***

Recomendaciones para la incorporación de la Prueba Digital en los procesos judiciales no penales

Ana Di Iorio[1], Marisa Repetto[2], María Fernanda Rosales[3], Pablo Cistoldi[4], María Fernanda Diaz[5], Bruno Constanzo[6], Santiago Trigo[7], Mario Adaro[8], Lucia Algieri[9], Bibiana Luz Clara[10]

Resumen

En este trabajo expondremos los avances del proyecto “Guía de Recomendaciones para la Implementación de Protocolos de Adquisición, Preservación y Presentación de la Prueba Digital” cuyo objetivo es el desarrollo de un conjunto de Buenas Prácticas de extracción, adquisición, preservación y presentación de prueba digital que permitan dar validez y acreditar los hechos que resultan controvertidos en el marco de los procesos judiciales civiles y comerciales, laborales y de familia.

Palabras Claves: Prueba Digital, Protocolo, Correo electrónico

Keywords: Digital Evidence, Forensic Guidelines, E-mail

[1] Ingeniera en Informática. Especialista en Gestión de la Tecnología y la Innovación. Directora del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense InFo-Lab. Docente Investigadora Universidad FASTA. diana@ufasta.edu.ar
[2] Licenciada en Ciencia Política y Administración Pública. Abogada. Docente. Universidad Nacional de Cuyo. marisarepetto@hotmail.com
[3] Ingeniera en Informática. Especialista en Informática Forense. Docente Investigadora Universidad FASTA. rosalesmar@ufasta.edu.ar
[4] Abogado. Especialista en Criminalidad Económica. Docente Investigador Universidad FASTA. pcistoldi@ufasta.edu.ar
[5] Abogada. Jueza del Juzgado de Paz Letrado y Contravencional del Departamento de Lavalle Provincia de Mendoza. Magister en Magistratura y Gestión Judicial Universidad de Mendoza y Universidad Nacional de Cuyo, segunda cohorte, diazmariafernanda@hotmail.com
[6] Ingeniero en Informática. Docente Investigador Universidad FASTA. bconstanzo@ufasta.edu.ar
[7] Ingeniero en Informática. Docente Investigador Universidad FASTA. santiagotrigo@ufasta.edu.ar
[8] Ministro de la Suprema Corte de Justicia de la Provincia de Mendoza. Presidente del Instituto Federal de Innovación, Tecnología y Justicia (IFITEJ-JUFEJUS). Director de la Diplomatura en Innovación y Gestión Judicial Tecnológica. Universidad Champagnat. mariodanieladaro@yahoo.com.ar
[9] Licenciada en Criminalística. Docente Investigador Universidad FASTA. luciaalgieri@ufasta.edu.ar
[10] Abogada. Doctora en Derecho. Docente Investigador Universidad FASTA. BLuzClara@ufasta.edu.ar

***

Introducción

La transformación digital de la sociedad impacta de manera directa a las personas, las instituciones, los procesos y a sus relaciones. La información digital disponible es cada vez más abundante, y por consiguiente, la posibilidad de ser ofrecida como prueba en los procesos judiciales es un reto creciente para los Estados, y en particular, para sus operadores en materia de justicia.

La incorporación de la prueba digital a los procesos judiciales se fue realizando de manera paulatina. En los procesos penales se formalizaron diversas guías de buenas prácticas y protocolos de actuación.Sin embargo, en los restantes fueros esto es aún una tarea pendiente.

Presentamos en este trabajo los avances del proyecto “Guía de Recomendaciones para la Implementación de Protocolos de Adquisición, Preservación y Presentación de la Prueba Digital”, formulado en conjunto entre la Facultad de Ingeniería y la Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA, y la Facultad de Derecho de la Universidad Champagnat.

El objetivo es el desarrollo de un conjunto de Buenas Prácticas de extracción, preservación y presentación de prueba digital que permitan dar validez y acreditar los hechos que resultan controvertidos en el marco de los procesos judiciales no penales. Motiva este desarrollo el hecho de que los organismos de las Justicias Provinciales no cuentan con protocolos o guías de actuación para la recuperación ni la incorporación de pruebas digitales en el marco de los procesos civiles, comerciales, laborales, tributarios, administrativos y de familia.

Así, tanto los abogados a la hora de incorporar la prueba digital como los jueces al momento de valorar la prueba y decidir, se encuentran frecuentemente con problemáticas propias de esa disciplina vinculadas con la carencia de una aplicación adecuada de los principios forenses básicos, esto es, método, reproducibilidad del proceso, mantenimiento de la cadena de custodia y evitar la contaminación de la prueba.

La Junta Federal de Cortes y Superiores Tribunales de las Provincias Argentinas y Ciudad Autónoma de Buenos Aires (Ju.Fe.Jus) toma esta necesidad generalizada de los organismos de justicia, y la hace propia y formal a través de su Instituto Federal de Innovación, Tecnología y Justicia (IFITEJ).

Asimismo, el compromiso de adopción temprana del desarrollo de este proyecto por parte de la Suprema Corte de Justicia de la Provincia de Mendoza permitirá su

***

validación y transferencia al resto de las provincias que constituyen una demanda potencial importante, en tanto la propia Ju.Fe.Jus será la promotora de tal transferencia.

Presentación del trabajo

Antecedentes

En los procesos penales a partir del año 2016 se formalizaron diversas guías de buenas prácticas y protocolos de actuación, tal como la *Guía de obtención, preservación y tratamiento de la evidencia digital* [11]. Este documento ha sido diseñado y pensado para el accionar de los agentes fiscales del Ministerio Público Fiscal de la nación en la tarea de la investigación penal.

De igual manera se formalizó por Res 483/16 de la Procuración General de la Suprema Corte de Justicia de la provincia de Buenos Aires la *Guía Integral de empleo de la Informática Forense en el Proceso Penal*[12].

Sin embargo, en los restantes fueros no penales no ha ocurrido lo propio.

La evidencia digital es el conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico (Infolab, 2016).

Y una de las características principales de la evidencia digital, y que la torna compleja en sí misma, es su **volatilidad.** Ello conlleva a que, por su propia naturaleza, sea frágil, fácil de alterar y dañar o directamente de destruir.

De acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por **tres principios fundamentales**: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en corte o no.

La **relevancia** es una condición técnicamente jurídica, que hace referencia a aquellos elementos que son significativos a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos.

---

[11] La “Guía de obtención, preservación y tratamiento de la evidencia digital” fue aprobada por Resolución de la Procuración General de la Nación N° 756/2016, con el fin de recomendar a todos/as los/as magistrados/as del Ministerio Público Fiscal que ajusten su proceder a los lineamientos de este documento en todos los casos en que resulte aplicable, disponible en https://www.mpf.gob.ar/ufeci/enlaces/protocolos-y-guias-de-actuacion/.

[12] La “Guía Integral de empleo de la Informática Forense en el proceso penal” se desarrolla a partir del Modelo PURI - Proceso Unificado de Recuperación de la Información Digital de la Facultad de Ingenieria de la Universidad FASTA disponible en https://info-lab.org.ar/images/pdf/PAIF.pdf

***

Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio.

La **confiabilidad** refiere a que el proceso aplicado para obtener la evidencia digital sea en la medida de lo posible repetible y auditable, esto implica que si un tercero sigue el mismo proceso con las mismas herramientas, deberá obtener los mismos resultados verificables y comprobables.

La **suficiencia**, está relacionada con la completitud de la evidencia digital, es decir que, con las evidencias que se recolectaron y analizaron se tiene suficientes elementos para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada (Rosales, 2021).

Si bien puede haber otros elementos que ayuden en el gobierno de la evidencia digital, ISO ha determinado que estos tres establecen las condiciones necesarias y suficientes para que los expertos en informática forense recaben, aseguren y preserven elementos materiales probatorios sobre medios digitales, los cuales podrán ser revisados y analizados por terceros interesados y sometidos a contradicción según el ordenamiento jurídico donde se encuentren [13].

En consecuencia, la metodología que utilicemos para la identificación, recolección, obtención y preservación de la información será crucial para que la evidencia digital pueda ser utilizada como evidencia útil en el proceso judicial (prueba en sentido estricto).

Con esta finalidad, en el marco del proyecto habremos de considerar los siguientes principios forenses (Di Iorio et al 2017, p. 76; InfoLab, 2022: 1m53s):

- **Evitar la contaminación:** Significa que siempre que sea posible se procurará mantener la la prueba inalterable, desde el momento que fue producida y recolectada.
- **Controlar la cadena de custodia:** Controlar durante todo el proceso el destino de los efectos, desde que la prueba es recolectada hasta que llega a su destino final.
- **Actuar metódicamente:** En todo momento debe actuarse por medio de un método o proceso validado que permita reconstruir las operaciones realizadas. Tiene que haber un método para la recolección, conservación y posterior análisis de esa prueba.

---

[13] La “Guía de obtención, preservación y tratamiento de la evidencia digital” fue aprobada por Resolución de la Procuración General de la Nación N° 756/2016, disponible en https://www.mpf.gob.ar/ufeci/enlaces/protocolos-y-guias-de-actuacion/.

***

Fases de Incorporación de la Prueba Digital

El desafío de acceder a estos nuevos tipos de rastros y documentos puede generar vértigo y ansiedad en las personas que trabajan en los poderes judiciales, ejerciendo la magistratura o litigando en ejercicio de la abogacía, incluso en quienes se desempeñan en peritajes técnicos.

Emerge así la necesidad de contar urgentemente con instructivos y recetas que nos permitan salir del paso con cierta seguridad.

Las recetas son necesarias, aunque no suficientes. Sirven para aplacar nuestro ánimo y para dar los primeros pasos, pero no tal vez para guiarnos durante todo el camino de incorporación de la prueba digital en el proceso judicial.

Además de las recetas, se requiere poder establecer objetivos claros. Esta necesidad se plantea, con distintas variantes, a cada jueza y juez responsables de la dirección de los procesos y la resolución de casos, a cada funcionario y auxiliares del sistema de justicia, y a quienes ejercen la abogacía como litigantes.

Pero la justicia no es sólo un conjunto de recetas y objetivos. Los sistemas judiciales, y cada tribunal, deben aportar algo valioso para la convivencia social. Son los valores (justicia, cuidado, pacificación…) los que dan sentido a las recetas y a los objetivos. Más allá de que las recetas nos ayudan a salir del vértigo que nos provocan las pruebas tecnológicas, y de la innegable utilidad práctica de fijar y cumplir objetivos medibles, son los valores los que deben integrar y orientar el conjunto de actividades del sistema judicial (tanto en general como en el caso a caso), para que nuestro trabajo brinde un aporte relevante para la convivencia social.

En los avances parciales realizados en el proyecto que aquí se presenta, hemos logrado formalizar las fases de la incorporación de la prueba digital en los fueros no penales: búsqueda, adquisición, ofrecimiento y admisión, producción y/ o presentación, alegatos y valoración de la prueba digital. Cada una de estas etapas contiene los usuarios y requisitos principales y sugerencias u observaciones.

Por ejemplo, en la fase de adquisición de la prueba digital, los usuarios protagonistas pueden ser los abogados, los justiciables, el perito forense o el tribunal. Los requisitos principales a tener en cuenta serán la licitud del proceso de adquisición, la confiabilidad y preservación, la temporalidad, la pertinencia, los costos y accesibilidad y el análisis de ventajas comparativas.

***

De las observaciones surge que la fase de adquisición y la fase de ofrecimiento no son necesariamente secuenciales. La licitud del proceso de adquisición, la confiabilidad y temporalidad de dicho proceso están directamente relacionadas con su necesidad y eficacia para fases futuras (producción, alegación y valoración).

Protocolos para la incorporación de la prueba digital.

En la guía desarrollaremos protocolos para la incorporación de los distintos tipos de prueba digital presente en: correos electrónicos, redes sociales, servicios de mensajería, sitios web y archivos en general.

A modo de ejemplo, en el siguiente apartado describimos la guía de buenas prácticas y recomendaciones en la adquisición de prueba digital en los correos electrónicos.

Consideraciones en la incorporación de Correos Electrónicos

En muchas ocasiones, los mensajes de correo electrónico son aportados únicamente mediante capturas de pantalla.

Si bien esto podría considerarse un puntapié para iniciar o evidenciar la existencia de cierta comunicación, no es la forma correcta de aportar este contenido ya que la captura de pantalla es fácilmente alterable o, incluso es posible crear una imagen apócrifa que falsee esa comunicación.

Por ello, debemos tener en cuenta ciertos recaudos técnicos a la hora de aportar una prueba de este tipo.

Por otra parte, es importante mencionar que hoy en día el correo electrónico podría asimilarse a una aplicación de mensajería instantánea.

Los mensajes de correo llegan casi al instante pero tienen una gran diferencia con la mayoría de las aplicaciones de mensajería instantánea: una vez que el mensaje es enviado, llegará a su destino (siempre y cuando exista la cuenta destino), sin la posibilidad de que el emisor pueda detener o eliminar el mensaje remotamente en la casilla destino de su receptor.

Por ejemplo, varias aplicaciones de mensajería instantánea, permiten eliminar el mensaje tanto del lado del emisor como del receptor. Con el correo electrónico esto no es posible debido a su estructura y funcionamiento.

Esta característica lo constituye como un tipo de evidencia que perdura en el tiempo, excepto cuando se da el caso de que el mismo propietario de la cuenta de correo

***
electrónico borre intencionalmente dicho mensaje de correo. Es decir, que todo mensaje que quiera ser aportado como prueba, no debe eliminarse de la cuenta o casilla de correo de quien lo quiera aportar.
Ahora bien, dicho esto, el correo electrónico también tiene una desventaja con respecto a las aplicaciones de mensajería más modernas.
En algunas ocasiones, es más complejo poder determinar su autenticidad si no se siguen ciertas consideraciones, ya que utiliza un protocolo bastante antiguo, pero no por eso obsoleto o ineficiente.
A medida que ha pasado el tiempo, se han implementado ciertas medidas de seguridad al correo electrónico para verificar su autenticidad.
Se describen a continuación un conjunto de buenas prácticas para la realización de esta tarea.

Buenas prácticas y recomendaciones a la hora de aportar un mensaje de correo electrónico como prueba digital en un proceso judicial

1. **Descargar el correo electrónico**

En primer lugar se debe descargar el mensaje original completo. Esto es fundamental, dado que el mensaje completo contiene todos los datos de interés: direcciones IP de servidores, dominios de servidor involucrados, registros de seguridad, asunto, emisor, destinatarios, cuerpo del mensaje, entre otros.
Dependiendo la aplicación que se utilice como cliente de correo electrónico esta opción puede variar de nombre, pero generalmente podemos encontrarla como “Ver mensaje original” o similar.
Al descargar este mensaje, simplemente, se genera un archivo de texto (".eml" o similar) conteniendo todas estas características.
El nombre con el que se almacena este archivo se sugiere que sea descriptivo.

2. **Descargar los archivos adjuntos**

Si el mensaje de correo tuviere adjuntos, se deben descargar estos archivos con nombres descriptivos para incorporar. Se recomienda no ejecutar estos adjuntos en la PC destino donde se ha descargado.

3. **Generar archivo comprimido y obtener hash**

***

Una vez descargados el correo electrónico original y los archivos adjuntos -si los hubiera- se deben comprimir estos en un único archivo y calcular la función de hash sobre el comprimido para garantizar la integridad del mismo.

4. **Generar acta o informe**

Realizar un acta o informe donde se especifiquen las partes intervinientes en el acto, las tareas realizadas, los nombres de los archivos que se incorporan, la función de hash utilizada y el valor de hash resultado.

Sugerencia: El valor hash siempre debe ser incorporado en este acta o informe, impreso en papel o firmado digitalmente, nunca enviarse como archivo de texto por el mismo medio en que es transportado el archivo de mensaje de correo propiamente dicho.

5. **Preservar los archivos**

Adjuntar el archivo de texto conteniendo el mensaje completo u original y los archivos adjuntos que se aportarán en el medio de almacenamiento que se considere pertinente. Se sugiere que se aporte en un medio de almacenamiento de sólo lectura, por ej. CD o DVD.

Consideraciones para verificar la autenticidad de un correo electrónico

- La autenticidad de un correo electrónico puede verificarse bajo ciertas condiciones y será efectiva en el único caso en que el mensaje de correo sea aportado por la cuenta receptora. Si desea aportar un mensaje de correo desde la cuenta emisora, algunos de estos parámetros no podrán ser visualizados.
- El remitente real de un mensaje puede ocultarse. Este enmascaramiento podría observarse y pasar inadvertido si sólo se observa la vista convencional de un correo electrónico y no la vista del mensaje original.
- Al observar el archivo de texto con el mensaje original, (generalmente ".eml") conteniendo todo el mensaje de correo electrónico, se debe prestar atención a los siguientes registros del archivo:
  - *"smtp.mailfrom":* especifica el usuario y dominio del servidor saliente del correo electrónico. Aquí es donde puede observarse realmente qué casilla de correo envió el mensaje. Si esta no coincide con el remitente, es posible que se esté tratando de un mensaje de correo falso o que intenta suplantar la identidad de un usuario (phishing). Lamentablemente, este parámetro también puede ser alterado.

***

- *"Received: from"*: especifica el nombre del equipo y dirección IP del servidor que envió el mensaje de correo electrónico. Si por ejemplo, se recibe un mensaje de correo electrónico de una cuenta que parecería ser "usuario@dominiol.com" pero cuando se observa este registro, se verifica que es "mail.fake.com", se puede determinar que el dominio del servidor saliente del correo (fake.com) es diferente al dominio por el que se suponía que se había recibido el correo (dominio.com).
- *"Message-ID"*: este campo proporciona un identificador de mensaje único que se refiere a una versión específica de un mensaje en particular. Este campo podría ser utilizado para comparar que el mensaje de correo sea el mismo si se lo observa desde la cuenta del emisor, como desde la cuenta del receptor o bien, si se lo quiere comparar con algún otro mensaje de correo aportado al proceso. Si son iguales, podría tratarse del mismo mensaje de correo.
- *Registro SPF* (Sender Policy Framework): Informa si la dirección IP del servidor saliente de ese mensaje de correo electrónico está autorizada para enviar correos bajo ese dominio. Es un registro que debe ser configurado por los administradores del correo electrónico. Puede tener tres resultados esperables: PASS, quiere decir que la dirección IP que envió el mensaje de correo electrónico recibido, está autorizada para hacerlo. Caso contrario es "FAIL". Si se observa que el valor de dicho registro es "NEUTRAL" quiere decir que no se ha configurado el registro, por lo que no se puede determinar, a través del mismo, la autenticidad del mensaje. Si el registro tiene el valor FAIL, en la mayoría de los casos, se podría decir que es un correo que intenta suplantar la identidad de un usuario ya que el mensaje de correo electrónico fue enviado a través de un servidor que no está autorizado para hacerlo aunque también podría tratarse de una mala configuración de dicho registro por parte de los administradores del sistema o del correo electrónico. Por lo general, los clientes de correo electrónico utilizados, cuando detectan el valor FAIL, envían el correo a SPAM o correo no deseado.
- *Registro DKIM* (DomainKeys Identified Mail): es un registro que permite firmar el correo con el dominio de la cuenta de origen. De este modo, el destinatario está seguro de que el correo ha sido enviado desde el servidor origen y no ha sido interceptado y/o reenviado desde otro servidor no autorizado. Si este registro poseé el valor "PASS" quiere decir que es auténtico. En cambio sí posee el valor "FAIL" podría indicar que el servidor por el cual fue enviado ese correo, no es el real y, por lo tanto, podría tratarse de una falsificación. También es un registro que se configura.

***

- *Registro DMARC* (Domain-based Message Authentication, Reporting and Conformance): Este registro complementa al SPF y DKIM y especifica qué hacer cuando alguno de los registros anteriores da error (valor "FAIL"). Si bien este registro no es utilizado para verificar la autenticidad de un correo, a través de él, es posible determinar por qué un mensaje de correo ha llegado a la bandeja de "SPAM" o correo no deseado.
- *"Received: by"*: mediante este registro se puede determinar la hora exacta en la que se recibió el correo. Nótese que esta fecha no será idéntica a la fecha de enviado del mensaje de correo electrónico si se lo está observando desde la casilla de correo del emisor del mismo. Siempre se tendrá una diferencia entre enviado y recibido.

Mediante todas estas consideraciones, será posible, no sólo incorporar un mensaje de correo electrónico a un proceso judicial, sino también, verificar la autenticidad del mismo. Es importante tener especial atención en que, los métodos aquí descriptos no están disponibles si se está utilizando el cliente nativo de correo electrónico de Windows 10 o superior. Por otra parte, si lo que se quiere es preservar una cadena de correos electrónicos, es decir, mensajes y sus respuestas, se deberá realizar esta operación por cada uno de los mensajes. Por ejemplo, si se realiza la preservación del último mensaje de correo dentro de una cadena de mensajes, sólo se preservarán los datos de este último y no así de todos los anteriores.

Reflexiones y Conclusiones

Resulta evidente que el incesante avance tecnológico impacta -y seguirá impactando- fuertemente sobre la justicia en muchas de sus dimensiones. Una de ellas es, indefectiblemente, la incorporación de la prueba digital en los procesos judiciales.

La creciente cantidad de dispositivos y aplicaciones, su uso masivo y el impresionante caudal de datos que se produce y circula mediante ellos, hacen surgir nuevas fuentes de información con valor probatorio.

Este planteo se relaciona con tres distintos modelos de dirección de las organizaciones: dirección por instrucciones, dirección por objetivos y dirección por valores. Las tres perspectivas son necesarias.

Desde nuestra visión, los valores sirven si conectan nuestro trabajo con las necesidades legítimas de la comunidad y de quienes concurren al sistema de justicia

***
en procura de solucionar sus conflictos: los justiciables. No es necesario buscar demasiado lejos para encontrarlos. En los preámbulos y en los textos de nuestras constituciones y de los tratados de derechos fundamentales hallamos una fuente de conexión que da sentido a la función de los sistemas judiciales y de cada proceso judicial concreto.

La elaboración de una guía para el empleo y valoración de la prueba digital debe abarcar e integrar estos tres planos: instructivos, objetivos y valores jurídicos fundamentales.

Un ejemplo muy claro de esto es el desafío que plantea la brecha digital, que podría amplificar en gran medida las barreras de acceso a la justicia. Todos conocemos recetas de alimentación sana cuyo costo es inalcanzable para la mayoría. En el ámbito judicial esto no debería suceder. Los instructivos para la presentación y valoración de la prueba digital deberán ser incluyentes, no excluyentes.

Lo mismo sucede con los objetivos de gestión de casos y de gestión del caso. Si recetas y objetivos no favorecen el acceso a la tutela judicial efectiva en condiciones igualitarias, por mayor calidad técnica que tengan, estarán lejos de la misión fundamental de un sistema judicial.

Ahora bien, ¿cómo elaborar instructivos y delinear objetivos útiles para todos sin renunciar a la verdad como fundamento de las resoluciones judiciales? Para esto no hay recetas. Aunque… Podemos empezar con algo.

En primer lugar, no debe perderse de vista las especiales condiciones de vulnerabilidad -o hiper vulnerabilidad- que puede presentar alguna persona o grupo social a la hora de acceder a la justicia. En este sentido, la revisión de los criterios de valoración de la prueba en cuestiones de violencia de género o de conflictos ambientales, pueden ser una buena analogía de los desafíos que seguramente habrá de plantear la prueba digital cuando exista disparidad de condiciones entre las partes y el riesgo de afectación de derechos fundamentales.

Existen además herramientas prácticas, como la inclusión de criterios de temporalidad y accesibilidad económica de la prueba compleja, el desarrollo de nuevas clases de indicios y presunciones, el trabajo con las cargas probatorias a lo largo del proceso, etc. Todas ellas, utilizadas de modo crítico y flexible, pueden ayudar a alcanzar niveles aceptables de aproximación a la verdad, tutelando a la vez el acceso igualitario a la justicia.

***

Para el Instituto de Innovación, Tecnología y Justicia -IFITEJ- de la Junta Federal de Cortes y Superiores Tribunales de la República Argentina - Ju.Fe.Jus, la Universidad Champagnat y la Universidad FASTA es de gran importancia y relevancia apoyar el trabajo investigativo en materia de prueba digital para procesos no penales.

Esta investigación posibilitará contar, en los distintos poderes judiciales del país, con una guía de buenas prácticas que sistematice y parametrice las principales problemáticas y abordajes en materia de prueba digital: su adquisición, reconocimiento, ofrecimiento y valoración, alcanzando una validación y uso por parte de los diversos actores de los sistemas de administración de justicia.

Agradecimientos

Queremos agradecer a las y los investigadores que forman y formaron parte de este proyecto, a las autoridades de la Facultad de Ciencias Jurídicas y Sociales y de Ingeniería de la Universidad FASTA, de la Facultad de Derecho de la Universidad Champagnat y de la Junta Federal de Cortes y Superiores Tribunales de Justicia por confiar en nosotros para este desarrollo.

Referencias

Infolab. (2016). Guía Integral de empleo de la Informática Forense en el proceso penal" se desarrolla a partir del Modelo PURI - Proceso Unificado de Recuperación de la Información Digital. Mar del Plata. Facultad de Ingeniería de la Universidad FASTA. [Archivo PDF] https://info-lab.org.ar/images/pdf/PAIF.pdf

Di Iorio, A. H., et al (2017). El Rastro Digital del Delito: Aspectos Técnicos, Legales y Estratégicos de la Informática Forense. Mar del Plata. Universidad FASTA. [Archivo PDF] http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1593

ISO/CEI 27037:2012. (2012). *Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales.* Recuperado de: https://www.iso.org/standard/44381.html (consultado 24/04/2023)

***

Procuración General de la Nación. Resolución N° 756/2016 (2016). *Guía de obtención, preservación y tratamiento de la evidencia digital*. Recuperado de https://www.mpf.gob.ar/ufeci/enlaces/protocolos-y-guias-de-actuacion/

Rosales, M.F. (2021). *Guía de recomendaciones para la preservación de la prueba sobre el uso y acceso a los Sistemas de Información en un entorno corporativo*. Mar del Plata. Facultad de Ingeniería de la Universidad FASTA.