SUPERIOR TRIBUNAL DE JUSTICIA DE LA PROVINCIA DE RIO NEGRO

ACORDADA Nº 8/2012

En la ciudad de Viedma, Provincia de Río Negro, a los **12 días del mes de noviembre de dos mil doce**, reunidos en Acuerdo los Señores Jueces del Superior Tribunal de Justicia: Dr. Víctor Hugo Sodero Nievas, Presidente y Dres. Enrique J. Mansilla y Sergio M. Barotto, y

CONSIDERANDO:

Que en los últimos años el desarrollo de las Tecnologías de la Información y las Comunicaciones (TICs) ha evolucionado y permite que sean hoy cada vez más las personas que poseen acceso a las mismas.

Que no son ajenos a este proceso los poderes judiciales como parte de esta sociedad dinámica, cambiante, compleja y con más exigencias de perfeccionamiento y precisión que les impone a los jueces al momento de resolver los casos que llegan a su gobierno.

Que en este contexto y en orden a la diversidad de situaciones que aparecen y que obligan al legislador a modificar normativas que así lo recepten tanto en el ámbito civil, de familia, laboral, penal y hasta disciplinario también insta a los poderes judiciales a dictar normas de creación de organismos técnicos auxiliares a esos fines.

Que en ese orden la inclusión de los cuerpos técnicos especializados es una adecuada y necesaria herramienta para los jueces al momento de decidir sobre el mal uso de los TICs, ley 26388 (delitos informáticos).

Que el uso de nuevas tecnologías permite investigar diferentes hechos delictivos relacionados con la conducta de las personas: - Uso del software sin su respectiva licencia; - ocultamiento de información, - usurpación de identidad en redes sociales y correos electrónicos, - amenazas y difamaciones; estafas mediante la utilización del phishing (pesca de datos personales); uso de ingeniería social engañosa para obtener claves bancarias o de acceso a otros servicios; sistemas de filmación los cuales pueden ser usados a la hora de dictaminar los hechos de un delito; entre otros.

Que en el ámbito de este Poder Judicial, desde el año 2010 se vienen realizando experiencias de análisis forenses sobre el uso y mal uso de las TICs., con resultados positivos en los distintos fueros.

Que por resolución Nº 502/12 STJ modificatoria de la 616/10 STJ, ambas relacionadas al Área de Informatización de la Gestión Judicial se escindió de su órbita la Informática Forense, pasando a formar parte de los Cuerpos Técnicos Auxiliares.

Que el paso siguiente es disponer la creación de dicha área, que sustituye el art. 8vo. de la Res. 502/12 STJ, definir sus misiones y funciones y su estructura escalafonaria para proceder al llamado a concurso para la cobertura del/los cargos que ella contemple.

Por ello, en uso de las atribuciones que le confiere los arts. 206 inc.1 y 224 de la C.P., 44 inc. a y j y 159 inc. a de la ley K 2430, 5 del CPP.

EL SUPERIOR TRIBUNAL DE JUSTICIA DE LA PROVINCIA
RESUELVE:

1º) CREAR el Departamento de Informática Forense en el ámbito de los Cuerpos Técnicos Auxiliares, con asiento de funciones en la ciudad de Viedma, con competencia Provincial, pudiendo crearse Delegaciones en las demás Circunscripciones de la Provincia, cuando la demanda lo requiera previa evaluación de la disponibilidad presupuestaria.

2º) DISPONER que el Departamento de Informática Forense esté a cargo del "Jefe de Informática Forense", el que ostentará jerarquía de Jefe de Departamento.

3º) ESTABLECER sus misiones y funciones que como ANEXO 1 y 2 forman parte de la presente.

4º) ESTABLECER los REQUISITOS DEL JEFE DEL DTO. DE INFORMATICA FORENSE: a) Ser mayor de edad; b) Ser argentino nativo o naturalizado con tres (3) años de ejercicio de la ciudadanía; c) Poseer grado académico de un mínimo de cuatro (4) años vinculado con la Informática, expedido por Universidad Nacional Pública o Privada, d) Contar con especialización acreditable de Informática Forense con evaluación formal y e) Tener una experiencia profesional comprobable de al menos dos (2) años en tareas similares.

5º) Notifíquese, protocolícese y oportunamente archívese.

Firmantes:
SODERO NIEVAS - Presidente STJ - MANSILLA - Juez STJ - BAROTTO - Juez STJ.
LATORRE - Secretaria de Superintendencia STJ.

ANEXO 1

MISIONES Y FUNCIONES GENERALES DEL DEPARTAMENTO DE INFORMÁTICA FORENSE

1.- Asistir a los Magistrados y Funcionarios del Poder Judicial en el requerimiento técnico-procesal en la investigación de delitos.

2.- Disponer su intervención profesional en las causas judiciales de todos los fueros a requerimiento de los distintos titulares de los órganos jurisdiccionales, de los Ministerios Públicos y de la Auditoría General Judicial en su función de investigación.

3.- Coordinar con el área OITEL de la Procuración General cuestiones que sean de incumbencia en común.

MISIONES y FUNCIONES DEL JEFE DEL DTO. DE INFORMATICA FORENSE

1. Asistir a Magistrados y Funcionarios en determinar las medidas preliminares para el abordaje de la investigación de una causa relacionada a un delito informático.

2. Asesorar en los procedimientos y acciones para el secuestro y recolección de evidencias digitales. Deberá atento al desarrollo de las ciencias informáticas revisar y redactar y mantener actualizado los procedimientos para tales fines.

3. Recepcionar y diligenciar las solicitudes que para establecer puntos de pericias sean necesarias oficiar a las empresas públicas y privadas, como por ejemplo Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, empresas de Telefonías Fijas y de Celular, Prestadores de Internet (ISP), Proveedores de Servicios de Mail, Redes Sociales, entidades bancarias, etc.

4. Capacitarse en los nuevos delitos informáticos y nuevas herramientas y técnicas para el análisis de la prueba digital.

5. Capacitar a los Informáticos Forenses que de él pudieren depender, y a los Magistrados y Funcionarios en el estado del arte de la materia.

6. Auditar peritajes realizados externamente por otros peritos establecidos por las partes de una causa, cuando un Magistrado o Funcionario lo solicite.

7. Definir las herramientas de software y hardware necesarias para realizar las tareas del Informático Forense.

8. Procesar la información digital y realizar los Informes Periciales acorde con los parámetros establecidos por los Magistrados y Funcionarios.

9. Utilizar las herramientas específicas, como personal especializado, que se aplican a los Dispositivos Tecnológicos.

10. Recolectar evidencias digitales para examinar, determinar su origen y contenido y así demostrar cómo, cuándo y quién pudo realizar un delito informático que se encuentra en investigación.

11. Llevar a cabo las tareas principales según lo establecido en el ANEXO 1 - GUIA DE PROCEDIMIENTOS y así poder realizar las Pericias Informáticas acorde lo establecido.

12. Evacuar las dudas de los Magistrados y Funcionarios y realizar un Informe Técnico si así lo requirieran.

13. Utilizar las herramientas y técnicas del Área para el procesamiento de la evidencia digital como ser:

a) Peritar sobre control, actualización y adquisición de licencias de software. Ley de Propiedad Intelectual 11.723 y su modificación Ley 25.036.

b) Peritar sobre robo, hurto, borrado o accesos a la información de una determinada empresa o institución, procesada y/o generada por los sistemas informáticos.

c) Peritar sobre recupero de datos borrados y rastreo de información en los distintos medios informáticos (magnéticos – ópticos).

d) Peritar sobre contratos en los que la informática se encuentre involucrada (contratación de servicios, adquisición de equipamiento informático y de sistemas, tercerización de servicios).

e) Peritar sobre aspectos laborales vinculados con la informática.

f) Peritar sobre robos o determinación de identidad a través de correos electrónicos, redes sociales y mensajería.

g) Peritar sobre aspectos vinculados al comercio electrónico y operaciones realizadas a través de Internet.

h) Peritar sobre dispositivos de grabación de video privados y del ámbito público.

i) Realizar todo otro encargo que al Departamento de Informática Forense se le efectúe, siempre que se encuentre relacionado con el objeto especial de su experticia.

ANEXO 2

GUIA DE PROCEDIMIENTOS

Objetivos

1. Evitar la contaminación y dispersión de la prueba durante el proceso judicial.
2. Formalizar el procedimiento de actuación pericial en materia informática.
3. Definir el alcance de los servicios de informática forense.

Procedimientos

- 1. **Del procedimiento general de investigación judicial con tecnología informática:**

En el ámbito penal, el procedimiento general de investigación judicial utilizando servicios de informática forense, consta de dos fases principales:

a) Incautación confiable de la prueba y mantenimiento de la Cadena de Custodia.

b) Análisis de la información disponible con arreglo al incidente investigado y redacción del informe pericial.

La primera etapa debe ser llevada a cabo por personal policial junto a los operadores judiciales encargados de conducir el procedimiento (Jueces, Fiscales y/o Secretarios). La segunda etapa debe ser efectuada en el laboratorio el Perito Informático, siguiendo los estándares de la ciencia forense para el manejo de evidencia digital, en función a los puntos de pericias que sean solicitados.

- 2. De la identificación y preservación de evidencia digital:

La identificación de material informático para peritaje por parte del personal policial debe ser efectuada conforme las pautas de la Guía de Procedimiento para el Secuestro de Tecnología Informática. Es de especial importancia la utilización de precintos de seguridad desde el momento del secuestro del material, y todos aquellos medios tendientes a garantizar la autenticidad e integridad de la evidencia digital.

- 3. Del requerimiento judicial:

Cuando sea requerido, el Perito actuante evacuará las consultas previas de Magistrados y Funcionarios para eliminar ambigüedades y definir el alcance de los puntos de pericia en lo que respecta a los servicios de informática forense. Se debe proveer toda la información necesaria para realizar la tarea pericial, de manera clara y precisa. El oficio con los puntos de pericia deberá enviarse desde el organismo requirente indefectiblemente junto con el material probatorio sometido a peritaje. Sólo se realizarán pericias que involucren la utilización del hardware y software específicamente adquirido para informática forense. Quedan excluidas del servicio de pericias informáticas toda tarea administrativa o técnica (tareas de transcripción de texto o simplemente dactilográficas, tareas de ordenamiento de información o cruzamiento de datos, tareas de escucha, tareas de filmación, copias simples de CD/DVD y otros dispositivos de almacenamiento) que no sea propia de la disciplina.

- 4. De la recepción del material secuestrado:

El material informático secuestrado deberá ser enviado al Departamento de Informática Forense o sus Delegaciones si las hubiese. Se cotejará la existencia de los precintos sobre los secuestros y la correcta identificación de los elementos enviados a peritaje. Todo organismo judicial o policial que intervenga en el manejo de la Cadena de Custodia, deberá tener presente las sanciones previstas en la Ley 26.388. En caso de detectarse la alteración o ausencia de precintos de seguridad, se dejará constancia en un acta de recepción que deberá ser suscripta por el responsable del traslado. En causas judiciales pertenecientes al ámbito penal, es responsabilidad del personal policial el traslado de todo el material secuestrado hasta los organismos judiciales. Cada una de las personas que haya trasladado los elementos probatorios deberá dejar registrada su intervención con los medios que se establezcan.

- 5. De la presentación del dictamen:

El dictamen será presentado siguiendo los estándares utilizados para la presentación de reportes informáticos forenses. Se intentará minimizar el volumen de información en soporte papel, suministrando toda la información complementaria que sea necesaria para el objeto de la pericia en soporte digital. Los elementos probatorios originales que almacenen evidencia digital deberán resguardarse hasta finalizar el proceso judicial, si se pretende que sean utilizados como prueba, conforme el Art. 237 del Código Procesal Penal y Correccional vigente.

- 6. De la remisión del material secuestrado:

Una vez finalizado el peritaje, se remitirá el dictamen y los elementos informáticos al organismo de origen. Los elementos analizados deberán ser resguardados con los medios adecuados para preservar la integridad y la autenticidad de la evidencia digital.

----------o0o----------