Repositorio Institucional para la Gestión de Evidencias Móviles

Analía Méndez[1], Cecilia Lara[1-2], Liliana Figueroa[1], Graciela Viaña[1], Norma Lesca[3]

[1] Instituto de Investigación en Informática y Sistemas de Información, Facultad de Ciencias Exactas y Tecnologías, Universidad Nacional de Santiago del Estero
amendez@unse.edu.ar; clara@unse.edu.ar;
lmvfigueroa@yahoo.com.ar; gv857@hotmail.com

[2] Oficina de Informática Forense del Gabinete de Ciencias Forenses del Ministerio Público Fiscal de Santiago del Estero
clara@unse.edu.ar

[3] Poder Judicial de la Nación – Juzgado Federal Nro. 2 - Santiago del Estero

norma.lesca@gmail.com

Resumen. Los dispositivos móviles se caracterizan por poseer información digital almacenada de naturaleza dinámica, propensa a cambios y modificaciones indeseadas o no autorizadas. Para efectuar la labor forense sobre este tipo de materiales tecnológicos se han desarrollado guías de procedimiento y normas internacionales para la identificación, recolección, adquisición y preservación de evidencia digital. En tal sentido, desde el 2017 se está trabajando en los proyectos de investigación "Computación Móvil: desarrollo de aplicaciones y análisis forense" y "Métodos y herramientas para el análisis forense de dispositivos móviles", financiados por el Consejo de Ciencia y Técnica de la Universidad Nacional de Santiago del Estero, para tratar esta temática, y se elaboró un Protocolo de Actuación para la obtención de evidencias digitales de dispositivos móviles en el ámbito judicial que permita orientar el cumplimiento de buenas prácticas y garantizar la calidad de los procesos aplicados y de los resultados obtenidos, tomando como referencia a la familia de normas ISO/IEC 27000. Dicho protocolo pretende apoyar la condición de admisibilidad que la prueba digital debe cumplir para constituirse en eficaz para la investigación judicial.

Este artículo es el resultado de la investigación inicial que plantea una estrategia de almacenamiento basada en repositorios institucionales digitales, para la gestión de evidencias digitales extraídas de dispositivos móviles a fin de constituir un instrumento que respetando las pautas establecidas por el protocolo de actuación permita la preservación de las evidencias digitales.

Palabras claves: evidencia digital, dispositivos móviles, repositorio institucional.

1 Introducción

Este trabajo está enmarcado dentro del cumplimiento del objetivo "Analizar alternativas de construcción de repositorio digital para la gestión de evidencias digitales extraídas de dispositivos móviles", definido en el proyecto de investigación denominado "Métodos y herramientas para el análisis forense de dispositivos móviles" [1].

Los Smartphone, dispositivos móviles inteligentes, además de las funciones básicas de los teléfonos convencionales, cuentan con la operatividad y capacidad de computadoras portátiles ya que disponen de procesadores de texto, planillas de cálculo, acceso a Internet, cámaras fotográficas sofisticadas, conexión en la nube con ayuda de ciertas aplicaciones, localizadores geo referenciales, videoconferencia, así como otras diversas aplicaciones soportadas por sus sistemas operativos (Android, IOS, Windows, etc.), constituyéndose de este modo en una profusa fuente de información y de herramienta de trabajo en un contexto de recolección de evidencias forenses [2].

Estos dispositivos han dejado de ser un lujo para convertirse en una necesidad; la brecha y funcionalidad entre los dispositivos se ha vuelto cada vez más delgada, siendo actualmente una distinción únicamente el tamaño, si hablamos por ejemplo de las Tablet y los Smartphone.

Cuando un dispositivo móvil está involucrado en un delito o en un incidente, se debe analizar y tomar en cuenta que el dispositivo contiene información personal, laboral, e incluso puede reflejar costumbres o hábitos de la persona, convirtiéndose así en fuente de información muy sensible para ser tomada para una investigación.

Para realizar una investigación, los peritos forenses requieren seguir procedimientos adecuados, una cadena de custodia bien definida, normas de preservación de evidencia físicas (por ejemplo, huellas dactilares en el dispositivo), así como también utilizar herramientas y tecnologías que permitan obtener una apropiada y rápida recuperación de la información almacenada en el dispositivo. La información obtenida será analizada, y servirá para redactar un informe detallado de las actividades efectuadas, con la finalidad de buscar evidencias que revelen la causa y forma en la que se llevó a cabo un posible delito; en algunos casos ésta información puede obtenerse incluso luego de haber sido borrada del dispositivo móvil.

En este contexto, el protocolo de actuación propuesto en el marco del proyecto "Computación Móvil: desarrollo de aplicaciones y análisis forense", contempla aspectos fundamentales de lo que constituye una buena práctica pericial forense aplicada sobre dispositivos móviles y pretende apoyar la condición de admisibilidad que la prueba digital debe cumplir para constituirse en eficaz para la investigación judicial [3]. Sus lineamientos procuran ofrecer suficiente respaldo jurídico para la labor de los peritos informáticos en la investigación penal, además de servir como una herramienta para la planificación y control de dicho proceso en la Investigación Penal Preparatoria (IPP) [1].

Igualmente, se requiere contar con un marco para el diseño de un repositorio de evidencia digital extraída de dispositivos móviles durante la IPP, considerando la integridad de sus datos, la conservación a largo plazo y el acceso seguro al material almacenado.

La preservación digital es uno de los aspectos a tener en cuenta a partir de la despapelización de los procesos judiciales en la modernización de la gestión. En este contexto, el objetivo es garantizar que las evidencias digitales se conserven también de forma íntegra y puedan ser accesibles e interpretables a lo largo del tiempo.
En este artículo, que es el resultado del estudio inicial sobre repositorios institucionales, se propone comenzar el análisis de las pautas esenciales que debería cumplir dicho repositorio de evidencias digitales de modo que se permita su almacenamiento, recuperación, distribución y acceso de manera segura por parte de los involucrados en el proceso de investigación judicial, en cumplimiento con estándares internacionales.
El desarrollo del contenido de este artículo se organiza de la siguiente manera: en la sección dos se aborda una revisión del concepto de evidencia digital forense y consideraciones legales de las evidencias digitales, en la sección tres se indaga sobre repositorios digital forense institucional, proponiendo los aspectos a tener en cuenta en el proceso de creación y desarrollo de un repositorio digital para la gestión de evidencias digitales móviles según lo establecido en estándares internacionales como la Norma ISO 16363, en la sección cuatro se plantean conclusiones y anhelos futuros.

2 Conceptualización de evidencia digital forense

Los dispositivos móviles han transformado la dinámica de nuestras interrelaciones sociales, constituyen en la actualidad una necesidad personal y social que facilita la comunicación y el manejo de la información a nivel mundial. Las diferenciaciones y funcionalidades de los diversos modelos de dispositivos se han ido reduciendo, equiparándose en algunos casos a potentes computadoras de bolsillo [4].
Paralelamente al desarrollo tecnológico de los dispositivos móviles, la capacidad de procesamiento de información y las formas de intercambio de datos avanzaron influyendo en nuevos tipos de evidencias forenses.
A la información de relevancia para un proceso de investigación judicial, que se almacena en formato digital y puede ser procesada o transmitida por medio de diferentes sistemas o dispositivos informáticos, se la denomina evidencia digital [5]. Normalmente es recogida o captada por un perito informático mediante la aplicación de técnicas especializadas a fin de constituirse en una prueba válida en un proceso de investigación forense [6].
Así mismo, en Guidelines for the Management of IT Evidence, se define a la evidencia digital como cualquier información digital extraída de un medio informático que se encuentra expuesta o propensa a la intervención humana o tecnológica [7] [8].
Evidencia digital, evidencia electrónica o registro electrónico son términos que se utilizan de manera amplia para describir cualquier registro generado por, o almacenado en, un sistema computacional y que puede ser utilizado como evidencia en un proceso legal [9].
Particularmente, la recolección de evidencia digital forense se complejiza constantemente debido a la evolución incansable de los dispositivos móviles que, a su vez, genera mayor cantidad de información para ser analizada [6].

2.1 Aspectos legales de las evidencias digitales móviles

Se sabe que el Proceso Penal está regulado por los Códigos Procesales que dictan las provincias, en particular se destacan algunas referencias que están vinculadas con las evidencias digitales móviles:

- Las telecomunicaciones están protegidas, por la garantía del artículo 18 de la Constitución Nacional en cuanto dispone la inviolabilidad de la correspondencia y de los papeles privados. El Código Procesal Penal Federal [10] en su artículo 236 hace referencia específica a la Intervención de las comunicaciones telefónicas. A su vez el actual Código Procesal Penal Federal [11] en los artículos 150, 151, 152 y 157 se refieren a la interceptación, incautación de datos, apertura, examen y cadena de custodia de la correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación.
- En particular la provincia de Chubut cuenta con un moderno Código Procesal Penal, que expresamente hace referencia a la recolección de la evidencia en el artículo 181 "Interceptación de comunicaciones del imputado" [12].
- El Código Procesal Penal de la provincia de Santiago del Estero [13] también contempla, aunque con menos detalles, lo relacionado al secuestro e interceptación de comunicaciones. Así se hace mención en el Capítulo IV – Secuestro: artículo 251, y también en los artículos 245, 247 y 254.

Los códigos citados se refieren, con mayor o menor profundidad, a la recolección y custodia de evidencias de manera tal que tengan validez legal en un proceso penal. En este sentido, es sustancial contar con un Protocolo de Actuación en donde se establezca con la mayor precisión la actuación de los funcionarios y operadores judiciales involucrados en la Investigación penal para la recolección de evidencias. Asimismo, es necesario establecer un marco jurídico que reglamente la preservación de las evidencias digitales obtenidas en la IPP.

3 Repositorio digital forense

3.1 Preservación de contenidos

La preservación digital es un problema esencial en el contexto de la informática forense, en la cual las evidencias digitales crecen de manera exponencial y cuyos contenidos se hacen cada vez más dinámicos.

Una copia de las evidencias digitales móviles no garantiza necesariamente su supervivencia a largo plazo. Por ello, en ausencia de una estrategia de preservación conveniente, la digitalización puede ser sinónimo de derroche de recursos (humanos y financieros) en gran escala.

Esta situación plantea otros problemas en el contexto de los Laboratorios de Informática Forense:

- Se enfrentan al constante desafío de la capacidad de recursos de almacenamiento disponible, provocado por el aumento del volumen digital y la cantidad de elementos de prueba que pueden estar asociados a una investigación.
- No existe un marco jurídico que garantice la preservación de las evidencias digitales.
- No hay una experiencia sustentable en el desarrollo de almacenamientos masivos de evidencias digitales, ni aún menos de evidencias digitales móviles.
- Las experiencias y el conocimiento que se generan durante las actividades operativas deberían ser almacenados y compartidos, de manera tal que puedan ser utilizados como guías de buenas prácticas. Las actividades operativas de los peritos podrían desarrollarse con mayor eficacia si contaran con la posibilidad de compartir antecedentes en relación a las actividades de extracción y análisis de evidencias. Al respecto, corresponde destacar que las pericias informáticas son consideradas como una tarea de media o alta complejidad, que requieren de una infraestructura tecnológica y de recursos humanos especializados e involucrados con procedimientos operativos que aseguren la cadena de custodia de las evidencias digitales móviles.

El desempeño de los Laboratorios de Informática Forense, en lo que respecta a su capacidad operativa, aumentaría en su eficacia como consecuencia de la gestión del conocimiento generado durante los procesos de obtención y análisis de evidencia por parte de los peritos informáticos y la posibilidad de compartir estas experiencias. En este sentido, contar con un repositorio para la preservación y la gestión de evidencias digitales extraídas de dispositivos móviles durante la IPP exige la elaboración de pautas que permitan constituirlo como una herramienta útil tanto para el archivado, consulta y referenciación por parte del personal autorizado.
Si bien las herramientas forenses de extracción y análisis de evidencia digital brindan funcionalidades vinculadas a repositorios de trabajo operativo en relación a una causa, los mismos no están relacionados con la preservación del contenido a largo plazo, en relación a las evidencias digitales y a las experiencias en la tarea pericial. Por otro lado, estas funcionalidades no permiten la interoperatividad entre los repositorios de las diferentes herramientas, aspectos estos que son características sobresalientes de los repositorios institucionales.

3.2 Repositorios institucionales

Son numerosos los ejemplos que podemos mencionar en el ámbito de las universidades, los centros de investigación, instituciones públicas, etc. que han tomado la decisión de diseñar e implementar repositorios y archivos digitales de acceso abierto, que son espacios virtuales con soporte de base de datos, en los que se puede depositar documentación de todo tipo y en todos los formatos posibles. Particularmente en el ámbito de la Justicia se mencionan:

- El Repositorio Institucional del Poder Judicial de la Provincia de Rio Negro es un punto de acceso a la información pública digital. El Digesto de Acordadas y Resoluciones del STJ. El Centro de Documentación Jurídica actualiza diariamente la base de datos. En la actualidad, el organismo cuenta con una colección bibli-

ográfica única en la provincia, acceso a bases de datos especializadas, catálogo en línea, boletín de novedades y un Repositorio Digital que cuenta con más de 9.000 Acordadas y Resoluciones del Superior Tribunal de Justicia. [14]
- El Repositorio Institucional del Poder Judicial de Buenos Aires, creado mediante el Acuerdo n° 3937 de la Suprema Corte de la provincia de Buenos Aires. Este se formará con los trabajos jurídicos de producción del Tribunal, así como también con trabajos aportados por sus magistrados, funcionarios y agentes, siempre que hubieran sido previamente publicados en publicaciones periódicas o editoriales de reconocido prestigio, o aprobados como trabajo final en carreras de posgrado, bajo la supervisión y control del Área de Coordinación de Bibliotecas y Biblioteca Central, dependiente de la Secretaría de Servicios Jurisdiccionales. [15]

Los repositorios facilitan el acceso a la información organizada y constituyen una herramienta para el trabajo que desempeñan los integrantes de las instituciones donde se implementan. En el ámbito de las instituciones públicas, los repositorios pueden brindar mayor información sobre la manera en que se resuelven conflictos, se organizan las responsabilidades y se llevan a cabo los procedimientos, normas y reglas, así como todas las actividades de los integrantes de la institución pública, otorgando a los ciudadanos un conocimiento pormenorizado del quehacer judicial y en consecuencia una mayor credibilidad en su accionar [16].
Los repositorios pueden almacenar información en diferentes tipos de formato como libros electrónicos, revistas, audios, videos, imágenes, entre otros, organizando los datos en colecciones ordenadas sobre las que es posible aplicar operaciones de búsqueda y consulta.
Se trata de un sistema “que hace uso de Internet, sirve para almacenar y controlar la información guardada en los contenidos digitales y facilita el acceso de sus usuarios a estos contenidos, generalmente desde cualquier lugar” [17].
Las características de los repositorios institucionales pueden ser resumidas en los siguientes términos: [18] [19].

- Permiten almacenar diferentes formatos de archivos, considerando escalabilidad, extensibilidad y mantenimiento.
- Aceptan estándares de metadatos, adecuadamente descriptivos, de preservación y administrativos.
- Facilitan la interoperatividad cumpliendo con los principales protocolos de intercambio de información.
- Permiten diferentes formas de búsqueda y visualización de metadatos.
- Cuentan con sistemas de seguridad que aseguran autenticación y autorización de usuarios para el acceso a los metadatos.

Para una institución las ventajas de implementar un repositorio institucional son amplias [18] [20]:

- Tanto la información como los documentos institucionales están almacenados en una misma base de datos.

- Facilita el acceso a la información recolectada presentándola en forma clasificada y organizada.
- Permite búsquedas rápidas dentro de la estructura de almacenamiento por diferentes patrones, agilizando el tratamiento de la información.
- Para el diseño del almacenamiento se siguen normas internacionales y estandarizadas que favorecen el intercambio.
- Se preserva el material digitalizado ajeno a los deterioros propios del soporte físico.

3.3 Cumplimiento de estándares internacionales para repositorios digitales

La Norma ISO 16363:2012 [21] define los requisitos necesarios para que un repositorio digital sea reconocido como de confianza, describiendo criterios de auditoría y certificación y métricas contra las que se puede evaluar el mismo. Los requisitos están asociados con:

- La infraestructura organizacional:
  - Definición de una misión que refleje el compromiso con la conservación a largo plazo, administración y acceso a la información digital.
  - Un plan estratégico para su preservación.
  - Una política que especifique qué tipo de información se va a preservar, conservar, gestionar y brindar acceso.
- La gestión de los objetos digitales:
  - Identificación del contenido y propiedades de la información que se preservará.
  - Definición de un proceso de ingesta que verifique que cada paquete de información transferido esté completo y sea correcto.
  - Procesos documentados para adquirir información de descripción de la preservación.
  - Especificación de requisitos mínimos de información para permitir que la comunidad de usuarios designados descubra e identifique material de interés.
  - Políticas de acceso a la información.
  - Procedimientos para asegurar la trazabilidad de los objetos digitales y respaldar su autenticidad.
- La gestión de riesgos de infraestructura y seguridad:
  - Identificación y gestión de riesgos para las operaciones de preservación y los objetivos asociados con la infraestructura del sistema.
  - Definición de medios de almacenamiento y procedimientos de actualización del hardware.
  - Gestión de la cantidad y ubicación de las copias de todos los objetos digitales.
  - Análisis sistemático de los factores de riesgo de seguridad asociados con los datos, los sistemas, el personal y el entorno físico.

3.4 Consideraciones para su definición inicial

Para llevar adelante el desarrollo de esta herramienta será necesario previamente analizar y considerar pormenorizadamente diversos aspectos de importancia para su definición inicial [22] [21] :

- Desarrollar un plan de servicio, definiendo la misión institucional y objetivos estratégicos para la preservación y acceso a la información a largo plazo. También es necesario definir políticas vinculadas a las evidencias digitales móviles que se van a preservar, conservar, gestionar, así como también la comunidad de usuarios destinatarios del servicio.
- Realizar una evaluación de las necesidades estableciendo el tipo de evidencia digital y sus metadatos. Para este tipo particular de repositorio institucional es fundamental asegurar la trazabilidad y respaldar la autenticidad de la evidencia digital almacenada, garantizando su relevancia, confiabilidad y suficiencia.
- Desarrollar políticas de actuación que gestionen la recopilación de contenidos y mantenimiento, refinando las características a cumplir por parte del repositorio de acuerdo a la taxonomía de evidencias forenses requeridas a ser almacenadas. Para esto será preciso organizar entrevistas estructuradas para identificar las necesidades operativas de los peritos de evidencias digitales.
- Prepara la planificación considerando recursos humanos, equipamiento tecnológico y demás costos asociados, analizando y seleccionando la tecnología apropiada para la gestión de los contenidos periciales digitales.
- Diseñar el repositorio, considerando especialmente los aspectos vinculados con la gestión de los riesgos de infraestructura y seguridad, teniendo en cuenta que el tipo de información almacenada en el repositorio será de acceso restringido.
- Formar el equipo interdisciplinario que tendrá a su cargo el desarrollo y la posterior administración del repositorio institucional.

En particular, un repositorio de evidencias forenses, como herramienta de apoyo al desempeño de la investigación judicial, podría almacenar no sólo la evidencia digital obtenida de dispositivos móviles, sino también constituir un sistema de gestión del conocimiento almacenando toda información relevante al proceso forense y las experiencias resultantes de la labor pericial.
Un repositorio que aborde y satisfaga los requerimientos de almacenamiento de la información digital referente a un procedimiento forense deberá recolectar evidencia digital obtenida desde dispositivos móviles proporcionando funcionalidades que garanticen la preservación y consulta de diversos tipos de archivos multimediales.
En la figura 1 se muestran las consideraciones para la definición inicial del repositorio institucional.
En la figura 2 se muestra la arquitectura global del repositorio institucional en el contexto del Ministerio Publico Fiscal de la provincia de Santiago del Estero.

Fig. 1. Consideraciones para la definición inicial del repositorio institucional.

3.5 Repositorio institucional en el contexto del Protocolo de Actuación

Los lineamientos propuestos por [1] pretenden ofrecer suficiente respaldo jurídico para la labor de los peritos informáticos y auxiliares de la justicia en la investigación penal, además de servir como una herramienta para la planificación y control de dicho proceso en la investigación penal preparatoria.

Estos lineamientos comprenden el proceso completo de tratamiento de la evidencia digital, dándole especial relevancia a las actividades y técnicas vinculadas al tratamiento y operación pericial de dispositivos móviles. La propuesta inicial [3] ha sido refinada y organizada en fases, la cual intenta abarcar el proceso completo de tratamiento de la evidencia digital, poniendo especial énfasis en las actividades y técnicas relacionadas con dispositivos móviles. En la figura 3 se muestra esquemáticamente el

conjunto de fases, aunque el proceso puede requerir eventualmente volver a alguna de las fases previas dependiendo de los resultados obtenidos y el avance de la IPP.

Fig. 2. Arquitectura global del repositorio institucional.

A partir de la Recepción del Oficio sobre solicitud de pericia será apropiado identificar los elementos relevantes según los puntos de pericia y luego serán analizados considerándolos como potencial evidencia digital, estos finalmente serán conservados y almacenados en los repositorios institucionales.
En este sentido, la elaboración de pautas de registración de los ítems del repositorio sería de utilidad para la gestión eficiente por parte de los agentes judiciales y peritos.
En este sentido, la elaboración de pautas de registración de los ítems del repositorio sería de utilidad para la gestión eficiente por parte de los agentes judiciales y peritos.

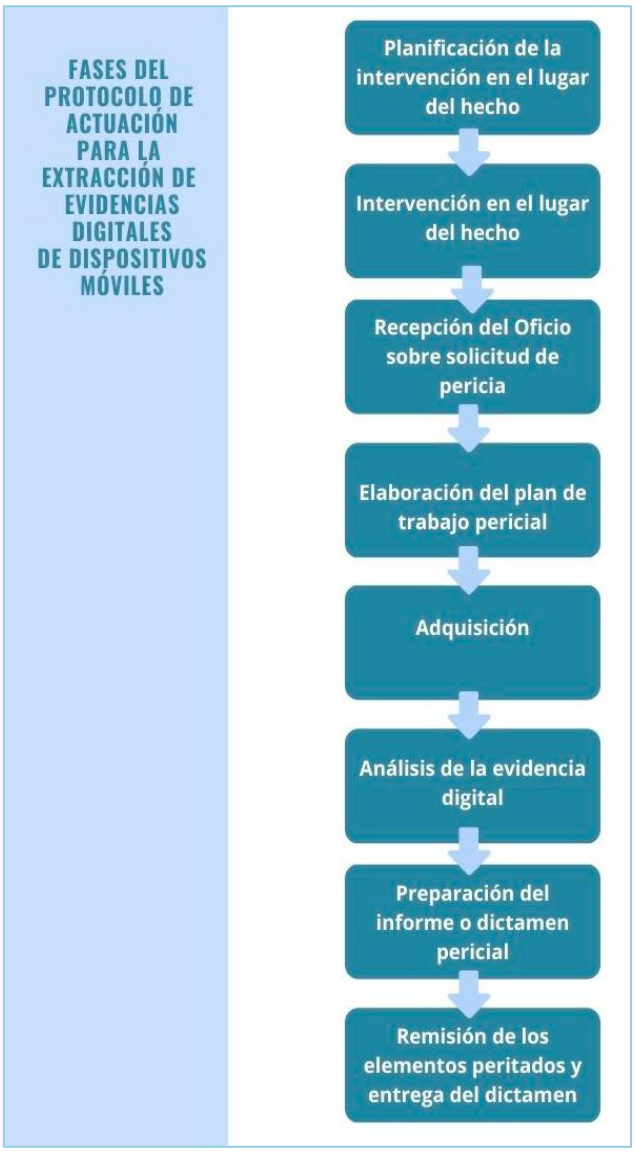

Fig. 3. Fases del protocolo de actuación para la extracción de evidencias digitales de dispositivos móviles

4 Conclusiones

Desde la conceptualización de la evidencia digital forense se pretendió abordar la complejidad de su recolección, la importancia del tratamiento de la información digitalizada y la gran influencia que la evolución de los dispositivos móviles está teniendo, impactando en la necesidad de establecer un Protocolo de Actuación en donde se detallen los procedimientos a llevar adelante para la recolección de las evidencias.
En ese contexto, el desenvolvimiento eficiente de los Laboratorios de Informática Forense debe contemplar aspectos relativos a la preservación de la evidencia digital, de modo que se asegure su resguardo, así como los correctos procesos de obtención y análisis de la evidencia, tanto para facilitar su acceso como para compartir experiencias de trabajo entre los peritos informáticos. A fin de cumplir estos objetivos, la definición y creación de un repositorio de evidencias digitales requiere el estudio de pautas a seguir para conformar una definición de repositorio ajustada a las necesidades del ámbito forense.
Un repositorio de evidencias forenses constituye una herramienta de apoyo al desarrollo de la investigación judicial, en donde además de almacenarse la evidencia digital podrían llevarse a cabo tareas de seguimiento de casos relevantes a los procesos forenses. Se establecieron las principales consideraciones para la definición de un repositorio adecuado al abordaje de dichas funciones según lo recomendado por los estándares internacionales y se definió una arquitectura global del repositorio institucional para el contexto del Ministerio Público Fiscal de la provincia de Santiago del Estero.
En un futuro, se pretende continuar el diseño y desarrollo del repositorio institucional validándolo respecto a las operaciones de almacenar, recuperar, distribuir y acceder de manera segura las evidencias digitales llevadas a cabo por parte de los involucrados en el proceso de investigación judicial.

Referencias

1. López, D. D. V. Evidencia digital (Bachelor's thesis) (2018).
2. Viaña, G.; Figueroa, L.; Lara, C.; Corvalán, A.; Lesca, N. Protocolo de actuación para recolección y preservación de la evidencia digital móvil en el Sistema Procesal Penal de Santiago del Estero. CoNaIISI 2018. ISSN 2347- 0372. (2018).
3. Herrera, S. I., Figueroa, L. M., Ghunter, D., Lara, C., Viaña, G., Mendez, A., & Lesca, N. Métodos y herramientas para el análisis forense de dispositivos móviles. In XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan) (2019).
4. Villadiego, A. Uso de la informática forense aplicada a delitos informáticos en la industria colombiana. (2019).
5. Rodríguez García, Carlos Emilio. "Introducción a la Informática Forense: Legal, teórica y práctica." (2019).
6. Bautista, D. R., & Rueda, J. S. R. La informática forense en dispositivos Android. Revista Ingenio, 9(1), 21-34 (2016).

7. Ghosh, A. Guidelines for the Management of IT Evidence. In APEC Telecommunications and Information Working Group 29th Meeting (2004).
8. Navarro Clérigues, Jorge. Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico. Diss. 2016.
9. Gómez, L. S. M. Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados. In Simposio Argentino de Informática y Derecho (SID 2015)-JAIIO 44 (2015).
10. Ley 23.984 – Código Procesal Penal de la Nación, http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=383, ultimo acceso 2020/06/20.
11. Ley 27.063 – Código Procesal Penal Federal, http://www.saij.gob.ar/27063-nacional-codigo-procesal-penal-federal-to-2019-lns0006496-2019-02-07/123456789-0abc-defg-g69-46000scanyel?, ultimo acceso 2020/06/20.
12. Ley XV N° 15 - Boletín Oficial 21/9/10 N° 11069. Código Penal Procesal de Chubut, http://www.mpfchubut.gov.ar/images/pdf/cpp.pdf, ultimo acceso 2020/06/20.
13. Ley provincial 6.941. Código Procesal Penal de la Provincia de Santiago del Estero (2009), http://www.jussantiago.gov.ar/jusnueva/Normativa/Ley6941.php, ultimo acceso 2020/06/20.
14. Piccinini, Liliana, et al. "Repositorio digital de resoluciones y acordadas." XVI Simposio Argentino de Informática y Derecho (SID 2016)-JAIIO 45 (Tres de Febrero, 2016). 2016.
15. Chazarra Bernabé, J., Requena López, V. M., & Valverde Jerónimo, S. Desarrollo de un repositorio de objetos de aprendizaje usando DSpace. (2010).
16. Duperet Cabrera, E., Pérez Martínez, D. G., Cedeño Rodríguez, M. Y., Ramírez Mustelier, A., & Montoya Acosta, L. A. Importancia de los repositorios para preservar y recuperar la información. Medisan, 19(10), 1283-1290. (2015).
17. De Giusti, M. R. "Curso de posgrado: Bibliotecas y repositorios digitales. Tecnología y aplicaciones." Curso de posgrado de Repositorios Digitales (Facultad de Informática, 2018) (2018).
18. Flores, W. X. V., & Escobar, J. E. F. Repositório Digital. (2017).
19. Weiser, Mark, David P. Biros, and Greg Mosier. "Development of a national repository of digital forensic intelligence." (2016).
20. Gómez, L. S. M., & Herrera, H. H. Gestión del conocimiento aplicada al peritaje informático. In XI Workshop de Investigadores en Ciencias de la Computación (2009).
21. Viaña, G.; Figueroa, L.; Lara, C.; Lesca, N.; Binda, A. Importancia de la evidencia digital móvil en el Sistema Procesal Penal. CIIDDI 2018. ISBN 978-950-623-153-8. (2018).