LABORATORIO DE FORENSIA DIGITAL: PROPUESTA DE ESTRUCTURA Y FUNCIONAMIENTO

FORENSIC DIGITAL LABORATORY: STRUCTURE AND OPERATION PROPOSAL

Luz Clara, Bibiana I; Aráoz Fleming, José Daniel I; Parra de Gallo, Herminia Beatriz I

I. luzbibianaclara@gmail.com, jdaraoz@ucasal.edu.ar, bgallo@ucasal.edu.ar, Facultad de Ingeniería, Universidad Católica de Salta, Argentina

RESUMEN

Resultan fundamentales y necesarios los laboratorios forenses dedicados al análisis de la evidencia digital, organizaciones con estructuras que brinden un servicio cada vez más útil para la sociedad. Estructuras que apoyen al privado en las pericias de parte, pero que también coadyuven con la justicia en la resolución de los conflictos crecientes en donde las Tecnologías de la Información y las Comunicaciones (TICS) se ven involucradas y que cada vez crecen más. Y desde estas premisas se propone la optimización del DigiLab, un laboratorio forense existente en la Facultad de Ingeniería de la Universidad Católica de Salta. El presente trabajo describe el marco teórico, los antecedentes y la propuesta de puesta en valor de dicho laboratorio, enfatizando los aspectos propios de la organización funcional del mismo, sobre la base de los tres ámbitos que abarca el DigiLab: la investigación y docencia en la universidad, la asistencia técnica a terceros y la capacitación técnica de recursos humanos especializados en Forensia Digital.

.

PALABRAS CLAVE:

Forensia Digital; laboratorio forense; evidencia digital.

ABSTRACT

The forensic labs are fundamental and necessary, they are dedicated to digital evidence analysis, organizations with structures that offer a very useful service for the society. These structures support the private sector in the part expertise, but also assist to the justice in the resolution of the increasing conflicts where the Information and Communication Technology (ICT) are involved. And from these premises, they propose the DigiLab optimization, a forensic lab which exists in the Faculty of Engineering of Universidad Católica de Salta. This work describes the theoretical framework, the backgrounds and the put in value of this lab, highlighting the own aspects of its functional organization, on the base of three ambits which the DigiLab encompasses: the research and teaching at university, the technical assistance to thirds parts and the

technical training of the human resources who are specialized in Digital Forensic.

KEYWORDS:
Digital Forensics; forensic laboratory; digital evidence.

INTRODUCCIÓN

Desde anteriores trabajos, que surgieran del seno de la Universidad Católica de Salta, se viene destacando la importancia que adquirieron las pericias informáticas en el ámbito del derecho.

En los tiempos que corren, en donde la pandemia que atraviesa la humanidad por la aparición del COVID-19, ha hecho sustancialmente necesario el uso de las redes informáticas, en donde la necesidad ha llevado al contacto físico a su mínima expresión potenciándose la necesidad de apelar a los entornos de comunicación virtual. Con ello toma mayor trascendencia aún la necesidad de recolectar y analizar la evidencia de tipo digital.

Y es en el ámbito virtual donde incluso se mueve al día de hoy la educación de nuestros alumnos; de todos los niveles, primario, secundario y universitario. Es en este ámbito en donde profesionales, comerciantes, empresarios, asalariados, profesores, estudiantes, vienen transcurriendo su vida desde principios del corriente año; totalmente en la mayoría de los casos y en forma parcial en los menos.

Y así como internet es el nuevo mundo en donde se desarrollan la mayor parte de nuestras actividades, para lo bueno, también se ha convertido en el lugar favorito de delincuentes y malhechores.

Es justamente allí donde debe actuar la justicia y sus aliados. Y son los peritos, los ingenieros y técnicos especializados en informática, en telecomunicaciones, quienes justamente deben potenciar y maximizar su actuación en este contexto.

Por ello resultan fundamentales y necesarios los laboratorios forenses dedicados al análisis de la evidencia digital, organizaciones con estructuras que brinden un servicio cada vez más necesario para la sociedad. Estructuras que apoyen al privado, en las pericias de parte, pero que también coadyuven con la justicia en la resolución de los conflictos crecientes en donde las Tecnologías de la Información y las Comunicaciones (TICS) se ven involucradas y que cada vez crecen más. Estructuras que, se conviertan en iconos de la sociedad en que están insertas. Estructuras que tengan un rol estratégico en el mundo en que estamos insertos, en el mundo de la tecnología, en la sociedad del conocimiento, en la vida virtual.

Y es desde estas premisas desde donde se propone la optimización del DigiLab, un laboratorio forense existente en el ámbito de la Facultad de Ingeniería de la Universidad Católica de Salta (UCASAL). Abonando con ello la conformación de un laboratorio específico destinado de manera complementaria a la formación de los futuros ingenieros en informática, en las metodologías y herramientas vinculadas al análisis forense digital.

El presente trabajo está estructurado en las siguientes secciones: la primera sección describe los Antecedentes del Laboratorio de Forensia Digital; en la segunda sección se avanza sobre el marco teórico utilizado para esta propuesta; luego en la tercera sección se desarrolla la PROPUESTA DE DEFINICIÓN DE LA ESTRUCTURA ORGANIZATIVA DEL LABORATORIO DE FORENSIA DIGITAL con una descripción puntual de los aspectos relacionados (dependencia organizativa, objetivos, cobertura y alcance, recursos financieros, estructura funcional y procedimientos generales); la última sección detalla las conclusiones arribadas.

ANTECEDENTES DEL LABORATORIO DE FORENSIA DIGITAL

La Facultad de Ingeniería de la UCASAL cuenta con un Laboratorio Forense Digital denominado **DigiLab**, el cual fue creado en el año 2016. Se planteó como un espacio destinado a los "*Desarrollos de innovación que logren mejorar la sociedad mediante la transmisión y la aplicación de los conocimientos provenientes de la investigación, en el campo de las Tecnologías de la Información y las Comunicaciones*".

Si bien en su momento surgió como un lugar para el desarrollo de la transferencia de conocimientos a partir de los proyectos de I+D que se trabajan en esa unidad académica de la UCASAL, luego fue tomando forma para constituirse en un área específica para las actividades del Grupo de Investigación de Forensia Digital de la Facultad de Ingeniería de la UCASAL.

Allí se desarrollaron los sucesivos proyectos de investigación encarados en el período 2016-2019, entre los que se pueden mencionar:

- "Aplicación de Metodologías, Procesos y Técnicas Forenses Digitales en Nuevas Tecnologías" aprobado por RR N° 987/15.
- "Aplicación de Tecnologías semánticas a la forensia digital etapa 1" - estudio y diseño de una ontología semántica aprobado por RR Nº 656/15.
- "Aplicación de metodologías, procesos y técnicas forenses digitales en nuevas tecnologías" aprobado por RR Nº 1.603/17.
- "Aplicación de tecnologías semántica a la forensia digital de Internet de las Cosas (IoT)" aprobado por RR N° 1582/17

A los que se suman los actuales proyectos en curso:

- “Desarrollo de un laboratorio de forensia de internet de las cosas” aprobado por RR Nº 324/2020
- “Aplicación de tecnologías semánticas a la Seguridad de la Información: Estudio y Diseño de una Ontología para un modelo de seguridad de la Factura Electrónica” aprobado por RR 362/2020.
- “Estudio e Implementación de requerimientos de calidad en un Laboratorio de Forensia Digital” aprobado por RR Nº 325/2020.

Otro antecedente de interés que se debe considerar es el trabajo denominado “Proyecto de Creación de un Laboratorio de Forensia de IoT” (Rivetti, Gamarra, & Gallo, 2020) formulado por el Grupo de Forensia Digital de la UCASAL, en el que se establecen los componentes mínimos de un Laboratorio de Forensia de IoT considerando la infraestructura tecnológica en seis áreas: software, hardware, estructura de datos, comunicaciones, interacción con el usuario y seguridad informática. En dicho trabajo se identificaron las etapas principales de un proyecto de esta envergadura, considerando el proceso completo, desde la planificación estratégica, la formulación del proyecto, su implementación y evaluación de funcionamiento.

MARCO TEÓRICO

Desde el Grupo de Investigación en Forensia Digital de la UCASAL se propone la optimización del laboratorio DigiLab totalmente acoplado a la impronta y la normativa existente en la sociedad en donde cumpliría sus funciones; abierto no solo a la provincia de Salta sino con pretensión de proyectarse al resto de nuestro país. Un laboratorio que, desde la complejidad del análisis proyectado, cuente con las mejores y más modernas herramientas y vaya actualizándose constantemente, como lo requiere el objeto de sus pericias.

Desde ese punto de vista será fundamental la actuación del personal del laboratorio desde los primeros momentos de actuación, cumpliendo y exigiendo el cumplimiento de los protocolos existentes, tales como la “Guía de obtención, preservación y tratamiento de evidencia digital”[1] , el “Protocolo General de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos”[2] , así como las distintas normas y protocolos existentes en los ámbitos provinciales al

[1] Aprobada por Resolución PGN Nª 756/16, de fecha 31 de marzo de 2016, y que puede ser consultada en el sitio http://www.mpf.gob.ar/resoluciones/PGN/2016/PGN-0756-2016-001.pdf [Consultada el 02/09/2020]

[2] Aprobado por Resolución del Ministerio de Seguridad de la Nación N° 234/2016, y cuyo texto completo puede ser consultado en http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm [Consultada el 02/09/2020]

respecto[3], por citar solo algunos ejemplos; así como impulsando, desde la propia experiencia, la generación de nuevos protocolos de actuación, en este trabajo conjunto que se pretende con las fuerzas de seguridad, con la justicia, con los colegios profesionales incumbentes y con los demás actores del sistema judicial.

Como bien sostienen (Roatta, Casco, & Fogliato, 2012) en su trabajo interdisciplinario sobre tratamiento de la evidencia digital y normas ISO/IEC 27037:2012, enmarcado en dos proyectos radicados en diferentes unidades académicas: Análisis Digital Forense, Conceptos y aplicaciones (proyecto acreditado en la Facultad de Ingeniería de la Universidad Nacional de Rosario - Argentina) e Informática Forense con herramientas de software libre (proyecto acreditado en la Facultad de Tecnología Informática de la Universidad Abierta Interamericana - Argentina): "*La evidencia digital bien procesada puede aprovecharse al máximo en distintos escenarios. En cada uno de ellos existe una orientación diferente respecto de lo que se pretende obtener: calidad probatoria, precisión en el análisis, restauración del servicio y/o el costo de la recolección de la evidencia. Los componentes clave que proporcionan credibilidad en la investigación son la metodología aplicada durante el proceso y la calificación de los individuos que intervienen en el desarrollo de las tareas especificadas en la metodología*".

Otros trabajos relacionados al estudio de la ISO/IEC 27037:2012, la norma que propone recomendaciones para el tratamiento de la evidencia digital también son de interés. En ese sentido, se toma en cuenta los aportes de (Sudyana, 2019) respecto de la evaluación de distintos marcos de trabajo en los cuales se aplicó esta norma. Por su parte, (Ajijola, Zavarsky, & Ruhl, 2014) realizó una interesante investigación entre la norma ISO/IEC: 27037:2012 y las Forensics Guidelines de NIS T SP 800-101 Rev. 1:2014 destacando coincidencias y diferencias que son de utilidad incluir en el análisis de los procedimientos a fijar para el DigiLab. El trabajo de (Veber & Smutny, 2015) describe las experiencias de aplicación de la norma ISO 27037:2012 en la República Checa, enfocándose principalmente en las actividades de identificación, recolección, adquisición y preservación de la evidencia digital que propone la norma citada.

Asimismo, como material de consulta vinculado a la temática contamos con muy buenas publicaciones como la del National Institute of Standars and Technology (NIST)[4], dependiente del U.S. Departament of Commerce, con recursos para directores de laboratorio, diseñadores, consultores y otras partes interesadas involucradas en la construcción o renovación de laboratorios de ciencias forenses y que cuentan con información trascendental y actualizada para este tipo de organizaciones.

---

[3] Se pueden encontrar en http://www.fiscalespenalesalta.gob.ar/instrucciones-y-recomendaciones/ [Consultada el 02/09/2020]

[4] https://www.nist.gov/publications/forensic-science-laboratories-handbook-facility-planning-design-construction-and

Una temática particular que debe estudiarse con cuidado en lo relativo a la *evidencia digital.* En tal sentido, el Grupo de Forensia Digital se encuentra en el estudio de investigaciones como las de (Anderson Coronel-Rojas, Areniz-Arévalo, Cuesta-Quintero, & Rico-Bautista, 2020) que analiza distintas metodologías para la adquisición de evidencia digital; el trabajo de (Buitrago Medrano, 2019) realiza un estudio exhaustivo acerca de la evidencia digital en casos de delitos financieros; (Puga Rodríguez, 2019) aborda la evidencia digital en casos de pornografía infantil; el trabajo de (Parra Sichaca, 2018) describe los requisitos que la justicia de Colombia requiere para reconocer la validez de la prueba digital; entre otros trabajos que permitirán formular los procedimientos metodológicos y formales necesarios para el procesamiento de la evidencia digital.

Por otra parte existen muy buenas experiencias a nivel internacional de este tipo de laboratorios, tales como la de AKIRUTEK Peritos Informáticos[5], un laboratorio ubicado en Bilbao (España), que ofrece, además de la informática forense, servicios de ciberseguridad, la empresa DURIVA[6], con sedes en México, Chile, Colombia y Argentina, con especial dedicación al peritaje informático y la localización y extracción de evidencia digital o DragonJAR Soluciones y Seguridad Informática S.A.S.[7], una empresa enfocada a prestar servicios de Seguridad Informática y Análisis Forense Digital para Colombia y Latinoamérica.

De especial interés es la propuesta de la Universidad FASTA y el Ministerio Público de la Provincia de Buenos Aires, sobre "Aspectos Estratégicos, Organizaciones y de Infraestructura en el Diseño de Laboratorios Judiciales de Informática Forense" (Di Iorio et al., 2017), del cual particularmente se toma en consideración los siguientes elementos: Aspectos Estratégicos e Institucionales, Aspectos Edilicios y Estructurales y Aspectos Tecnológicos.

PROPUESTA DE DEFINICIÓN DE LA ESTRUCTURA ORGANIZATIVA DEL LABORATORIO DE FORENSIA DIGITAL

El plan propuesto por (Rivetti et al., 2020) para el desarrollo de un Laboratorio de Forensia de IoT puede utilizarse como base para abordar un proceso de optimización y mejora del DigiLab, considerando las 4 etapas planteadas: a) Definición de la Misión y la Visión del Centro de Servicios de Informática Forense; b) Análisis del Contexto Externo e Interno; c) Formulación de Estrategias y d) Plan de acción.

Las dos primeras etapas señaladas se cumplieron, dando pie a un documento interno de

[5] Se pueden ver detalles en https://akirutek.com/laboratorio-informatico-forense/ [Consultada el 02/09/2020]

[6] Se pueden ver detalles en https://duriva.com/ [Consultada el 02/09/2020]

[7] Se pueden ver detalles en https://www.dragonjar.org/quienes-somos [Consultada el 02/09/2020]

reformulación de la identidad del DigiLab en términos de dos objetivos fundamentales: asistencia técnica a terceros y apoyo a la formación experimental en Forensia Digital.

A la fecha, se está avanzando en la tercera etapa, referida a la Formulación de Estrategias, en la que específicamente se propone trabajar sobre 5 aspectos:

- Creación de la estructura organizativa que conformará el Centro de Servicios de Informática Forense.
- Generación de acciones de capacitación a fin de preparar al personal que integrará el centro.
- Definición y adquisición de la infraestructura tecnológica para el Laboratorio de Informática Forense
- Desarrollo de procedimientos técnico-legales para el análisis forenses
- Plan de Crecimiento

El presente trabajo aborda el detalle de uno de esos aspectos: la ESTRUCTURA ORGANIZATIVA del DigiLab.

a) Dependencia Organizativa

DigiLab funciona bajo la dependencia directa del Instituto de Estudios e Investigaciones Interdisciplinarias en Ingeniería (IEsIIng), que a su vez depende orgánicamente de la Facultad de Ingeniería de la UCASAL, como entidad abocada al desarrollo de la I+D en temáticas propias de esa unidad académica. Así lo establece la Resolución Rectoral N° 864/16 de creación del DigiLab.

Si bien el DigiLab se ubica físicamente en el Edificio de Laboratorios de la Facultad de Ingeniería de la UCASAL, en Salta (Argentina), está preparado para interactuar de modo virtual con otras instituciones, agentes o requirentes externos si fuera necesario.

b) Objetivos Generales

- Investigar las tecnologías, metodologías y herramientas utilizadas en los procesos Forenses digitales y estudiar la factibilidad de su aplicación.
- Ofrecer al sector público y privado los servicios que a través de los recursos propios o la contratación de terceros se puedan llevar a cabo.
- Producir propuestas técnicas y académicas tendientes a reformar o reformular el tratamiento normativo y legal de la evidencia digital en los ámbitos periciales y empresariales.
- Facilitar y gestionar la integración de los alumnos pertenecientes a los últimos años de las carreras de la Ingeniería en los proyectos de investigación y transferencia con

impacto a organizaciones a nivel Nacional e Internacional.

- Apoyar la educación y capacitación en las tecnologías de la comunicación e información en el ámbito de la UCASAL, la Provincia de Salta y de la Región mediante la invitación de expertos de prestigio provincial, nacional e internacional, que dicten seminarios y cursos vinculados al objeto del DigiLab.
- Generar precedentes a fin de la creación de centros conexos similares tendientes a la investigación, capacitación y concientización sobre los riesgos asociados a las nuevas tecnologías emergentes.

c) Cobertura y Alcance de sus acciones:

DigiLab cuenta con tres ámbitos de acción perfectamente identificadas:

- Investigación y Docencia: en la que intervienen el cuerpo de investigadores, docentes y alumnos de la Facultad de Ingeniería, a través de los Proyectos de Investigación, de Desarrollo Tecnológico y/o de Transferencia de Conocimientos que se formulen y en los que tenga competencia la Forensia Digital. En este sentido, es dable considerar la inclusión de docentes, investigadores y alumnos de otras carreras (como Derecho o Psicología), siempre en el marco de trabajos interdisciplinarios que pudieran surgir.
- Asistencia Técnica a Terceros: en la que a solicitud de requirentes externos a la UCASAL (organismos judiciales provinciales, nacionales, profesionales del área de la criminalística, derecho y seguridad informática) se desarrollan tareas de asesoramiento y/o asistencia técnica específica en temáticas de Forensia Digital. Como ejemplo puede citarse los siguientes:
    - Asistencia Técnica en la formulación de una Propuesta de Auditoría Informática del Sistema de Voto Electrónico para el Tribunal Electoral de la Provincia de Salta (2017).
    - ObE Forensics, una aplicación informática para el análisis forense de correos electrónicos, que actualmente se encuentra en fase de prueba y experimentación.
- Capacitación Técnica Especializada en Forensia Digital: en la que se mantiene una línea ininterrumpida de acciones tendientes a la formación de recursos humanos componentes para la recolección y análisis de la evidencia digital. Se puede mencionar:
    - Curso de Forensia Digital: curso de 40 hs que se impartió en 6 oportunidades, durante el período 2013 a 2020, y permitió la capacitación de cerca de 150 asistentes.
    - Curso de Análisis Forense de Correos Electrónicos: curso de 20 hs que se

impartió en 2 oportunidades, durante el período 2018-2019, y permitió la capacitación de cerca de 35 personas.

d) Recursos financieros y presupuestarios para el funcionamiento:

DigiLab cuenta con recursos financieros suficientes para su funcionamiento que provienen de tres fuentes diferentes:

- El tesoro institucional de la UCASAL, al ser DigiLab un recurso tecnológico gerenciado por la Facultad de Ingeniería.
- Los ingresos provenientes de las acciones de capacitación técnica.
- Los aportes de terceros que requieren de los servicios ofrecidos.

e) Organización Funcional y Física:

El DigiLab es gerenciado por la figura de un Coordinador, quien responde a las directivas y funciones que le caben a quienes cubren el rol de coordinación de laboratorios en el ámbito de la Facultad de Ingeniería de la UCASAL, y además, particularmente se agrega las siguientes responsabilidades:

- Asistir al equipo de investigadores forenses que trabajan en el DigiLab.
- Asesora a los organismos judiciales y/o requirentes de los servicios forenses acerca de la presentación de las muestras, procesos de recolección, extracción y análisis forense.
- Instrumenta con los organismos judiciales y/requirentes sobre todos los aspectos necesarios de la Cadena de Custodia de la muestra de evidencia digital a procesar.
- Proponer y aportar profesionales de diversas disciplinas para que oficien como consultores del DigiLab en los análisis forenses que así lo requieran.
- Promover la incorporación de las innovaciones tecnológicas necesarias que permitan un desempeño de vanguardia del DigiLab.

En función de la demanda, podrán crearse otros roles destinados a tareas que requieren cierta experticia como el conocimiento de una herramienta forense puntual o la implementación de técnicas forenses de cierta particularidad.

Respecto de la organización física, se prevén los espacios suficientes para:

- Zona de Laboratorio: en donde estarán ubicados los equipos destinados a la recolección y análisis forense de las evidencias digitales.
- Zona de Recepción y Registro de Elementos y Muestras: referidas a las evidencias digitales para analizar.
- Zona de Administración y Archivo de Informes: para el registro regular de las

actividades, así como la documentación técnica resultantes de las actividades desarrolladas.

Cada zona deberá cumplir con los requisitos exigidos por la normativa vigente en cuanto a medidas, ventilación, iluminación, privacidad, y salubridad laboral. Y tendrá los equipos necesarios para el desempeño de las tareas, conservación de las muestras, y gestión de residuos. En la zona destinada a la Recepción y Registros de Elementos y Muestras es de vital importancia el cumplimiento de la Cadena de Custodia.

f) Procedimientos de Trabajo:

Considerando las 3 funciones principales del DigiLab, se proponen para cada una un procedimiento básico de desarrollo de actividades.

f.1) Investigación y Docencia:

Al respecto, todas las acciones relacionadas con esta área deben responder a lo dispuesto en los reglamentos instituciones, ya sea emanados del Consejo de Investigaciones de la UCASAL, como de la Coordinación General de Laboratorios de la Facultad de Ingeniería. En ambos casos, hay normativa referida a la utilización de los espacios físicos, equipos y recursos disponibles tanto para la investigación como para la docencia, los cuales se organizan e implementan en función de una agenda de horarios, para permitir el acceso a cada ámbito correspondiente, según sea el rol y actividad de los requirentes.

f.2) Asistencia Técnica a Terceros:

En este caso, y considerando particularmente las actividades relacionadas a la recolección y análisis forense, se deben tener presente estas pautas:

- Recepción de las muestras y elementos a periciar: La recogida, preparación y envío de los objetos, vestigios, sustancias, muestras o piezas que hayan de ser analizados se adecuarán a los protocolos y las especificaciones técnicas de gestión de muestras establecidas para el tratamiento de la evidencia digital.
- El transporte de las muestras desde el lugar de su obtención hasta el servicio encargado de su análisis se efectuará a través de los medios adecuados de transporte para mantener intactas las características de las muestras y la cadena de custodia.
- Es de vital importancia que al momento de la recepción de la muestra se debe verificar la integridad de la "cadena de custodia" desde la toma de la muestra hasta el momento de recepción en el Servicio de Laboratorio Forense.
- La integridad de la cadena de custodia se acreditará mediante el procedimiento adoptado al efecto, el cual debe contar con la aprobación institucional de la Facultad

de Ingeniería de la UCASAL[8].

- Los objetos, vestigios, evidencias, sustancias, muestras o piezas que deban ser estudiados se remitirán al DigiLab acompañados de información relativa:
    - Órgano o Autoridad judicial solicitante, mediante correspondiente oficio; o requerimiento formal por escrito si el solicitante fuera un particular.
    - Formulario de envío de muestras en el cual ha de constar la investigación solicitada, antecedentes y datos de interés sobre el caso, datos de la víctima y según tipo de caso del sospechoso.
    - Identificación de las muestras con un, listado de las muestras enviadas, n.º de referencia, etc.
    - Cadena de Custodia con el nombre o identificación de la persona responsable de la recogida de la muestra, fecha y hora de recogida y condiciones de almacenaje de la muestra hasta su envío al laboratorio.
    - Se facilitará por parte del Laboratorio Forense, que canalizarán las peticiones y envíos, los modelos y formularios necesarios para la adecuada gestión de las solicitudes.
- DigiLab garantizará, mediante los procedimientos y apoyos técnicos necesarios, la integridad de la cadena de custodia de las muestras remitidas, su adecuada gestión y su mantenimiento de acuerdo con las posibilidades técnicas y las necesidades procesales, así como las físicas de almacenamiento.
- Todas las acciones de procesamiento de la evidencia digital (preparar muestras, clasificarlas, realizar el análisis, interpretación estadística, muestreo de resultados, técnicas de detección de indicios, etc.) deberán ajustarse al cumplimiento de la Cadena de Custodia.
- Elaborar informes técnicos y dictámenes ajustados al formato correspondiente (judicial y/o técnico), con ajuste a las siguientes consideraciones:
    - Membrete Oficial del DigiLab e identificación formal del Caso.
    - Órgano (Judicial u otros) solicitante y procedimiento.
    - Registro de la fecha y hora de entrada de las muestras y de emisión del informe de resultados. Descripción de la muestra/s remitida/s y su estado.
    - Garantía de la cadena de custodia.
    - Trascripción del estudio solicitado, con indicación de las metodologías, técnicas y

[8] A la fecha el Procedimiento de la Cadena de Custodia así como los formularios involucrados se encuentra en fase de análisis por parte de la Facultad de Ingeniería

herramientas utilizadas.

  - Resultados obtenidos, en versión reducida (aspectos más destacables relativos al análisis solicitado) y en versión completa (aspectos técnicos que permitan la replicación del análisis).
  - Consideraciones técnico legales que sean necesarias.
  - Los informes serán firmados por quienes los hayan realizado y validados por la firma del Coordinador del DigiLab.

- Cuando no fuera posible realizar un análisis forense por ausencia de medios técnicos o humanos, previamente a cualquier derivación de las evidencias, el Coordinador del Laboratorio deberá comunicarlo a la autoridad solicitante, así como las alternativas posibles para el cumplimiento de lo solicitado.
- El personal del DigiLab está obligado a comunicar a la autoridad judicial o al requirente, a través del Coordinador de Laboratorio, las limitaciones parciales o absolutas para la práctica de lo solicitado por razón de la alteración de la cadena de custodia, alteración de las muestras, defectos de conservación o cualquier otra causa.
- Secreto profesional, acuerdos de confidencialidad: Los Técnicos Especialistas y demás personal del DigiLab están obligados a guardar secreto de las actuaciones en que intervengan, o de las que tengan conocimiento con motivo de su actividad laboral. A tal fin se firmará un convenio de confidencialidad cuya duración será por todo el tiempo durante el cual se encuentre trabajando en el laboratorio, y luego de finalizada su tarea durante los cinco años siguientes.

f.3) Capacitación Técnica:

Las acciones referidas al desarrollo de capacitaciones técnicas y profesionales, ya sea en carácter de cursos de posgrado y de cursos de extensión al ámbito técnico, se desarrollarán en plena concordancia con las normativas que en tal sentido están vigentes en la UCASAL desde la Secretaría de Extensión Universitaria y la Dirección de Formación Contínua.

Estas actividades se desarrollarán con los equipamientos y recursos tecnológicos disponibles en el DigiLab y/o en otros laboratorios informáticos de la Facultad de Ingeniería, así como mediante la utilización de los EVA(Espacios Virtuales de Aprendizaje) disponibles desde el Sistema de Educación a Distancia de la UCASAL.

CONCLUSIONES

Si bien lo dicho hasta ahora forma parte de la propuesta que a la fecha se encuentra en

implementación en el DigiLab, ya se han observado cuestiones que necesitan una revisión y/o incorporación de aspectos que inicialmente no se habían planteado, como por ejemplo:

- El DigiLab puede crecer en función de los recursos forenses que se vayan incorporando. Si bien desde el contexto del software libre existen muchas y variadas herramientas forenses, particularmente en el caso de las herramientas propietarias hay un costo importante que deberá considerarse con cuidado, y ello está vinculado a las estrategias de financiamiento externo que puedan lograrse para este laboratorio.
- El proyecto denominado "Estudio e Implementación de requerimientos de calidad en un Laboratorio de Forensia Digital" aprobado por RR Nº 325/2020, generará importantes insumos para la optimización del DigiLab en términos de generar un espacio adecuado en asepsia y resguardo de datos para el tratamiento de la evidencia digital. Se espera que como resultado de este proyecto, DigiLab inicie la certificación de normas de calidad ISO/IEC 9001:2015, ISO/IEC 27001:2015 y a futuro, la norma ISO/IEC 27037:2012.
- Resulta necesario formalizar el funcionamiento del DigiLab en un Reglamento Interno, que se ajuste además a las normativas que en tal sentido ya cuenta la Facultad de Ingeniería para sus ámbitos de formación práctica.
- Al estar radicado en una institución universitaria, se debe aprovechar intensamente el desarrollo de la Investigación y la Docencia en el DigiLab. Todo lo cual trae aparejado ventajas indiscutidas desde el punto de vista del crecimiento del proyecto, pero también surgen aspectos que deberán cuidarse especialmente –como el acceso de alumnos y docentes- a espacios en donde se estén realizando tareas de análisis forense de evidencia digital real.
- Es importante incorporar a DigiLab en la línea de Gestión Transparente, poniendo a disposición de la comunidad los recursos humanos, económicos, físicos e informáticos disponibles en DigiLab, así como los servicios y acciones realidas, con detalle de la información sobre la asignación de los mismos, fechas, montos, cantidades, y plazos; sin salirse del marco de reserva y privacidad de los datos cuando así corresponda.

BIBLIOGRAFIA

Ajijola, A., Zavarsky, P., & Ruhl, R. (2014). A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012. *2014 World Congress on Internet Security, WorldCIS 2014*, 66–73. https://doi.org/10.1109/WorldCIS.2014.7028169

Anderson Coronel-Rojas, L., Areniz-Arévalo, Y., Cuesta-Quintero, F., & Rico-Bautista, D.

(2020). Definición de una metodología de adquisición de evidencias digitales basada en estándares internacionales, (April).

Buitrago Medrano, D. (2019). *La Recolección Y Custodia De Las Evidencias Digitales Del Auditor Forense En Entidades Financieras*. *Doctoral dissertation, Universidad Mayor de San Andres. Facultad Ciencias Económicas*. https://doi.org/.1037//0033-2909.I26.1.78

Di Iorio, A. H., Constanzo, B., Vega, P., Lamperti, S., Giaccaglia, M. F., & Cistoldi, P. (2017). Aspectos Estratégicos , Organizacionales y de Infraestructura en el Diseño de Laboratorios Judiciales de Informática Forense Strategic , Organizational and Infrastructure Aspects in the Design of Judicial Digital Forensics Laboratories, 1–10.

Parra Sichaca, P. D. (2018). Requisitos jurídicos para la validez jurídica de la prueba digital. *Universidad Católica de Colombia*.

Puga Rodríguez, R. D. (2019). *La evidencia digital en los delitos de pornografía infantil*. *Master's thesis, Quito: UCE*. https://doi.org/.1037//0033-2909.I26.1.78

Rivetti, E., Gamarra, A., & Gallo, H. B. P. De. (2020). Proyecto de Creación de un Laboratorio de Forensia de IoT. *REDI - Revista Digital Del Departamento de Ingeniería e Investigaciones Tecnológicas UNLAM (In Press)*.

Roatta, S., Casco, M. E., & Fogliato, M. (2012). El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012, *1*, 1–7. Retrieved from http://sedici.unlp.edu.ar/bitstream/handle/10915/50586/Documento_completo.pdf-PDFA.pdf?sequence=1

Sudyana, D. (2019). Analysis and Evaluation Digital Forensic Investigation Framework Using Iso 27037:2012. *International Journal of Cyber-Security and Digital Forensics*, *8*(1), 1–14. https://doi.org/10.17781/p002464

Veber, J., & Smutny, Z. (2015). Standard ISO 27037:2012 and collection of digital evidence: Experience in the Czech Republic. *European Conference on Information Warfare and Security, ECCWS*, *2015-January*(January 2016), 294–299.