores.

Considerando estas cuestiones, PURI planteó un proceso de seis fases para guiar una investigación informático-forense, donde cada fase tiene etapas, tareas, técnicas y herramientas asociadas. Las fases planteadas por PURI son:

1. **Identificación**, donde se individualizan los equipos involucrados.
2. **Recolección**, donde se toma contacto físico y/o se trasladan físicamente los equipos a un laboratorio.
3. **Adquisición**, que consiste en la realización de imágenes – copias forenses informáticas que duplican el contenido de los medios de

3 Libro Colectivo: PODESTÁ, A., CASTELLOTE, M., CONSTANZO, B., WAIMANN, J., ITURRIAGA, J., "Dificultades de Investigaciones Penales en Cloud Computing", *Tercer CIIDDI - Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática*, 2014.

almacenamiento – y copias lógicas de los datos almacenados en el dispositivo.

4. **Preparación**, donde el experto informático detalla lo adquirido y prepara el entorno de trabajo para realizar el análisis adecuado en base a las necesidades de la investigación.

5. **Análisis**, donde se efectúa el análisis de los datos propiamente dicho, en base a lo trabajado en las fases anteriores, y se distingue la información que constituye la "evidencia digital"[4].

6. **Presentación**, donde finalmente se elabora el informe de los resultados obtenidos, detallando el proceso realizado de forma que tenga validez forense.

Las tareas que deben realizarse, y las técnicas y herramientas a utilizar, varían en cada fase de acuerdo a los dispositivos que estén involucrados, la complejidad de la situación que se debe analizar, la utilización de técnicas de protección y/o eliminación de la información o características propias del hardware involucrado, entre otros factores.

Además, es posible que en alguna de las fases se detecte la necesidad de volver a una fase anterior para profundizar el resultado que se volcará al informe. Por ejemplo, de la fase de análisis podría detectarse que había otro dispositivo involucrado y es necesario recolectarlo, adquirir sus datos y analizarlo para trabajar con el panorama completo del incidente.

En este punto se hace evidente que el proceso PURI está pensado exclusivamente desde el punto de vista técnico-informático, mientras que en una investigación penal resultará necesario actuar de acuerdo a los procedimientos legales que imponen las normas, no permitiendo tanta flexibilidad como con la que podría desenvolverse un investigador independiente. En estos aspectos, en el desarrollo del

4 Sitio Web: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Fecha de consulta 10 de Febrero de 2015)

Protocolo de Actuación (PAIF) se vio la necesidad de adaptar el proceso PURI de modo tal de poder circunscribir el margen de acción del experto informático al procedimiento penal normado por la Provincia de Buenos Aires, República Argentina, respetando de esta manera los principios y garantías que rigen una investigación judicial[5].

Las tareas especificadas en cada fase usualmente tienen técnicas, algoritmos y/o herramientas asociadas. PURI recomienda, en general, la utilización de herramientas de código libre y también herramientas comerciales, en el caso que estén establecidas en el ámbito forense o implementan una técnica especial propia. Para cuestiones donde no hay herramientas disponibles, se recomiendan los trabajos académicos que describen la técnica.

III. Estructura y puntos destacados del Protocolo

Desde hace unos años, diferentes autores y organizaciones han estado trabajando en guías de buenas prácticas en informática forense. Al analizar estas guías se detectó que si bien constituyen un excelente aporte procedimental, muchas abarcan sólo una parte del proceso, otras son muy generales, y otras focalizan únicamente en problemáticas delictivas específicas.

A la hora de diagramar la estructura del Protocolo de Actuación en Informática Forense (PAIF) se procuró en primer lugar identificar a los destinatarios, a saber: fiscales, investigadores judiciales, peritos y especialistas en informática (sin perjuicio de otros posibles lectores del documento (defensores y abogados de parte, jueces). A continuación, se procedió a elegir un formato que permitiese facilitar su lectura y utilización, sin perder la integridad y la posibilidad de actualización.

En este sentido, se dividió el documento final presentado en dos acápites principales: el Protocolo propiamente dicho y un Marco General donde se incluyen los

5 Sitio Web: http://sedi.unlp.edu.ar/handle/10915/22317 (Fecha de Consulta 10 de Febrero de 2015)

aspectos teóricos y de fundamentación de cada acción recomendada en el Protocolo, tanto a nivel técnico como a nivel legal y estratégico.

En el entendimiento que servirá de guía para los diferentes actores que intervienen en el proceso penal, se han analizado y previsto las distintas utilidades diferenciadas para los diversos destinatarios del Protocolo.

En el Protocolo (propiamente dicho) se presentan los aspectos básicos a considerar en las investigaciones vinculadas a la informática forense, formalizándose de este modo un estándar de actuación para la obtención de evidencias digitales válidas cumpliendo los principios forenses básicos (evitar la contaminación, utilizar una metodología y controlar la cadena de custodia) dando así garantía a lo obrado en el marco del proceso judicial, pudiendo ser adoptado y promovido entre profesionales de la informática forense y organismos judiciales.

De esta forma, teniendo en cuenta las distintas etapas por las que atraviesa una investigación penal, se diseñó un esquema comprensivo tanto de la etapa de pesquisa como de la forense. La estructura propuesta quedó conformada de la siguiente manera:

- Breve introducción
- Plan de Investigación Penal. Fase de Identificación
    - Competencia y Jurisdicción aplicables. Identificación de objetos y equipos intervinientes
    - Medios de Identificación
    - Pedido de allanamiento y control del contenido de la orden de allanamiento
- Plan de Investigación Penal. Fase de Recolección
- Plan de Investigación Penal. Cadena de custodia

    - Procedimientos del sistema de Cadena de Custodia
    - El Registro de Cadena de Custodia
- Plan de Investigación Penal. Puntos periciales
- Tareas periciales. Fase de adquisición
- Tareas periciales. Fase de preparación
- Tareas periciales. Fase de análisis
- Tareas periciales. Elaboración del dictamen pericial
- Presentación del Perito en el Juicio Oral
- Decomiso de las evidencias.

Por otra parte, se elaboró un documento denominado "Marco General" donde se podrá encontrar una descripción amplia y abarcativa de los conceptos de Informática Forense y Evidencia Digital, la correlación de éstos dentro del proceso penal, las consideraciones sobre un plan de investigación penal y los roles de los expertos informáticos dentro de éste[6]. También se realizaron descripciones sobre el manejo y las fuentes de evidencia digital. Asimismo se brindaron fundamentaciones teóricas relativas al Plan de Investigación Penal (la identificación de la evidencia, la etapa de recolección, el proceso de cadena de custodia, el manejo en la escena del crimen o en un allanamiento), la fijación de puntos periciales, las tareas periciales, la elaboración del dictamen pericial, la presentación del perito en un juicio oral y finalmente se realizaron propuestas para el decomiso de las evidencias.

Complementario a estos dos acápites principales, se confeccionó una serie de ***Hojas de Datos,*** es decir, de documentos anexos que describen características técnicas para la toma de decisiones en etapas precisas. En este sentido, se elaboraron tres hojas

6 Revista: MARAFIOTI, L. Prueba digital y proceso penal. Revista de Derecho Penal y Procesal Penal Buenos Aires, año 4, núm 75, 2012, pp 1904-1911

de datos haciendo hincapié en: Evidencias en Medios Tecnológicos, Recomendaciones para actuaciones en Escenas del Crimen y Allanamientos y en las Técnicas y Herramientas de Informática Forense (etapas y fases de PURI).

Asimismo se realizaron propuestas de **Formularios y Modelos** para la actuación judicial, a saber: Actas de Levantamiento de Soporte de Evidencia Digital (LSED), Acta de Levantamiento de Evidencia Digital (LED) y Planilla de Cadena de Custodia[7].

Finalmente, se elaboró un Glosario técnico-jurídico y se mencionaron las fuentes bibliográficas y normativas consultadas.

El texto del documento se encuentra actualmente en etapa de revisión jurídica.

Iς. Experiencias en la elaboración del Protocolo de Actuación en Informática Forense. Reflexiones y conclusiones.

Una característica sobresaliente de este proyecto, es que utiliza conocimientos científicos y tecnológicos pertenecientes tanto a la disciplina de la informática, como a la disciplina del derecho y a la criminalística. La interdisciplinariedad del trabajo es lo que asegura la riqueza de los resultados obtenidos.

El PURI se nutrió de procesos y guías de buenas prácticas en informática forense nacionales e internacionales, que fueron adoptadas e integradas en un esquema de fases, etapas, tareas, técnicas y herramientas recomendadas a nivel científico.

Sin embargo, es dable recordar que dichas guías existentes en otros países resultan inaplicables en nuestra normativa, siendo por tanto necesario elaborar una propia acorde a los principios y garantías previstas por nuestra Constitución Nacional Argentina y por las leyes de fondo y procesales, las cuales delimitan el accionar estatal en el ámbito del proceso penal.

De esta forma, se elabora el Protocolo de Actuación en Informática Forense

7 Sitio Web: http://www.senadoba.gov.ar/seclegbusquedaacyprodetalle.aspx?expe=93252 (Fecha de Consulta 13 de Febrero de 2015)

desde las miradas de la disciplina legal y con el aporte de nuevos conocimientos sobre métodos, técnicas y herramientas generadas por el grupo de investigación, destinadas plenamente a dar solución a un vacío técnico-legal existente en la normativa de la Provincia de Buenos Aires.

En su redacción, se trabajó intensamente en integrar fuentes, disciplinas y lenguajes diversos, lo cual presentaba ciertas complejidades a la hora de estudiar el tema; sin embargo, esto permitió lograr un enriquecimiento en la elaboración del Protocolo.

La garantía del éxito del proyecto está dada por la concurrencia multidisciplinaria en el trabajo, tanto por la participación de los investigadores académicos como de los integrantes de los estamentos judiciales, dando una respuesta integral al problema abordado.

En síntesis, este proyecto significa la transferencia a la sociedad de conocimiento científico–tecnológico genuino desarrollado en un ámbito académico para lograr un mejor actuar en el proceso judicial y, en definitiva, mejorar la justicia. Esto significa, dar respuesta a una necesidad social que, al momento, no se encontraba resuelta.