Análisis del Marco Normativo Legal para el Ciclo de Vida de la Evidencia Digital

Mg. Aldo Santiago Igarza; Esp. Cintia Verónica Gioia; Mg. Jorge Eterovic;

Programa CyTMA2 / Departamento de Ingeniería e Investigaciones Tecnológicas
Universidad Nacional de La Matanza
Florencio Varela 1903 (B1754JEC), San Justo, (5411) 4480-8900

asigarza@unlam.edu.ar; cgioia@unlam.edu.ar; eterovic@unlam.edu.ar

1. Resumen.

Con el crecimiento de las conductas delictivas que llegan a la justicia y que involucran dispositivos informáticos, surge la necesidad de acudir cada vez más a expertos en informática forense que actúen como peritos informáticos de oficio o de parte, siendo crucial su actuación en materia probatoria.

La exigente labor que hoy en día se requiere de especialistas en informática forense obliga a los mismos a mantener un conocimiento detallado y actualizado tanto a nivel de metodologías de prácticas forenses y procesos vinculados como en las normas y legislaciones asociadas con el tratamiento de la evidencia digital.

Disponer de un análisis comparativo exhaustivo de las diferentes normas y procesos del Ciclo de Vida de la evidencia digital dentro del marco normativo, jurídico y legal, son la base fundamental para el trabajo de un investigador forense informático o perito informático.

El proyecto de investigación se enfoca en el análisis de metodologías y procesos forenses informáticos y en el marco jurídico legal vigente para el aseguramiento del tratamiento de la evidencia digital en sus diferentes etapas del Ciclo de Vida, desde la identificación, adquisición o recolección, preservación, análisis hasta la presentación de resultados técnicos a tribunales de la justicia.

Como resultado de esta investigación se espera poder hacer un aporte sobre cómo abordar un peritaje informático a partir de diferentes escenarios según el tipo de pericias a realizar, los tipos de delitos informáticos involucrados y la aplicación de la normativa legal vigente.

Palabras Clave:

Informática Forense, Evidencia Digital, Procesos Forense, Marco Normativo Legal.

2. Contexto.

Este proyecto de investigación está siendo presentado como un Programa de Investigación Científica, Desarrollo y Transferencia de Tecnologías e Innovaciones (CyTMA2) en el Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza.

El presente proyecto es del tipo investigación básica basado en el análisis del marco normativo y jurídico de la República Argentina, orientado a la comparación de los procesos del Ciclo de Vida de la Evidencia Digital.

3. Introducción.

La informática forense hace su aparición como una disciplina auxiliar de la justicia, para enfrentar los desafíos y técnicas de los intrusos informáticos, como también de garante de la verdad alrededor de la evidencia digital que se pudiera aportar en un proceso que involucra un delito informático [1].

De acuerdo con Dupuy y Kiefer [2], la evidencia digital es: "Cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". La evidencia digital es un término utilizado para describir cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal [1].

La evidencia informática está comprendida por aquellos datos o información que se almacena, transmite o recibe en un dispositivo informático y que tiene valor probatorio en el marco de una causa judicial. La evidencia digital es intangible, inmaterial, volátil, frágil, anónima, duplicable, editable, ocultable y eliminable [3].

La informática forense es una disciplina científica técnica-legal que involucra el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable en una causa judicial [4].

La identificación de la evidencia digital implica identificar las fuentes potenciales de la evidencia digital, los elementos a secuestrar y documentar todo lo necesario para la identificación de esta.

La preservación de la evidencia digital consiste en extremar los recaudos a fin de evitar la contaminación de la prueba [5]. En esta etapa del proceso es muy importante mantener la cadena de custodia registrando todas las operaciones realizadas sobre la evidencia digital y resguardando de forma segura los elementos secuestrados utilizando etiquetas de seguridad.

Los elementos de prueba originales deben ser conservados hasta la finalización del proceso judicial, preservándolos de las altas temperaturas, campos magnéticos y golpes. La creación de una imagen forense es indispensable y en el caso que no sea posible, el acceso a los dispositivos originales se realiza mediante mecanismos de protección contra escritura. Es importante implementar mecanismos de autenticación de la evidencia digital de manera de garantizar que la misma no fue alterada.

El análisis de la evidencia digital tiene como objetivo buscar y obtener evidencia digital relevante para la investigación (a partir de puntos de pericias solicitados), mediante la aplicación de diversas técnicas y herramientas forenses. Es importante registrar la evidencia digital relevante.

La presentación de la evidencia digital consiste en la elaboración del dictamen pericial con los resultados obtenidos en las etapas previas. El dictamen debe ser claro, objetivo y preciso, conteniendo la descripción de las tareas y elementos utilizados para repetir el proceso en caso de ser necesario [6].

Los resultados de un análisis científico de la evidencia digital deben poder ser repetibles, mesurables e irrefutables.

La cadena de custodia involucra la custodia de todos los elementos del caso e incluye documentar cada uno de los eventos que se han realizado con la evidencia indicando por cada uno quién, cuándo, donde, en qué estado, quién tuvo acceso y adicionando toda información

que caracterice a como se llevó a cabo la custodia [7].

Los procesos relacionados con el manejo de la evidencia digital, asociados a la identificación, recolección, adquisición y preservación de datos, establecen principalmente cuáles son los requisitos para el manejo de la evidencia digital, los procedimientos a considerar para asegurar la cadena de custodia, los roles y responsabilidades del perito informático en cada etapa, la documentación a realizar y los componentes esenciales del Ciclo de Vida de la evidencia digital [8], [9].

4. Líneas de Investigación, Desarrollo e Innovación.

La informática forense es inter-disciplinaria y requiere un estudio detallado de las normas, leyes, procesos, técnicas y tecnologías, además de los diferentes roles y responsabilidades de las personas involucradas, conformando un conjunto de conocimiento formal, científico y legal que apoya directamente a la administración de la justicia para al esclarecimiento de los hechos como así también en investigaciones internas en las organizaciones.

Si bien las herramientas forenses son la base esencial del análisis de la evidencia digital en medios informáticos, las mismas no hacen por sí solas a la tarea del perito informático. Por tal motivo el proyecto no se centra en la investigación de las herramientas forenses en sí, sino en la investigación de metodologías, técnicas, prácticas y procedimientos forenses y en el marco jurídico legal vigente para el aseguramiento del tratamiento válido de la evidencia digital en sus diferentes etapas del Ciclo de Vida.

También se estudiarán las diferentes regulaciones y lineamientos generales a considerar para la implementación de un laboratorio de informática forense, de manera de basar la misma en un entorno regulado y basado en normativas de trabajo para la investigación forense.

5. Resultados y Objetivos.

El objetivo de este proyecto de investigación es abordar un análisis comparativo exhaustivo de las diferentes metodologías, procesos, procedimientos, normas, y prácticas relacionadas con la informática forense, dentro de un marco jurídico y legal como base para el trabajo del investigador forense informático o perito informático.

Se definirán los procesos relacionados con el manejo de la evidencia digital, asociados a la identificación, recolección, adquisición y preservación de datos, estableciendo principalmente cuáles son los requisitos para el manejo de la evidencia digital, los procedimientos a considerar para asegurar la cadena de custodia, los roles y responsabilidades del perito informático en cada etapa, la documentación a realizar y los componentes esenciales del Ciclo de Vida de la evidencia digital, dentro del marco normativo, jurídico y legal de nuestro país.

6. Formación de Recursos Humanos.

El equipo está integrado por docentes-investigadores que pertenecen distintas cátedras de la carrera de Ingeniería en Informática de la UNLaM, más otro docente-investigador abogado, especializado en temas jurídico-informáticos y un alumno de la carrera de Ingeniería en Informática que está haciendo sus primeras experiencias en investigación.

Dos de los miembros del equipo de investigación se encuentran desarrollando sus respectivos trabajos de tesis de posgrado de la Maestría en Informática de la UNLaM y en la Maestría en Teleinformática y Redes de Computadoras de la Universidad de Morón. Ambos están siendo tutoreados por el Mag. Jorge Eterovic, integrante del proyecto de investigación.

7. Referencias

[1] Cano, Jeimy J. Computación Forense. Descubriendo los Rastros Informáticos. 2da edición. Editorial Alfaomega. Bogotá, Buenos Aires, México. 2016. ISBN: 978-958-682-922-9.

[2] Dupuy, D., Kiefer, M. "Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet". Editorial B de F. Buenos Aires - Montevideo. 2017. ISBN: 978-9974-745-06-3.

[3] Darahuge, M. E., Arellano González, L. "Manual de Informática Forense (Prueba Indiciaria Informático Forense)". Editorial Errepar. Buenos Aires. 2011. ISBN: 978-987-01-1249-5.

[4] Darahuge, M. E., Arellano González, L. "Manual de Informática Forense III (Prueba Indiciaria Informático Forense)". Editorial Errepar. Buenos Aires. 2016. ISBN: 978-987-01-1953-1.

[5] Sain, G., Azzolin, H. "Delitos Informáticos. Investigación criminal marco legal y peritaje". Editorial B de F. Buenos Aires - Montevideo. 2017. ISBN: 978-9974-745-27-8.

[6] Aboso, G. E., Zapata, M. F. "Cibercriminalidad y Derecho Penal". Editorial B de F. Buenos Aires - Montevideo. 2006. ISBN: 9974-578-74-4.

[7] Marqués Arpa, T., Serra Ruiz, J. "Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital". RECSI 2014, Alicante. España. Sitio web: http://web.ua.es/en/recsi2014/documentos/papers/cadena-de-custodia-en-el-analisis-forense-implementacion-de-un-marco-de-gestion-de-la-evidencia-digital.pdf (visitado en marzo de 2018).

[8] Domínguez, F.L. "Introducción a la Informática Forense". Editorial RAMA. Buenos Aires. 2015. ISBN: 978-8499-642-09-3.

[9] Di Iorio, A. "La necesidad de adopción de un Proceso Unificado de Recuperación de Información: "PURI – Una propuesta". Congreso Argentino de Ingeniería Forense 2014. Copitec. Argentina. 2014. Sitio Web: http://www.copitec.org.ar/comunicados/CAIF2014/calidadserviciopericial.pdf (visitado en marzo de 2018).