Lineamientos para la creación de laboratorios informáticos forenses

Gastón Semprini, Poder Judicial de Río Negro. Licenciado en Sistemas de Información por la Univ. de Belgrano y Experto en informática forense por la Univ. Tecnológica Nacional.

Jefe del área de informática forense del Poder Judicial de Río Negro.

gsemprini@jusrionegro.gov.ar

Abstract.: Para la creación de un laboratorio pericial informático es necesario tener en cuenta ciertos elementos, a saber: servicios periciales proporcionados, protocolos de trabajo, normas estándares y guías de buenas prácticas forenses, profesionales capacitados, manuales operativos, procedimientos operativos estandarizados, sistemas de gestión. Todo ello con el objeto de llevar adelante los distintos servicios periciales con la excelencia y calidad que ésta especialidad requiere. En este trabajo se desarrolla una guía tentativa de cómo llevarlo adelante.

Keywords: Laboratorio Pericial Informático, Normas Estándares, Protocolo Interno, Lineamientos de Trabajo.

1 Introducción

En el transcurso de los últimos años la rama de la ciencias forenses y en especial la informática forense, la cual es una es una especialidad de las ciencias informáticas ha tomado gran trascendencia, de tal magnitud, que organismos de Gobierno y Poder Judicial nacional y provincial han tomado la iniciativa de implementar áreas específicas relacionadas a esta especialidad, con el objetivo de dar respuesta a distintos ilícitos que tengan asociados dispositivos tecnológicos.

El objetivo de este trabajo es brindar ciertos elementos a tener en cuenta, que permitan poder fortalecer las áreas periciales destinadas a la informática forense, entre ellas los lineamientos específicos que sirvan de soporte a la hora de implementar un Laboratorio Pericial Informático Forense. Para ellos comenzaremos brindando algunas definiciones abordadas por distintos autores que estudian esta disciplina.

A) Esta rama científica es definida como una disciplina de las ciencias forenses que, considerando las tareas propias asociadas con la eviden-

cia, procura describir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso, como así también entendiendo los elementos propios de las tecnologías de los equipos de computación para así ofrecer un análisis de la información residente en dichos equipos [Cano, 2009]

B) La información que se encuentra en los dispositivos tecnológicos se la denomina evidencia digital. De acuerdo con el HB:171 2003 "Guidelines for Managment of IT Evidence" evidencia digital es cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" o "también es considerada evidencia digital a cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal" [1].

C) El informático forense es "la persona que permitirá avanzar en la búsqueda de la verdad, en el análisis de la información residente en los dispositivos tecnológicos y realizar una reconstrucción de los hechos en base a la evidencia digital analizada" [1].

D) A su vez ampliando su espectro, la informática Forense según fue definida en el primer DFRWA celebrado por un grupo de expertos en el año 2001, consiste en el ejemplo de métodos científicos comprobables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar la evidencia digitales procedentes de fuentes digitales con el propósito de hacer posible la construcción de hechos considerados delictivos o ayudar a la prevención de actos no autorizados y capaces de provocar una alteración en operaciones planificadas de organismos y empresas. [2]

E) Se entiende además por informática forense al conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática. Tomando como "prueba indiciaria", desde la criminalística, al conjunto de huellas de cualquier tipo y naturaleza, que se hayan producido como resultado de una acción cualquiera y que al ser metodológicamente investigados, permiten reconstruir los hechos acaecidos. En General, pero no de manera excluyente, se relacionan con actos delictivos. [3]

F) La "informática forense" es a la informática lo que la medicina legal es a la medicina. Como toda disciplina forense tiene sus particulari-

dades que justifican su diferenciación, tomando parte de la informática en general y de la seguridad informática en lo particular. [3]

Sin importar cual fuera la definición que cada uno adopte, es importante dejar en claro que la informática forense es una disciplina científica.

2 Modelo de trabajo en un laboratorio pericial informático

Todo laboratorio pericial informático debe contar con un modelo de trabajo que permita establecer los lineamientos diarios de todos los integrantes del área. Para ello se sugiere llevar adelante el modelo presentado por Gómez [Gómez, 2013], en donde se especifica que en las unidades periciales forenses tiene que haber un cambio de paradigma centrado en un nivel de maduración que permitirá dar un mejor servicio a largo plazo. Planteando para ello 6 factores que deberán tenerse en cuenta:

1) Alineamientos a la especialidad: se tendrá en cuenta los principios de la misma, buenas prácticas, protocolos, procedimientos operativos estandarizados (SOPs) y manuales de operaciones.
2) Sistematización del Proceso Forense: evaluar las herramientas, técnicas forenses implementadas, metodologías utilizadas, testing de herramienta y manuales de calidad.
3) Separación de roles profesionales: se tomara en consideración las misiones y funciones de los profesionales que integran el área, responsables o peritos, asistentes técnicos, asistentes de peritos, responsables de calidad y el director.
4) Desarrollo de competencias: se especificarán el uso de herramientas, informes técnicos, dictámenes o informes periciales, investigación y desarrollo y lineamientos de servicio.
5) Distribución de la jornada laboral: tomar en cuenta las actividades operativas, elaboración de informes, capacitaciones, producción científica y control de calidad
6) Gestión de conocimiento: considerar la cooperación entre pares, implementación del Laboratorio, cooperación académica y acreditaciones.

Fig. 1. Modelo de calidad del servicio pericial

3 Metodología forense

Todo laboratorio pericial informático debe contar con una metodología de trabajo para el tratamiento de la de la evidencia digital que se encuentre bajo investigación. Si bien esta es una ciencia medianamente nueva, no existe un método único y aceptable, por lo cual algunos autores especifican distintos modelos a tener en cuenta.

4.1 Modelo Publicado por el Departamento de Justica de los Estados Unidos en el 2001 es el utilizado e incorporado en el protocolo del Departamento de informática forense del Poder Judicial [5] [6]

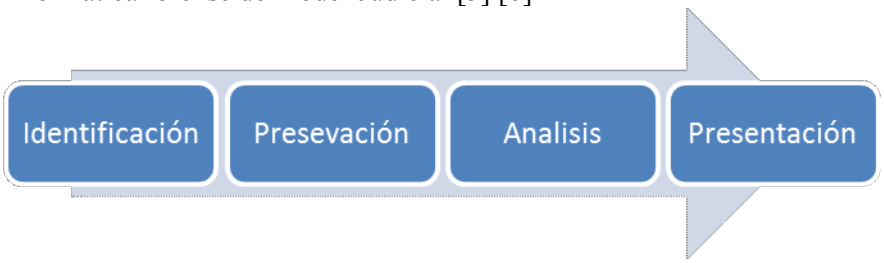

Fig. 2. Ciclo de vida de la evidencia

4.2 Modelo del DFRWS (2001) [7] Este modelo no fue tomado como un modelo final, sino fue propuesto para ser tomado para ser considerado en un modelo a futuro. Este proceso si bien es planteado como un proceso lineal de 7 pasos, el mismo puede ser de readecuado de acuerdo a la sircunstancia del caso. Estos pasos son (1. La Identificación, 2. La Preservación, 3. La Colección, 4. El Examen, 5. El Análisis, 6. La Presentación, 7. La Decisión)

4.3 Modelo Braian Carrier y Eugene Spafford [8], donde proponen un modelo con cinco fases. Cada una de esas fases posee distintos pasos a tener en cuenta. [8]. (1. Fase de Preparación, 2. Fase de Despliegue, 3. Fase de Investigación Fisica de la escena del crimen, 4. Fase de investigación de la Escena Digital del Delito, 5. Fase de Revisión)

En base al prenotado modelo, Venansius Baryamureeba y Florence Tushabe en el 2004 propusieron un modelo similar, con el objetivo de mejorar algunos aspectos. [7]

4.4 Modelo Extendido de Séamus ó Ciardhuáin presentado en el año 2004 dividió el modelo en 13 etapas las cuales se especifican de forma de cascada. A saber [7] (1. La conciencia; 2. Autorización, 3. Planificación, 4. La notificación, 5. Buscar e identificar la prueba, 6. La colección de la prueba, 7. Transporte de la prueba, 8. El almacenamiento de la prueba, 9. El examen de la prueba, 10. La hipótesis, 11. La presentación de la hipótesis, 12. La prueba / defensa de hipótesis, 13. La diseminación de información)

4.5 Modelo de Casey 2004 el cual es una evolución de su primer modelo del 2001 y es otro de los utilizados por el área de informática forense del Poder Judicial de Rio Negro. Está compuesto por 6 etapas, contemplándose en algunas de ellas el sistema de cadena de custodia, que es la etapa del proceso de investigación previa a la extracción y análisis de la evidencia digital [9]. (1. Autorización y preparación, 2. Identificación, 3. Documentación, adquisición y conservación, 4. Extracción de información y análisis, 5. Reconstrucción, 6. Publicación)

Es importante tener presente como mínimo cumplir con las etapas básicas mostradas en la figura 2, como así también reagrupar con algún otro sistema, generando su propio modelo metodológicos para su laboratorio pericial informático.

Normas estándares, guías de buenas prácticas y bibliografía académica desarrollada por autores que estudian la ciencia.

En una especialidad científica como lo es la informática forense, es importante que un laboratorio pericial informático realice su trabajo mediante normas estándares, procedimientos de buenas prácticas desarrollados por entidades de gobierno y autores reconocidos.

Algunas de las principales normas, guías de buenas prácticas a tener en cuenta:

La norma IRAM 301 ISO/IEC 17025 establece los requisitos generales para la competencia en la realización de ensayos o de calibraciones, incluido el muestreo. Cubre los ensayos y las calibraciones que se realizan utilizando métodos normalizados, métodos no normalizados y métodos desarrollados por el propio laboratorio. Como así también es utilizada por los laboratorios cuando se desarrolla sistemas de gestión para sus actividades de calidad. Algunos aspectos que la norma especifican:

3.1 Requisitos relativos a la gestión:

1. Aspectos relacionados con lo que el "laboratorio debe tener y hacer" como ser: misiones y funciones del personal para cada tarea; contar con un Sistema de Gestión; control de todos los documentos que formen parte del laboratorio; revisión de los pedidos, ofertas y contratos que se deban realizar en el laboratorio; subcontratación de ensayos y de calibrado; compras de servicios y de suministros; servicios al cliente; quejas; mejoras; acciones correctivas; acciones preventivas; control de los registros donde se establecen los procedimientos de identificación, recolección, codificaciones, acceso, archivo, almacenamiento, mantenimiento de los registros de la calidad y técnicos; instituir auditorías internas

3.2 Requisitos técnicos:

1. Aspectos relacionados a todos los factores que se deben tener en cuenta a la hora de determinar la exactitud y la confiabilidad de los ensayos o de las calibraciones realizados en un laboratorio como ser: factor humanos; instalaciones y condiciones ambientales; validación de los métodos utilizados; equipos utilizados; mediciones realizadas; muestreos; informe de los resultados y aseguramiento de la calidad de los resultados.

La ISO/IEC 27037 provee una guía para los procesos específicos relacionados con el manejo de evidencia digital. Estos procesos son la Identificación, recolección, adquisición, preservación de datos, fundamentales para mantener

la integridad y autenticidad de la evidencia digital en un proceso judicial. Algunos aspectos de la norma:

1. Términos y Definiciones: diferentes de identificación, recolección, adquisición, preservación, dispositivos digital, evidencia digital, DEFR y DES (misiones y funciones de personal capacitados), confiabilidad, respetabilidad, reproducibilidad, espacio asignado, copia de evidencia digital, medio de almacenamiento digital, facilidad de preservación de la evidencia, valor hash, imagen, periférico, expoliación, tiempo de sistema, manipulación, timestamp, espacio no asignado, validación, función de verificación, datos volátiles.
2. Requisitos para el manejo de la evidencia digital: procesos para el manejo de la evidencia en las diferentes etapas del ciclo de vida de la evidencia (Identificación, Recolección, Adquisición y Preservación).
3. Componentes claves del ciclo de vida de la evidencia: procedimientos de cadena de custodia, personal con sus respectivos roles y responsabilidades para cada tarea, documentación durante los procedimientos, manejo de dispositivos digitales que pueden contener potencial evidencia digital, prioridades en la recolección y la adquisición, prioridades en la preservación, embalajes y transporte de los dispositivos tecnológicos con posible evidencia digital.
4. Procedimientos de identificación, recolección, adquisición y preservación de computadoras, periféricos y medio de almacenamientos digitales, dispositivos de red, dispositivos de CCTV. Se abordan diferentes factores que puede suceder al momento de tener que realizar la identificación, recolección, adquisición y preservación de todos los dispositivos digitales que almacenan evidencia digital y los diferentes escenarios que se pueden dar. Como por ejemplo si los mismos se encuentran encendidos o apagados.

Otras normas relacionadas a la informática forense son la ISO 27041, 27042, 27043, 27050. Sus objetivos fundamentales son el aseguramiento de las herramientas y procedimientos a tener en cuenta para el análisis forense de la evidencia digital.

Guías de buenas prácticas

Entre las guías de buenas prácticas desarrolladas por diferentes organismos y o instituciones podemos encontrar:

Las guías de buenas prácticas del Departamento de Justicia de los Estados Unidos (NIJ) [7]. La NCJ 199408 APR. 04 desarrollan políticas y procedi-

mientos específicos que para la adquisición preservación, análisis y presentación de la evidencia digital a tener en cuenta en un laboratorio pericial informático. También sugieren la utilización de diferentes planillas en las etapas del ciclo de vida de la evidencia.

Otra guía importante es la NCJ 219941 APR. 08, en la que se describen todos los dispositivos informáticos que pueden contener evidencia digital, procedimientos que se debe tener en cuenta para la recolección de evidencia en el lugar del hecho. Se especifican diferentes tipos de delitos y que evidencia digital hay que tener en cuenta para cada uno de ellos.

Las guías de buenas prácticas de las NIST (National Institute of Standars and Technology) [8] entre ellas la NIST 7387 "Cell Phone Forensic Tools: An Overviwe and Analysis Update escrito por Rick Ayers, Eayne Jansen, Ludovic Moenner, Aurelien Delaitre, que sirven para hacer frente a las distintas investigaciones que estén asociados a dispositivos móviles, proporcionando información sobre herramientas forenses para el análisis forense a dichos dispositivos. Se especifican procedimientos y técnicas de conservación, adquisición, análisis y generación de informes. Características específicas que se deben tener en cuenta a la hora de analizar tanto dispositivos celulares de tipo GSM, como así también los dispositivos móviles inteligente (Smartphone).

Otra de las guías de la NIST a tener en cuenta es la NIST Interagency Report 7559 Forensics Web Services (FWS) desarrolladas por los Anoop Singhal, Murat Gunestas, Duminda Wijesekera el objetivo de la misma es poder brindar información para analizar artefactos relacionados a los servicios web.

Las guías de SWGDE (Scientific Working Group on Digital Evidence) [9] desarrolladas por un grupo de profesionales que hacen investigaciones científicas relacionadas a la evidencia digital. Este grupo ha desarrollado varias guías de buenas prácticas. Cuentan con una específica para el análisis forense de teléfonos celulares denomina "Best Practice for Mobiles Phone Forensics". Otro para computadoras "Best Practices for Computer Forensics Tablet of Contents", otra guía sobre el testeo de hardware y software denominada "Recommended Guidelines for Validation Testing", como así también una guía para el desarrollo de los procedimientos operativos estandarizados denominada "Model Standard Operating Procedures for Computer Forensics"

También podemos nombrar la Guía de Buenas Prácticas de ACPO [10] "ACPO Good Practice Guide for Digital Evidence", en la misma se detallan procedimientos para la identificación, incautación, recuperación y análisis de la evidencia digital que se encuentran almacenada en dispositivos tecnológicos. Posee anexos donde se desarrolla el análisis forense de redes, delitos relacionados con sitios web, foros y blogs.

Otras guía es las RFC 3227 [11] concretada para recolectar y archivar evidencia" (Guidelines for Evidence Collection and Archiving) escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group, allí se hace referencia a las buenas prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar dichos datos.

También se debería tener en cuenta la guía estándar australiana "Guía para el manejo de evidencia en IT" (HB171:2003 Handbook Guidelines for the management of IT evidence) [12]. Si bien esta guía no ésta disponible para su libre distribución, se sugiere ver el artículo desarrollado por Ajoy Ghosh.

Es necesario además contar con un protocolo interno que regule los servicios periciales y la forma de trabajo en el laboratorio. A modo de ejemplo el Poder Judicial de Rio Negro implementó el "Protocolo de actuación y procedimientos internos del área de Informática Forense" el cual fue aprobado por acordada del Superior Tribunal de Justicia [6], sirve de guía para la interacción entre los organismos Jurisdiccionales y del Ministerio Publico con dicha área.

Las áreas Forense deben contar con "Procedimientos Operativos Estandarizados" (SOPs). [9] Los mismos tienen como función guiar una tarea del trabajo, de manera tal, que la misma no solo sea realizada correctamente sino que también conlleven a optimizar tiempos y recursos utilizados. Esto ayudará a obtener mejores resultados, teniendo en cuenta principios científicos y legales para que dichos resultados y conclusiones sean aceptados. Cada uno de estos SOPs deberán ser revisados anualmente y ajustarlos si fuera necesario.

Un procedimiento operativo estándar es un documento que describe las operaciones que se deben realizar, repitiéndose constantemente, llevando a que el procedimiento cuente con una calidad absoluta. El propósito de un SOPs es llevar a cabo las operaciones correctamente y siempre de la misma manera. Estos SOPs deberán estar disponibles en el Laboratorio para poder consultarlos al momento de llevarse a cabo dicha tarea. [13] [14].

Es importante destacar que tanto el protocolo interno que regula los lineamientos del área como la estandarización de los procedimientos son fruto de las normas estándares, guías de buenas prácticas, y bibliografía académica de la especialidad.

4 Conclusiones y sugerencias

El objetivo de este trabajo fue poder brindar los lineamientos a tener en consideración para la creación de laboratorios informáticos forenses. Es importante tener en cuenta que dentro de este concepto tan amplio se deberían

aplicar los conceptos resaltados en el trabajo, como ser la implementación de un modelo de trabajo dentro del laboratorio; un modelo metodológico que establezca los procedimientos científicos de las pericias informáticas realizadas en el laboratorio; implementar un protocolo de trabajo teniendo en cuenta la política institucional del organismo donde se desarrollara dicho laboratorio; desarrollo de procedimientos operativos estandarizados.

Es importante destacar que este trabajo no tiene la finalidad de centrarnos en las herramientas forenses. Si bien es cierto que las mismas son la base esencial del análisis de la evidencia digital en medios informáticos, eso dependerá exclusivamente de la experticia del profesional o perito que las utilice. Es importante hacer énfasis en los aspectos abordados a lo largo de este trabajo, porque en definitiva las herramientas no hacen al perito sino los métodos, técnicas y procedimientos forenses que este utilice.

Algunas sugerencias sobre aspectos abordados a lo largo de esta presentación:

Estructura organizacional y capacitación de los profesionales. La estructura organizacional de un laboratorio pericial informático no fue desarrollada en este trabajo porque creo que ese tema debe ser tratado con un análisis más profundo. Si es importante destacar que la estructura organizacional debe contar con su respectiva dependencia jerárquica, como así también las misiones y funciones de cada persona que integre dicho organigrama.

Es importante tener presente la valoración de los profesionales especializados que integran áreas en esta especialidad. Esta disciplina al ser medianamente nueva la formación como profesionales se realiza dentro del laboratorio, no siendo lo mismo para los médicos legales donde su formación especializada es mediante una residencia en una Institución Educativa Universitaria. Es claro que vamos hacia ese camino, pero como toda nueva especialidad forense, necesita su maduración y contar con Profesionales que la enseñen.

La modalidad de residencia llevada adelante en el área de informática forense del Poder Judicial de Rio Negro es la utilizada por empresas multinacionales como GOOGLE, la llamada “Managing Innovation 80-20”. Donde el 80 porcientos del tiempo es asignado al trabajo diario, y el otro 20 porcientos es utilizado para la lectura de libros y papers académicos no solo de la especialidad forense sino de otra especialidad relacionada. Vale la creación de herramientas forenses útiles para el ámbito de trabajo, generación de trabajos académicos presentados en congresos académicos que permita no solo acentuar los conocimientos adquiridos sino también su implementación en el área.

Lugar físico, es sumamente importante tener en cuenta donde se dará ingreso a la evidencia secuestrada a peritar, se sugiere contar con sistemas de cámara de seguridad. Prever lugar físico para cada etapa del ciclo de vida de la evidencia "identificación, preservación, análisis y presentación como así también sala de secuestro, sala de servidores, sala de reunión. Sistema de seguridad para cada lugar.

Sistema de gestión [15] no solo permitirá brindar de forma inmediata información a las autoridades superiores sino también conocer y saber la salud operativa del área, permitiendo cuantificar tiempos de realización de una pericia en espera (backlog), tiempos de respuesta de los diferentes proveedores (correos electrónicos, redes sociales, proveedores de internet, entidades bancarias, otros) a quienes se solicita información, cantidad del elemento humano que hoy es necesario para abordar eficientemente el cúmulo de trabajo que el área tiene en espera, gigabytes analizados por año, solicitudes realizadas por organismo, por ciudad, entre otros.

Protocolo, procedimientos operativos estandarizados, manuales operativos, que permitirán obtener calidad y excelencia en los trabajos realizados en el laboratorio.

Realizar capacitaciones en las áreas que interactúan con el laboratorio, para ello es importante que la institución de la que formamos parte, entienda la importancia de capacitar a toda persona que utilizara el servicio de laboratorio pericial y así lograr un apoyo institucional para que las mismas concreten la capacitación pertinente.

Protocolo, estandarización y realización de SOPs de todos los procedimientos que se lleven adelante en el laboratorio, no solo relacionados a la especialización sino también relacionada a las condiciones que debe tenerse en cuenta en un laboratorio de estas características. Se sugiere que en el protocolo interno se incluya procedimientos que regulen la forma de interactuar con el área, teniendo en cuenta la política institucional del organismo. Contar con guías de procedimientos de cadena de custodia, traslado de los dispositivos tecnológicos secuestrados al laboratorio y todo lo que se considere necesario con respecto al funcionamiento del mismo.

Esto no es un proceso sencillo, cada etapa requiere de un tiempo de maduración, de comunicación en la organización, de capacitación a los operadores del sistema judicial. Es importante tener en cuenta que en muchos lugares este tipo de laboratorio puede comenzar en la sede policial como un apéndice de las áreas de criminalísticas, en los ministerios públicos como parte de la policía judicial o en los poderes judiciales como integrantes por ejemplo de los cuerpos de investigaciones forenses [19].

Habrá que tener en cuenta en aquellos lugares donde ya funciona el sistema acusatorio penal o está en vías de desarrollarse, que pasaría con las pericias que requiere la defensa pública, este importante ítem merecerá un debate en un futuro próximo.

No importa el lugar donde el laboratorio se cree, sino tener siempre presente que es excluyente contar con todo lo aquí descripto para lograr una mayor excelencia en el trabajo pericial realizado, para evitar en la medida máxima posible cuestionamientos en la etapa de juicio.

5 Referencias

[1] Cano, Jeimy. Computación Forense. Descubriendo los Rastros Informáticos. Alfaomega. Méjico. (2009)

[2] Introducción a la Informática Forense. Francisco Lázaro Domínguez

[3] Darahuge, María Elena y Arellano González, Luís. Manual de Informática Forense. Errepar. Buenos Aires. (2011)

[4] Gómez, Leopoldo Sebastián. Calidad de Servicios Pericial mediante procedimientos operativos estandarizados Análisis Forenses de dispositivos de telefonía celulares. CAIF 2014. Congreso Argentino de Ingeniería Forense 2014

[5]Acordada 05/14 Superior Tribunal de Justicia. Disponible en http://tsjrn.opac.com.ar/pergamo/cgi-bin/pgopac.cgi?VDOC=3.44381&n=Acordada-N%BA-005-2014-30-04-2014-Departamento-de-Inform%E1tica-Forense-Protocolo-de-actuaci%F3n-Procedimientos-Internos-y-Gu%EDas-Operativas-Aprobaci%F3n

[6] Electronic Crime Scene Investigation: A guide for first responders, U.S. Department of Justice

[7] An Extended Model of Cybercrime Investigations, de Séamus Ó Ciardhuáin, International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1 https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

[8] Getting Physical with the Digital Investigation Process, de Brian Carrier y Eugene H. Spafford, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2 https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7A-FB6C-325D-BF515A44FDEE7459.pdf

[9] Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Segunda edición, por Eoghan Casey, Academic Press 2004, ISBN:0121631044

[10] Electronic Crime Scene Investigation: Guide for first responder, U.S Department of Justice. And Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Nacional Institute of Justice
https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[11] NIST (National Institute of Standars and Technology)
http://csrc.nist.gov/publications/nistir/nistir-7387.pdf
http://csrc.nist.gov/publications/nistir/ir7559/nistir-7559_forensics-web-services.pdf

[12] SWGDE (Scientific Working Group on Digital Evidence)
https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics%20V2-0
https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-1
https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Recommended%20Guidelines%20for%20Validation%20Testing%20V2-0
https://www.swgde.org/documents/Current+Documents/SWGDE+QAM+and+SOP+Manuals/2012-09-13+SWGDE+Model+SOP+for+Computer+Forensics+v3

[13] ACPO “Good Practice Guide for Digital Evidence”
http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[14] RFC 3227 “Guidelines for Evidence Collection and Archiving”
http://www.rfc-base.org/txt/rfc-3227.txt

[15] HB171:2003 Handbook Guidelines for the management of IT evidence
http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

[16] Semprini, Gaston Estandarización de procedimientos y protocolos del laboratorio de informática Forense. SID 2015. Anuales 44 JAIIO – Jornadas Argentinas de Informática – Rosario

[17] Gómez, Leopoldo Sebastián. Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados. SID 2015. Anuales 44 JAIIO – Jornadas Argentinas de Informática.

[18] Semprini, Gastón y Alfredo Bozzetti. Hacia una autogestión de la Informática Forense. SID 2014. Anuales 43 JAIIO – Jornadas Argentinas de Informática. Capital Federal.

[19] Acordada 19/14 Superior Tribunal de Justicia, disponible a pedido de bibliotecajstj@jusrionegro.gov.ar