Plan Estratégico para la implementación de un Centro de Servicios de Informática Forense

Sergio Daniel Appendino[1], Fredi Aprile[1], Herminia Beatriz P. De Gallo[1]

[1] Grupo de Investigación sobre Informática Forense
Facultad de Ingeniería de la Universidad Católica de Salta,
Salta, Argentina
{sappendino, faprile,bgallo}@ucasal.edu.ar

Abstract. El proceso de implementación de un centro de servicio profesional y científico supone la formulación de un plan estratégico que oriente la propuesta. La definición de la misión esencial, la visión que se persigue y los objetivos marcan las líneas a seguir en la transformación paulatina de la idea inicial en un hecho concreto. Elaborados estos componentes, se toman de base para definir un Plan de Acción que vuelque a la práctica la idea inicial, dando forma a una institución que cada día tiene mayor demanda, tanto desde los contextos judiciales como empresariales: un Centro de Servicios de Informática Forense.

Keywords: Informática Forense

1 Introdución

El presente documento resulta de las conclusiones arribadas en el Proyecto de Investigación sobre "APLICACIÓN DE METODOLOGIAS, PROCESOS Y TECNICAS PARA LA REALIZACION DE PERICIAS INFORMATICAS" aprobado por Resolución Rectoral N° 332/11 y desarrollado en la Facultad de Ingeniería de la UCASAL. Con el objetivo de estudiar y definir una metodología científica para el desarrollo del proceso de pericias informáticas acorde al proceso judicial propio del Poder Judicial de la Provincia de Salta, el proyecto fue desarrollado durante los años 2012 y 2013, y el presente informe muestra parte de los resultados logrados en el mismo.

2 Conceptos Metodológicos

Los autores referentes del tema identifican tres etapas en la planificación estratégica (formulación, implementación y evaluación) partiendo de la definición de la misión, visión, el análisis interno y del entorno para concluir en los objetivos que se persiguen.
Se propone el enfoque estratégico como un mecanismo adecuado para este trabajo ya que la formulación de una estrategia debe hacerse respetando el ser de la

organización, el deber ser, los escenarios probables, los recursos internos y los desafíos que se le presentan.
En resumen, los pasos a seguir son: 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.

2.1 Definición de la Misión y la Visión

Declarar la ***Misión Institucional*** significa responder a la pregunta ¿Qué nos hace "ser"? ¿Cuáles son las características esenciales que nos distinguen de otros?
Un Centro de Servicios de Informática Forense es una institución que surge de la necesidad de dar respuesta a la demanda de la justicia respecto de la recolección de evidencias significativas o determinativas para ser presentadas como pruebas en un proceso judicial y que permita la determinación del/los responsable/s de delito/s tanto informáticos como otros contemplados en el Código Procesal Penal y cuya prueba se encuentra conservada en dispositivos de Tecnología de Información (TI). Se declara entonces como Misión del Centro de Servicios de Informática Forense: "Ser un colaborador de la justicia en la identificación de evidencias relevantes para ser presentadas en juicio".
La ***Visión Estratégica*** permite identificar ¿Cómo queremos cumplir nuestra misión?, i.e., define el camino a seguir para no desviarnos de la misión esencial. Tratándose de acciones que impactan directamente en la seguridad, la vida y la libertad de las personas, es imprescindible que el servicio a brindar se sustente en la ciencia y la técnica, dando rigor y formalidad profesional a las actividades que se desarrollan.
Es así que definimos como Visión del Centro de Servicios de Informática Forense: "Ser una institución referente para la Justicia", para lo cual formulamos los siguientes propósitos: a) Sustentar nuestro trabajo en la ciencia, el rigor metodológico y la formalidad professional; b) Contribuir al desarrollo de la Informática Forense; y c) Actualizar nuestra base de conocimientos de manera acorde al desarrollo tecnológico.

2.2 Análisis del Contexto Externo e Interno

Además del ***contexto básico*** conformado por las instituciones jurídicas, se debe considerar el ***contexto tecnológico*** que impacta también en la comisión de delitos.
Por su parte las instituciones jurídicas (Poder Judicial, Ministerio Público, comunidad forense) se caracterizan por el desconocimiento de las tecnologías informáticas y de las comunicaciones, y se ven sorprendidas y avasalladas por la diversidad y complejidad de la "prueba digital". Esta situación dificulta la tarea pericial debido principalmente a que el promotor de dicha prueba generalmente desconoce lo que está solicitando. Se observa que el ambiente jurídico, principal demandante de la Informática Forense, presenta características que dificultan el desarrollo del Centro de Servicios de Informática Forense, a saber: a) Barreras de comunicación muy altas con los actores judiciales (abogados, jueces, Fiscales, personal administrativo); b) Dificultades para comprender y absorber la prueba intangible; c) Dificultad para especificar los puntos de pericia desde el vocabulario técnico; d) Legislación muy

genérica y poco actualizada; y e) Falta de tipificación de algunos de los delitos más comunes relacionados con las Tecnologías de la Información y las Comunicaciones.
Por su parte el contexto tecnológico actual no detiene su crecimiento y diversificación, generando un ámbito de dependencia tecnológica sin posibilidades de obviar. Esto impacta cada vez en el acto delictivo, haciendo que la "prueba digital" esté presente cada vez con más fuerza en las evidencias de la comisión del delito, abriendo posibilidades de intentar comprender lo que pasó antes, durante y después del hecho.
Un apartado especial merece el aporte de la investigación en las ciencias de la criminalística y su relación con la Informática Forense, dando el ámbito adecuado para que desde el conocimiento Científico Tecnológico se logre la identificación, preservación, adquisición, análisis, documentación y presentación de la prueba, en especial a partir de la consideración de la prueba digital como "prueba indiciaria" sumando el componente "virtual" a los hechos investigados.
La conformación del Centro de Servicios de Informática Forense supone varios desafíos internos. Por una parte, resulta necesario considerar el ambiente interdisciplinario que se requiere para el desarrollo adecuado de la Informática Forense. No solo desde su vinculación con las ciencias jurídicas y criminalísticas, sino con otras disciplinas tecnológicas como la electrónica, las telecomunicaciones, la ingeniería de sistemas y el tratamiento de imágenes, videos y voz. Considerar este ámbito plural ayuda a definir el alcance de la actividad pericial. Por otra parte, al ser tan amplia la brecha de comunicación con el contexto externo (ámbito judicial), requiere un esfuerzo extra al profesional tecnológico que debe introducirse en la ciencia jurídica mediante la capacitación y la actualización continua para comprender cabalmente el ámbito en el que debe desarrollar su trabajo.

2.3 Formulación de Estrategias

La conformación del Centro de Servicios de Informática Forense requiere de un trabajo orientado en cinco líneas:
Creación del Centro de Servicios de Informática Forense: Resulta fundamental definir las características institucionales del Centro, mediante la descripción de las funcionalidades y la estructuración organizacional del mismo.
Generación de acciones de capacitación: desde dos espacios de trabajo. Por un lado se requiere la instrucción necesaria a impartir en las áreas internas al Centro de Servicios de Informática Forense, que tienen que ver con la formación específica en Informática Forense y en particular sobre la identificación de pruebas. Por otro lado, es necesario capacitar al cuerpo de profesionales judiciales (jueces, fiscales, abogados en general, administrativos), mediante un plan de alfabetización tecnológica, delitos informáticos, tecnologías informáticas y de las comunicaciones y su impacto en la comisión de delitos. Estas acciones de capacitación se proponen como línea de trabajo continua, de manera que –mantenida en el tiempo- promueva la concientización y la culturalización de los recursos humanos en el tema que nos ocupa. El plan de capacitación deberá tener presente la conformación de grupos de capacitandos en función de los criterios habituales para estos casos (grado de conocimiento

tecnológico de la audiencia, niveles de la estructura funcional de la organización, interés o motivación en el tema, etc.)

Conformación de un Laboratorio de Informática Forense: mediante la incorporación de personal especializado en las distintas disciplinas de la TI Forense, como el tratamiento de las imágenes, videos y la voz, las Telecomunicaciones y la Informática y también mediante la adquisición del equipamiento necesario de herramientas Forenses, tanto Software como Hardware e Infraestructura, con el fin de contar con una batería de herramientas para atender las distintas alternativas que pueden surgir a partir de los distintos soportes de prueba, sus sofisticaciones, ámbitos geográficos y plataformas tecnológicas. Esta línea de trabajo presupone un plan de adquisición de productos de hardware y software que permitan –a mediano y largo plazo- la constitución de un ámbito tecnológico adecuado para garantizar la realización de pruebas y exámenes forenses con el marco científico y metodológico necesarios. A corto plazo debe implementarse una red de puestos de trabajo en cantidad suficiente, con equipamiento informático básico de última generación, más la instalación complementaria correspondiente (cableado estructurado, servidores, impresoras, etc.). A mediano plazo y largo plazo se debe incorporar componentes específicos para la actividad: Herramientas de hardware y software para la Satinado, Recolección y Preservación de evidencias; para el Análisis de Evidencia y para la Presentación de Informes.

Desarrollo de procedimientos técnico-legales: para garantizar la revisión científica, tecnológica y técnica de la prueba indiciaria es necesario establecer procedimientos formales, basados en normas de calidad, acerca de todos los procesos involucrados en la actividad pericial: recolección de la prueba y cadena de custodia, análisis y diagnóstico tecnológico, elaboración del informe técnico de pericia.

Plan de Crecimiento: con una mirada táctica/estratégica del sector demandante, es necesario tener en cuenta que en un futuro no muy lejano se requerirá una estructura de recursos humanos, tecnológicos y de infraestructura necesaria para alinear el servicio a las necesidades venideras. Las acciones formuladas deben consolidarse en el tiempo, mediante la realización de actividades que fortalezcan la propuesta. A saber: a) Tener presente los probables escenarios futuros en el desarrollo de la disciplina, contemplando las variables tecnológicas, sociales y su impacto en la comisión de delitos; b) Buscar el asesoramiento técnico de profesionales referentes en el ámbito de la Informática Forense, a fin de revisar y orientar las acciones hacia la búsqueda de la calidad; c) Monitorear el avance de la tecnología y de la ciencia con el objetivo de constituir la mejor arquitectura tecnológica para el desarrollo de la práctica de la Informática Forense; y d) Validar y ajustar los procedimientos técnico-legales mediante la experiencia continua.

3 Plan de Acción

Cada una de las estrategias definidas se concreta en un Plan de Acción. Si bien en el proyecto de investigación se ha destinado un espacio para desarrollar y formular en detalle cada una de estas estrategias, por razones de espacio en el presente documento se describen los más destacados: el Proyecto de Creación del Centro de Informática

Forense y el Procedimiento de Incautación de Pruebas Digitales, como un ejemplo del apartado correspondiente al desarrollo de los procedimientos técnico-legales.

3.1 Proyecto de Creación del Centro de Informática Forense

Con el objeto de formular los objetivos, características y descripción organizativa de un Centro de Servicios de Informática Forense que cubra el marco de lo estudiado en el presente proyecto de investigación, resulta necesario considerar un contexto real – el Gabinete de Informática del Ministerio Público de Salta- del cual partir, para analizar las fortalezas y debilidades actuales y formular los elementos que deberán ser considerados, a fin de formular una propuesta estratégica para la creación del Centro de Servicios.

Ante un ambiente en constante crecimiento y cambio, como lo es el de las Tecnologías con soporte Digital, la incorporación, la capacitación y el desarrollo de las distintas especialidades técnicas que den solución a los requerimientos recibidos de una manera adecuada y con soporte de conocimientos científicos forenses, hacen necesario repensar y plantear una nueva estructura funcional organizativa que contenga e integre el marco de conocimientos. Asimismo, el significativo e incesante crecimiento del número de solicitudes de Informes Técnicos por parte de las Fiscalías y la amplitud de conocimientos técnicos necesarios para resolver los requerimientos en el Área Digital hizo necesario desarrollar y ampliar la estructura de infraestructura y tecnologías de análisis de evidencias necesarias a fin de brindar adecuadamente los resultados del Área Forense Digital.

Tomando como caso ejemplo el Cuerpo de Investigaciones Fiscales (CIF) del Ministerio Público de la Provincia de Salta, es dable destacar que ante la importancia que aporta la Evidencia Digital puesta de manifiesto por los medios de comunicación tanto locales como Nacionales e Internacionales es necesario definir una estructura de Recursos Humanos, roles y responsabilidades dividida por funciones y que presenten la autonomía adecuada de funcionamiento del resto de las disciplinas definidas en el Artículo 7°- Estructura de la Ley 7665 de creación del CIF y compongan el área del campo del conocimiento Técnico Científico específico.

Las áreas de incumbencia propuestas dentro de la especialidad Forense Digital y que darían soporta a los procesos de evaluación y emisión de Informes Técnicos del CIF son:

Seguridad y Soporte Técnico Servidor CIF (Área Staf): Debido a la sensibilidad de información que se administra el Cuerpo de Investigadores Fiscales, a la Ley 7775 promulgada por el Senado y la Cámara de Diputados de la Provincia de Salta, "Registro Provincial de Condenados vinculados a Delitos contra las Personas y contra la Integridad Sexual" y a la incorporación de nuevas tecnologías que se están realizando en todas sus áreas, es necesario contar con un profesional técnico que se especialice en brindar soluciones tanto para la seguridad de la información interna como para el mantenimiento de la infraestructura de procesamientos de datos del todas las áreas del CIF. Asimismo este profesional, al estar fuera de la estructura operativa del trabajo diario, será el que lleve a cabo las evaluaciones de nuevas tecnologías que se implementen, tanto las internas para dar soluciones a los trabajos de las áreas técnicas del CIF como las que podrían ser utilizadas por el crimen

organizado. Eventualmente puede interactuar con estructuras de investigación a nivel Nacional como la Comisión Nacional del Cibercrimen, creada por la Jefatura de Gabinete de Ministros y el Ministerio de Justicia y Derechos Humanos, por Resolución Conjunta 866/2011 y 1500/2011.

Video, Imagen y Voz Forense: Área de análisis, desarrollo y soporte que tiene como funciones: a) Verificación e identificación de voz basadas en conversaciones por medio de herramientas biométricas Forense, como el software Batvox; b) Diseño de reconstrucciones virtuales de hechos investigados por medio de las herramientas de informática recientemente adquiridas como el Google Sketch Up Pro 8, Poser Pro 2012, Scene PD 5, Easy Street Drow 5, Adobe Photoshop CS6 y Corell Draw Graphics Suite X5; c) El mejoramiento de imágenes contenidas en fotos y/o videos por medio del software de análisis forense como por ejemplo el AmpedFive. Teniendo en cuenta que se encuentra actualmente en proceso de instalación 1.000 cámaras de seguridad de alta resolución en le provincia de Salta, 600 dentro del ejido Urbano de la Capital de Salta en donde se preveen para el área una significativa cantidad de trabajo; y d) Soporte técnico documental de video e imágenes relativos a las funciones del CIF (allanamientos, crímenes, accidentes, etc.) como también institucionales (videocámaras, conferencias, visitas, etc.).

Tecnología de Información Forense: Área de análisis y desarrollo que tiene como funciones: a) Verificación e identificación de evidencia digital contenida en soportes de medios magnéticos como son los discos rígidos, Pen-drives, tarjetas de memoria, etc. por medio del software Encase Forensics; b) Identificación y consolidación de datos para el desarrollo de estructuras de Bases y Bancos de Datos a fin de obtener, administrar y preservar la información relacionada a las evidencias digitales

Telecomunicaciones Forenses: Área de análisis y desarrollo que tiene como funciones:a) Verificación e identificación de evidencia digital contenida en soportes de aparatos de telefonía y geo-referenciados como son los aparatos celulares, tablet PC, GPS, cámaras de fotografía con GPS, etc., por medio de la herramienta de Hardware UFED y también de software MobilEdit; y b) Canalizar las solicitudes de información de las Fiscalías y servir de vínculo con las empresas prestatarias del servicio de Telefonía, sistematizando la información solicitada a fin de que sea posible la eficiente utilización del Software de entrecruzamiento de llamadas I2 Analyst´s Notebook.

3.2 Desarrollo de procedimientos técnico-legales

Resulta necesario formalizar los procedimientos para la recolección de la prueba y cadena de custodia, análisis y diagnóstico tecnológico, y la elaboración del informe técnico de pericia. Esta formalización permite ajustar el procedimiento a una norma que garantice la utilización de criterios metodológicos y buenas prácticas en la actividad, a saber:

Procedimiento para la Incautación de la Prueba Digital

Es de suma importancia tratar de individualizar acciones adecuadas que puedan llevarse a cabo cuando se trata de recuperar potenciales fuentes de pruebas digitales

de los lugares controlados por un sospechoso. Existe una diferencia radical entre recuperar físicamente los dispositivos y después examinarlos en un laboratorio forense y, capturar los datos de dispositivos antes de que sean apagados o desconectados de las redes o fuentes de alimentación. Este último requiere un mayor nivel de especialización y no debería ser llevado a cabo por cualquier persona que no tenga la formación adecuada y que está calificado para realizar el trabajo.

Preparar arribo a la escena

El proceso de planificación y preparación debe permitir una fácil identificación del nivel de apoyo que se requerirá en la escena, en situaciones en las que se pueden encontrar pruebas digitales.
En la legislación de la Provincia de Salta el único Organismo autorizado a realizar allanamientos y secuestros de incautación ordenadas por el Juez (o Fiscal) es la Policía de Salta, en el caso de secuestro de evidencia digital la persona responsable del operativo debería informar la necesidad de contar con el apoyo de una unidad de identificación compuesta por especialistas, en el caso de Salta, el Cuerpo de Investigadores Fiscales (CIF)
En caso de un escenario que no es ordenado por la Justicia es recomendable contar con la asistencia de un Escribano que certifique, tanto el escenario en general como todas las operaciones realizadas sobre la evidencia, y sea éste el que dirige el proceso de secuestro o incautación de elementos. La primera decisión a tomar es qué tipo de la incautación se debe realizar, si deberán secuestrarse equipos o se realizará la captura de datos en directo, inclusive puede ser necesaria una combinación de ambos. Si bien un procedimiento de allanamiento se inicia con la orden de un Juez con detalle del trabajo que se debe realizar, hay rango de decisiones que serán tomados en el lugar, cuando las circunstancias son más claras. Sin embargo sería deseable contar con la mayor cantidad información posible y que con antelación se conozca qué sistema de TI y las posibles fuentes de pruebas que puedan existir en el lugar de la escena. Los ejemplos de los tipos de información que ayuden a la planificación incluyen: Hardware/sistema operativo/software/aplicaciones y medios de almacenamiento relacionados con la información, la comunicación y la información relacionada con la red (ISP, teléfono, fax, módem , equipos de red LAN , etc.); Responsable del sistema informático y/o de la red (por ejemplo , si tiene un administrador o es administrada por una empresa externa); Cuantos equipos se puede encontrar; Qué cantidad de datos se pueden copiar y ¿existe una copia de seguridad del sistema disponible en medios de almacenamiento
La fase de preparación incluye los siguientes pasos: Asegurarse de que la toma de pruebas digitales esté autorizada correctamente e interpretar correctamente la orden judicial; en caso de que se deban recolectar datos de otra jurisdicción Judicial, asegurarse que se encuentra autorizado por la autoridad Judicial correspondiente; obtener la mayor cantidad de información posible sobre el sistema de TI que hay que peritar; elegir los miembros del equipo (incluir especialistas externos si es necesario); asignar tareas individuales para los miembros del equipo; informar a los miembros del equipo acerca de cómo realizar sus tareas, y proporcionar las herramientas y equipos adecuados y necesarios (logística).

Si se sabe o se cree que las pruebas digitales pueden ser encontradas en la escena, el equipo responsable del secuestro de elementos de debe incluir a los miembros especialmente entrenados para las tareas de búsqueda e incautación de los equipos informáticos y de evidencias digitales. En algunos casos puede incluso ser necesario consultar a un especialista independiente. Por ejemplo, si el sistema es administrado por una empresa externa o administrador, puede considerarse la participación de esta persona como testigo experto, siempre y cuando no sea el sospechado. Los avances en la tecnología o el ambiente de tecnología relacionado a las causas judiciales locales pueden obligar a cambiar las herramientas y equipos necesarios para la recolección de evidencias. Un equipo o conjunto básico es de sumo valor durante la búsqueda y el secuestro y debe estar disponible en el lugar de trabajo. Así se debe contar con: a) Herramientas para el armado/desarmado de componentes informáticos; b) Elementos para la documentación e identificación de la evidencia; c) Elementos para el empaque y transporte de la evidencia; y d) Elementos para la comunicación con el equipo técnico-jurídico que participa de la incautación

En la escena

La persona encargada del operativo o búsqueda debe garantizar la seguridad de todas las personas en el lugar y la integridad de todas las pruebas, tanto tradicionales como electrónicos/digitales. Debe tenerse en cuenta que las posibles pruebas en computadoras y otros dispositivos electrónicos pueden ser fácilmente alterados, borrados o destruidos.
Se proponen para esta etapa los siguientes pasos: a)seguir la política de competencia para fijar la escena, en general las trazadas por la especialidad de Criminalística; b) sacar todas las personas fuera de la zona inmediata donde se encuentra la evidencia se debe recogida; c) asegurar todos los dispositivos electrónicos, incluyendo los dispositivos personales y portátiles; d) rechazar ofertas de ayuda o asistencia técnica de cualquier persona no autorizada; e)se debe dejar un computador o dispositivo electrónico apagado si ya estuviera apagado; f)si un equipo está encendido o el estado no se puede determinar, evaluar la situación si es conveniente recuperar "datos en vivo" del mismo, sacar imágenes de la pantalla actual, u otra técnica que el perito decida; g) se debe proteger los datos volátiles física y electrónicamente por todos los medios posibles; h) identificar y documentar los componentes electrónicos relacionados que no serán recogidos; y otras cuestiones relativas a la búsqueda de pistas no necesariamente digitales y al resguardo de la prueba y de la escena del crimen.

Documentar la escena

Es un proceso continuo a lo largo de todo el procedimiento de secuestro. Es muy importante documentar con precisión la ubicación y el estado de los equipos, medios de almacenamiento, otros dispositivos electrónicos y convencionales.
En general, se debe documentar lo siguiente durante la recopilación de evidencias: a) Fotografiar o registrar con video, documentando la escena completa en 360 grados de cobertura, si es posible, y detallar los sistemas informáticos y los componentes, dispositivos y equipos electrónicos; b) Documentar con detalles todos los equipos de

almacenamiento digital que se encuentran, por ejemplo, marca, modelo, número de serie, etc.; c) Estado y la ubicación de cada sistema informático que contiene o puede contener pruebas digitales, incluyendo el estado de energía del computador o dispositivo, si se encuentra encendido, apagado o en modo de hibernación o suspensión; entre otras.

Recolección de la evidencia

Un sistema informático no deberá utilizarse como evidencia sólo porque se encuentran en el lugar. La recolección de los elementos debe ser justificada por autoridad competente, por lo que la autoridad que ordenó la búsqueda debe tomar una decisión consciente de que si un artículo está siendo recolectado por el perito, debe tener una sospecha razonable o evidencia suficiente que justifique el hecho. La evidencia electrónica, al igual que con cualquier otra evidencia, debe manejarse con cuidado y de manera que conserve su valor probatorio. Esto se refiere no sólo a la integridad física de un elemento o dispositivo, pero también a la electrónica de datos que contiene. Ciertos tipos de pruebas electrónicas por lo tanto requieren cuidados especiales para su recolección, embalaje y transporte. La evidencia digital es susceptible a daños o alteración de los campos electromagnéticos como los generados por la electricidad estática, los imanes, transmisores de radio y otros dispositivos por lo que deben ser protegidos adecuadamente. La recuperación de la evidencia no electrónica o pruebas convencionales, también puede ser crucial en el investigación de los delitos digitales/informáticos. Toda la evidencia debe ser identificado, asegurada y conservada dando cumplimiento de normas y procedimientos de documentación como registro de identificación, cadena de custodia, registro de actuario de Escribano y otras basadas en las leyes aplicables de cada jurisdicción.

Embalaje, transporte y almacenaje:

Las computadoras y los dispositivos de almacenamiento digital son instrumentos electrónicos frágiles, que son sensibles a la temperatura, humedad, golpes, electricidad estática, fuentes magnéticas, e incluso a algunas acciones como el encendido y apagado. Por lo tanto, se deben tomar precauciones especiales cuando se envasan, transportan y almacenan las pruebas. En general, todos los componentes del equipo digital y medios de almacenamiento deben ser manejados con sumo cuidado ya que un manejo inadecuado puede causar daños o la destrucción de pruebas electrónicas.

4. CONCLUSIONES

La propuesta de desarrollar un Centro de Servicios de Informática Forense no se agota en estos escritos, todo lo contrario, se ha formulado una guía de trabajo que deberá ser validada pragmáticamente en un proceso de implementación gradual y dirigido. La planificación estratégica incluye una etapa de evaluación, que tiene como fin último saber si las estrategias propuestas funcionaron adecuadamente. Todas las estrategias están sujetas a modificaciones futuras porque los factores externos e internos cambian

constantemente, de manera que sería necesario realizar la revisión de los factores externos e internos en que se basan las estrategias actuales, hacer mediciones del rendimiento, y tomar medidas correctivas. Es importante también incorporar una visión multidisciplinar, con la asistencia de la Justicia y la Criminalística para que sus aportes enriquezcan y permitan ajustar el modelo a la realidad técnico-jurídica necesaria. La Informática Forense no actúa solamente en el ámbito de la Justicia, resulta necesario considerar la perspectiva de difundir y consolidar la disciplina en el área empresarial y social de nuestro medio.

References

1. David, Fred R, Conceptos de Administración Estratégica, PEARSON EDUCACIÓN, México, 2003
2. Instituto Nacional de Estadística e Informática (INEI), Guía Teórica-Práctica para la formulación de Proyectos Tecnológicos, Perú, 2002, vigente al [www.ongei.gob.pe/publica/metodologias/5162.pdf] el 14/05/2013.
3. Orión Aramayo et alt., MANUAL DE PLANIFICACIÓN ESTRATÉGICA, Instituto de la Comunicación e Imagen de la Universidad de Chile, Chile, vigente al [guiametodologica.dbe.uchile.cl/.../planificacion_estrategica.pd] el 31/03/2013.
4. Iván Silva Lira, Metodología para la elaboración de estrategias de desarrollo local, Instituto Latinoamericano y del Caribe de Planificación Económica y Social (ILPES), Chile, 2003, consultado en [www.eclac.org/publicaciones/xml/7/13867/sgp42.PD], vigente al 14/05/2013.
5. Castillo, Rafael et alt., Concientización en la Seguridad Informática, Universidad de Los Andes, Colombia, consultado en [www.criptored.upm.es/guiateoria/gt_m142r.htm] vigente el 10/05/2013.
6. Richard Brian Adams, 2012 The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice, This thesis is presented for the degree of Doctor of Philosophy of Murdoch University
7. Data Protection and Cybercrime Division, 2013, Electronic evidence guide, A basic guide for police officers, prosecutors and judges, Version 1.0, Cyber Crime @IPA, www.coe.int/cybercrime, Council of Europe Strasbourg, France, 18 March 2013.
8. U.S. Department of Justice, Office of Justice Programs, 2008, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition,www.ojp.usdoj.gov/nij
9. Peter Sommer, 2013, Digital Evidence,Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers Information Assurance Advisory Council (IAAC), United Kingdom.
10. IACP Technology Policy Framework,2014,IACP Divisions, Committees, Sections, the IA CP National Law Enforcement Policy Center, and others, [http://www.theiacp.org/Portals] vigente al 10/03/2014.
11. SWGDE Model Standard Operation Procedures for Computer Forensics, 2012, Scientific Working Group on Digital Evidence, Version: 3.0
12. Good Practice Guide for Computer-Based Electronic Evidence, 2007,published by 7Safe, www.7safe.com/electronic_evidence , Association of Chief Police Officers (ACPO).
13. Best Practices For Seizing Electronic Evidence, 2013, v.3, A Pocket Guide for First Responders, U.S. Department of Homeland Security United States Secret Service.