Diseño y Desarrollo de un Prototipo de Aplicación para la Gestión de las Pericias en Informática Forense Adaptada al Sistema Jurídico Argentino (GEPIF)

Luis Enrique Arellano González, María Elena Darahuge, Carlos Orozco y Agustín Solimine
Sistemas / Informática / Universidad Argentina John F Kennedy
Dirección: Bartolomé Mitre 1411 - 1º Piso. C.P. 1037
Ciudad Autónoma de Buenos Aires
Teléfono: 05411-5236-1224
e-mails: arellano@kennedy.edu.ar, darahuge@kennedy.edu.ar, corozco@alumnos.kennedy.edu.ar, asolimine@alumnos.kennedy.edu.ar

Resumen

El diseño y desarrollo de un prototipo de aplicación para la gestión de pericias de informática forense adaptado al sistema jurídico argentino, es una inminente necesidad para los peritos informáticos que desempeñan diferentes roles como auxiliares de la justicia (perito oficial, de oficio, de parte, consultores técnicos). El proyecto se centra en la confección de una herramienta que permita guiar a los peritos en informática forense en cada una de las etapas de la elaboración del informe pericial, de manera tal que su aplicación pueda ser realizada de forma homogénea y con un procedimiento básico que luego podrá ser readaptado y retroalimentado acorde a las diversas situaciones que surjan en la gestión de la pericia en informática forense. Se utilizará como marco de referencia y modelo principal la estructura internacionalmente reconocida a mediados del siglo pasado e implementada por el Departamento Scopométrico de la Policía Federal Argentina, ya que permite la normalización, búsqueda, sistematización e intercambio de resultados periciales entre informes procedentes de diferentes áreas del saber, facilitando el apoyo a la decisión judicial obligatoria (sentencia). Asimismo, permite intercambiar datos de manera eficiente, efectiva y eficaz, entre los distintos órganos de investigación judicial, dependientes del poder judicial nacional e internacional.

Palabras clave: informática forense, perito, gestión pericias informático-forenses.

Contexto

El proyecto se encuentra inserto dentro de la investigación y desarrollo de los Proyectos Plurianuales de Investigación (PPI), el cual fue aprobado en octubre de 2015, es financiado por la Universidad Argentina John F Kennedy, su duración es de tres años y con una finalización estimada para el año 2018 y se relaciona con el proyecto Confiabilidad (trazabilidad y responsabilidad) de la cadena de custodia en Informática Forense (CCCIF). El Instituto Argentino de Normalización y Certificación – IRAM- a través del Subcomité Seguridad en Tecnología de la Información colabora con la información relacionada con las normas ISO de informática forense.

1. Introducción

La gestión pericial implica la realización de una serie de etapas que debe efectuar el perito en informática forense en cualquiera de los roles en que se desempeñe, de manera tal que su accionar se encuentre contenido en un entorno sistémico y jurídico que permita efectuar la reconstrucción de las tareas realizadas por parte de cualquier otro perito en informática forense. La estructura del informe pericial que se propone, con sus diferentes etapas, ha sido creada en 1940 por los organismos de seguridad y aplicadas

específicamente al área de las disciplinas criminalísticas [1], [14]. [24]. La informática forense es una disciplina criminalísitca, por lo tanto requiere la implementación de la estructura del informe pericial adaptado a dicha disciplina. El informe pericial está constituído por los siguientes elementos [7], [8] y [13]: Introducción, Objeto, Elementos ofrecidos, Elementos dubitados, Operaciones realizadas, Conclusiones, Recomendaciones, Anexos. En la actualidad no existe en el país ningún sistema que muestre la cronología y la sucesión de las etapas de un informe pericial de informática forense y que además refleje el entorno jurídico nacional.

Estado actual del conocimiento:

Actualmente los informes periciales de informática forense no se realizan de manera homogénea, ni estructurada, es decir, cada perito, consultor o asesor técnico, confecciona el informe pericial sin tener en cuenta una base sistémica y criminalística [4], [5], [6], [9]. [11] y [12]. La bibliografía actual de referencia respecto de la realización de los informes periciales de informática forense en relación al sistema jurídico argentino, se encuentra descripta a nivel de detalle en los Manuales de Informática Forense I y II [7] y [8]. Las aplicaciones desarrolladas por diferentes países del hemisferio norte (Encase: https://www.guidancesoftware.com/) o por los europeos (Deft Association: http://www.deftlinux.net/, Digital Forensics Framework, DFF http://www.digital-forensic.org/) se limitan solamente a la implementación de herramientas informáticas individuales o conformando un paquete de aplicaciones que únicamente resuelven necesidades de carácter operativo, es decir, que solo se corresponden con el área de operaciones realizadas del informe pericial en informática forense. Las normas internacionales [15], [16], [17], [18], como el RFC [2], relacionados con la informática forense, hacen referencia al sistema jurídico del derecho anglosajon (*common law*) [3], [22] y [23], el cual dista notablemente del sistema jurídico argentino, que no se basa en la jurisprudencia, sino en la codificación de leyes [26].

Situación problemática: Al efectuar un informe pericial informático forense se deben realizar un conjunto de etapas sistémicas y cronológicas que permitan la reconstrucción de la información por parte de cualquier profesional que así lo requiera. La importancia de registrar las acciones, tareas y documentación de la información en cada etapa es fundamental. Las etapas de la gestión pericial en informática forense son las siguientes:

1. Identificación y registro
2. Autenticación, Duplicación y Resguardo de la prueba
3. Detección, recolección y registro de indicios probatorios
4. Análisis e interpretación de los indicios probatorios. Reconstrucción y / o simulación del incidente
5. Cotejo, correlación y conclusiones, generación de la cadena de custodia e informe pericial informático forense.

Cada una de estas etapas se relaciona con el sistema jurídico argentino y sus códigos de fondo y forma [19] y [21].

La pregunta fundamental se circunscribe a determinar: ¿Cuál es el modelo de informe pericial más adecuado que permita una descripción exhaustiva de las tareas realizadas sobre la prueba indiciaria de informática forense y brinde al mismo tiempo un formulario digital computable que facilite el intercambio de información y resultados desde las diferentes áreas del conocimiento en apoyo a la decisión judicial obligatoria (sentencia)?

Hipótesis: El diseño y desarrollo de un modelo digital de gestión de pericias en informática forense permitirá la homogeneización de la elaboración de los informes periciales de informática forense en el ámbito de la justicia de la República Argentina.

Variable Dependiente: Relación entre el nivel de aplicación de un modelo digitalizado de gestión pericial de informática forense con otras disciplinas criminalísticas. [1], [14], [20] y [24].

Variables Independientes:

2. Relación entre el modelo de gestión pericial propuesto y el entorno judicial involucrado.
3. Grado de integración de la pericia en informática forense con el resto de las disciplinas criminalísticas.

4. Líneas de Investigación, Desarrollo e Innovación

Las principales disciplinas en las que se inscribe el presente anteproyecto son: la criminalística, la informática forense y el derecho. A partir de la criminalística se circunscribe la metodología y los procedimientos del tratamiento de las pruebas o evidencias propias de la informática forense. En relación a la informática forense se consideran las técnicas y métodos específicos requeridos por ésta disciplina al iniciar el proceso de identificación y registro de la prueba y las sucesivas etapas hasta su disposición final. El derecho interviene estableciendo las pautas procesales necesarias para dar validez a los indicios o prueba informático forense desde su etapa inicial de recolección hasta el destino final establecido por el Juez.

El desarrollo de la aplicación **GEPIF** no tiene un precedente en el ámbito nacional. Considerando los altos costos de las aplicaciones de código cerrado comerciales extranjeras existentes en el mercado de la informática forense, tanto a nivel de licencias como en la capacitación, **GEPIF** se realizará utilizando código abierto [10], [26] y licencia GPL, para posteriormente ser difundido en el ámbito nacional. Actualmente el paquete de aplicaciones de desarrollo internacional de código abierto de gestión de pericias como *Autopsy* (http://www.sleuthkit.org/autopsy/features.php) , ofrece un entorno de desarrollo modular, tanto para java como para python (http://www.sleuthkit.org/sleuthkit/framework.php). En el proyecto se revisarán los módulos existentes de *Autopsy* como punto de referencia para luego adaptarlos / modificarlos o generar nuevos acorde a las necesidades de los peritos en informática forense, en el marco de la criminalística y del sistema jurídico argentino.

5. Resultados Obtenidos / Esperados

El propósito del presente proyecto se focaliza en: ***Determinar*** los elementos requeridos para el diseño y desarrollo de un prototipo de aplicación de gestión de pericias de informática forense adecuados al sistema jurídico argentino que permita homogeneizar la elaboración de los informes periciales de informática forense en el ámbito de la República Argentina (en soporte de papel y digital).

Objetivo general: ***Diseñar y desarrollar*** un prototipo de aplicación para la gestión de las pericias de informática forense adaptado al sistema jurídico argentino.

En relación a los resultados esperados, el diseño de un prototipo de gestión de pericias en informática forense tiene como fin la homogeneización de la labor de los peritos en de informática forense. La aplicación podrá difundirse en el ámbito de la función pública (organismos e instituciones del poder judicial y de las fuerzas de seguridad), como así también en el ámbito académico privado y público de todo el territorio de la nación argentina. El proyecto será presentado en diversos congresos, seminarios y jornadas del área de la criminalística y de la informática forense en diferentes ciudades del país y en las conferencias internacionales de informática forense en la modalidad presencial y virtual. El impacto del proyecto radica principalmente en que en la actualidad no existe una aplicación de gestión de pericias informático forense adaptada al sistema jurídico argentino que

normalice para todo el país la labor de los expertos y/o peritos en informática forense en la gestión de la prueba indiciaria de informática forense, por consiguiente, es una necesidad inminente la formalización e implementación de un modelo común para los peritos en informática forense como auxiliares de la justicia. Al mismo tiempo deja abierta la posibilidad de futuras investigaciones, para comprobar el funcionamiento del modelo propuesto como referente de intercambio de datos entre las distintas disciplinas criminalísticas. A partir del año 2017 se ha concretado la incorporación del equipo de investigación al Subcomité de Seguridad en Tecnología de la Información del Instituto Argentino de Normalización y Certificación – IRAM-. El proyecto GEPIF permitirá generar una infraestructura de procedimientos de gestión de la pericia informático forense que conformarán el inicio de una propuesta de normalización para ser evaluada oportunamente por el IRAM:

6. Formación de Recursos Humanos

El equipo está conformado por un docente de la licenciatura en sistemas de la UAJFK y Director del Curso de Experto en Informática Forense de la UTN – FRA, Especialista en criptografía y seguridad teleinformática, Ingeniero en Sistemas, Abogado, Licenciado en Criminalística y Experto en Informática Forense, actualmente escribiendo la tesis doctoral en filosofía del derecho en la UBA. Una docente Ingeniera en informática, Especialista en Criptografía y Seguridad teleinformática, Magister en dirección estratégica en tecnologías de la información y Experta en Informática Forense, actualmente escribiendo la tesis del doctorado en Psicología Social de la UAJFK. Un abogado que además presentó y aprobó en 2016 el trabajo final de grado de la Licenciatura en Sistemas sobre informática forense y derecho continuando en el equipo de investigación como graduado. Dos alumnos cursantes del cuarto año de la Licenciatura en sistemas de la UAJFK interesados en el tema de investigación en relación con la seguridad de la información.

7. Bibliografia

1. Albarracín, Roberto. (1969). Manual de Criminalística. Buenos Aires: Editorial Policial.
2. Brezinski, D. Killalea, T. (2002). Request for Comments: 3227 - Category: Best Current Practice. Guidelines for Evidence Collection and Archiving.
3. Broen, Christopher. Computer Evidence Collection & Preservation. (2006). Massachussets, USA: Charles River Media.
4. Darahuge, María Elena; Arellano González, Luis Enrique (2005). “Metodología de la Inspección Ocular en la Informática Forense”, Investigación publicada en el Congreso Virtual Latinoamericano de Psicología Jurídica”.
5. Darahuge, María Elena; Arellano González, Luis Enrique. “La prueba documental informática” (recaudos procesales). Compendio Jurídico ERREIUS-ERREPAR, Septiembre 2010, Nº 44.
6. Darahuge, María Elena; Arellano González, Luis Enrique. “La recolección ilegítima de datos (el problema del phishing)”. Compendio Jurídico ERREIUS-ERREPAR, Agosto 2011, Nº 54.
7. Darahuge, María Elena; Arellano González, Luis Enrique. (2011). Manual de Informática Forense. Buenos Aires: Errepar.
8. Darahuge, María Elena; Arellano González, Luis Enrique. (2012). Manual de Informática Forense II. Buenos Aires: Errepar.
9. Darahuge, María Elena; Arellano González, Luis Enrique “Prueba documental informática, errores inauditos”. Compendio Jurídico ERREIUS-ERREPAR, Septiembre 2013, Nº 77.
10. Darahuge, María Elena; Arellano González, Luis Enrique “Aplicaciones de código abierto en informática forense”. Revista

Profesional&empresaria, D&G ERREIUS-ERREPAR, Enero 2014, Nº 172, Tomo XV.
11. Darahuge, María Elena; Arellano González, Luis Enrique Artículo: "La intervención notarial en la recolección de la prueba informático forense". Revista Profesional&empresaria, D&G ERREIUS-ERREPAR, Febrero 2014, Nº 173, Tomo XV.
12. Darahuge, María Elena; Arellano González, Luis Enrique "La prueba documental informática (recaudos procesales)". Revista Profesional&empresaria, D&G ERREIUS-ERREPAR, Abril 2014, Nº 175, Tomo XIV.
13. Darahuge, María Elena; Arellano González, Luis Enrique "La estructura formal del Informe Pericial". Revista Profesional&empresaria, D&G ERREIUS-ERREPAR, Diciembre 2014, Nº 183, Tomo XV.
14. Guzmán, Carlos. (2000). Manual de Criminalística. Buenos Aires: Ediciones La Rocca.
15. ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.
16. ISO/IEC 27041 — Information technology — Security techniques —. Guidelines on assuring suitability and adequacy of incident investigative methods (FDIS).
17. ISO/IEC 27042 — Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence
18. ISO/IEC 27043 — Information technology — Security techniques — Incident investigation principles and processes (FINAL DRAFT). ISO/IEC 27050 — Information technology — Security techniques —. Electronic discovery
19. Medina, Graciela; Maíz, Mónica Gabriela. (2008). Derecho procesal civil para peritos. 2da ed, actualizada. Buenos Aires: Rubinzal-Culzoni Editores.
20. Rosset, Ricardo; Lago, Pedro. (1962). El abc del dactilóscopo. Buenos Aires: Biblioteca policial.
21. Torres, Sergio Gabriel. (2014). Nulidades en el proceso penal. 6ta.,ed. Buenos Aires: Editorial Ad-hoc.
22. Smith, Fred Chris; Gurley Bace, Rebecca. (2003). A guide to Forensic Testimony. The art and practice of presenting testimony as an expert technical witness Boston
23. Vacca, John. (2002). Computer Forensic: Computer Crime Scene Investigation. USA: Ed, Charles River Media, Networking Series.
24. Zajaczkowski, Raúl Enrique. (2012). Manual de criminalística. Buenos Aires: Ediciones Dosyuna.
25. Códigos de fondo y forma y leyes relacionadas de la República Argentina
26. Grupo de Informática Forense: https://espanol.groups.yahoo.com/neo/groups/informatica-forense/