**SUPERIOR TRIBUNAL DE JUSTICIA DE LA PROVINCIA DE RIO NEGRO**

**ACORDADA Nº 11/2015**

En la ciudad de Viedma, Capital de la Provincia de Río Negro, a los **29 días del mes de mayo de dos mil quince**; reunidos en Acuerdo los Sres. y Sras. Jueces/Juezas del Superior Tribunal y;

**CONSIDERANDO:**

Que el Superior Tribunal de Justicia creó por Acordada 8/2012 el Departamento de Informática Forense, en cuyas Misiones y Funciones se establece, entre otras, el análisis de toda evidencia digital.

Que, en orden al crecimiento de las tareas profesionales en general y forenses en particular, se creó mediante la Acordada 19/2014 el escalafón profesional y técnico del Poder Judicial, incorporando en el escalafón C1 a los profesionales de la Informática Forense.

Que por dicho acto administrativo este Superior Tribunal modificó el Area de Informática Forense, dotándola de una nueva estructura orgánica y funcional, a partir de la cual se están realizando el respectivo concurso público de ingreso para cubrir dicha integración.

Que con el advenimiento de las Tecnologías de la Información y las Comunicaciones, llamadas habitualmente TICs, se permite a la población en general comunicarse a través de mails, mensajerías instantáneas, etc., obtener y compartir fotografías y video, utilizar las redes sociales, acceso a internet, geolocalización, manejo de archivos en la nube, etc. y que en los últimos años su desarrollo principal se ha visto canalizado a través de dispositivos móviles (notebooks, netbooks, tablets, smartphones, gps, smartwatches, etc.).

Que, como puede apreciarse, los dispositivos móviles no son más que una computadora con características y factores de forma diferentes, y su contenido a la luz de las ciencias forense no es más que evidencia digital.

Que el Área de Informática Forense viene desempeñando una tarea de crucial importancia como auxiliar de la justicia; tanto para Magistrados como para funcionarios del Ministerio Público.

Que en el último tiempo ha incorporado tecnología de última generación y ha desarrollado un laboratorio en la especialidad el cual trabaja en base a protocolos y procedimientos estandarizados para el tratamiento de la evidencia digital que incorpora una

guía de secuestros específica numerada y rubricada para cada causa.

Que el responsable del Area ha capacitado a agentes y funcionarios de este Poder Judicial en toda la provincia en el uso de dichos protocolos, como así también a otros operadores del sistema en general, y a los Abogados de las distintas Circunscripciones en particular.

Que el Ministerio Publico posee un área de análisis de las telecomunicaciones de los celulares limitándose a la interrelación de los mensajes de textos y sus llamadas enviadas y recibidas, como así también a la extracción de imágenes y videos, no realizando el análisis forense de otros contenidos.

Que, el desarrollo antes mencionado precisa que este Superior Tribunal atienda el análisis de dispositivos móviles y meritúe su tratamiento dentro del área de Informática Forense, a los efectos de proceder al análisis de la evidencia digital almacenadas en ellos,

Por ello, y en uso de las atribuciones que le son propias

**EL SUPERIOR TRIBUNAL DE JUSTICIA**
**RESUELVE:**

**Artículo 1°.-** Disponer que a partir de la fecha el área de Informática Forense se avoque al análisis forense de los contenidos digitales de los dispositivos móviles: notebooks, netbooks, tablets, smartphones, smartwatches, gps y otras formas que se desarrollen a futuro en base a estas premisas en su laboratorio.

**Artículo 2°.-** Aprobar al área de Informática Forense, las guías y procedimientos para el tratamiento de esta prueba indiciaria “Guía de procedimientos para pericias de dispositivos móviles” elaborado por el Lic. Gastón Semprini, el que como Anexo 1 corre agregado a la presente.

**Artículo 3.-** Establecer que el área de informática forense a través de su jefe y mediante la utilización del correo electrónico oficial y su firma digital gestione un protocolo propio de comunicaciones digitales -con la debida intervención del Juez y/o Fiscal que lo requiera- con las empresas proveedoras de correos electrónicos, de internet, de redes sociales, entidades bancarias, etc. a los efectos de obtener datos completos de sus usuarios e Ips de conexión involucrados en delitos informáticos. Cuando sea necesario la ostensión de los IPs de conexión pertenecientes a las compañías de telecomunicaciones (Movistar, Claro), el

pedido será realizado por la OITEL, quien posee el protocolo para actuar con las mismas.

**Artículo 4°.-** Capacitar a todos los usuarios de los juzgados y fiscalías en coordinación con la Escuela de Capacitación Judicial sobre los aspectos aquí tratados.

**Artículo 5°.-** Registrar, comunicar, publicar en el boletín oficial, cumplido archivar.

**Firmantes:**
**ZARATIEGUI - Presidenta STJ - PICCININI - Jueza STJ - APCARIAN - Juez STJ - MANSILLA - Juez STJ - BAROTTO - Juez STJ.**
**ARIZCUREN - Secretario STJ.**

# ANEXO 1

## GUIA DE PROCEDIMIENTOS PARA PERICIAS DE DISPOSITIVOS MOVILES

Ante un proceso judicial, en la que se requiera la intervención de un perito informático para realizar un procedimiento pericial sobre dispositivos móviles, se pueden dar en dos ámbitos diferentes, por un lado la intervención *in-situ* (lugar del hecho) o que el/los dispositivos se encuentren a disposición del Juzgado. Mas allá del ámbito de actuación, es importante destacar que la metodología implementada para la obtención o manipulación de la evidencia digital es similar en ambos casos, lo que puede variar es que el equipo se encuentre apagado o encendido. La obtención de la evidencia digital se realizará según la metodología del ciclo de vida de la evidencia digital (Identificación, Preservación, Análisis y presentación).

**1) Identificación:**

**a)** Colocarse guantes.
**b)** Fotografiar el/los dispositivos celulares
**c)** Estado en el que se pueda encontrar el dispositivo: Apagado o Encendido.

- Si el dispositivo celular se encuentra APAGADO, mantener de esa manera para ser analizado en el laboratorio con las herramientas específicas, y evitar sobreescritura.

- Si el dispositivo se encuentra ENCENDIDO realizar las siguientes operaciones:
  - Mantener batería cargada y no manipularlo. Evitar tocar la pantalla táctil.
  - Realizar los procedimientos necesarios para aislar al celular de la red. Este procedimiento se pude realizar de la siguiente manera:
    - cubriéndolo con varias capas de papel aluminio.
    - colocarlo en una Jaula Faraday.
    - encender un inhibidor de señal en cercanía del teléfono celular.
    - configurar dicho dispositivo en Modo de Avión (de este modo el celular no puede enviar o recibir llamadas telefónicas, mensajes de textos, mensajes con imágenes o mensajes de video, tampoco se podrá navegar en internet o usar los dispositivos Bluetooth. El resto de las aplicaciones siguen en funcionamiento como ser reproductor de música, juegos, agenda, etc. Esta función en general es realizada apretando el botón de apagado y seleccionar el "Modo Avión".

Otro modo es presionando Menú de la pantalla inicial, Configuración o Ajustes, Redes Inalámbricas o Wireless Networks, y luego la opción Modo Avión.

- Apagar dispositivo y quitar batería.

**d)** Dejar registrado todo en el "Formulario de registro de evidencia de celulares".

| | FORMULARIO DE REGISTRO DE EVIDENCIA | |
|---|---|---|
| Nro. EXPEDIENTE | CARATULA | JUZGADO |
| | | |

| Especificaciones del celular | |
|---|---|
| Marca | |
| Modelo | |
| Nro de serie | |
| Garantía | |
| IMEI | |
| Nro. Teléfono | |
| Porveedor de enlace | |
| Otros | |

| Almacenamiento | | | | |
|---|---|---|---|---|
| Cantidad | Tipo de Memoria | Marca/Modelo | Velocidad /Capacidad | Nro. De Serie |
| | | | | |
| | | | | |

| Accesorios y Periféricos | | | | |
|---|---|---|---|---|
| Cantidad | Tipo: | Marca/Modelo | Velocidad/Capacidad | Nro. De Serie |
| | | | | |
| | | | | |

| Observaciones: | | |
|---|---|---|
| Perito Informático Forense | Lugar | Fecha |
| Nombre:<br><br>Apellido:<br><br>DNI | | |
| | Firma: | |
| | Aclaración: | |

**2) Preservación**

Se obtendrá la información sobre el modelo del Celular, para poder realizar la

recolección y protección de la evidencia digital.

**a)** Identificar la tecnología general del teléfono celular.

**b)** Localizar cables, drivers y determinar el software o hardware forense a utilizar para la pericia informática. La selección de herramientas forenses para una pericia informática sobre telefonía celular depende de diversos factores, como el nivel de detalle requerido en los puntos de pericia, el modelo de teléfono celular en cuestión y la presencia de otras funcionalidades de almacenamiento externo del dispositivo.

**c)** Determinar funcionalidades del teléfono celular y posibles datos almacenados en el mismo.

**d)** Si el teléfono celular no tiene puerto de datos, no se cuenta con el cable de datos, o no existe software o hardware forense disponible para dicho modelo, se registra esa situación.

**e)** Si el teléfono contiene Tarjeta de Memoria Externa, realizar una Imagen Forense con la herramienta forense apropiada.

- Extraer de la misma toda evidencia digital que sea relevante en la causa.

**f)** Extracción de Información de la Tarjeta SIM (Subscriber Indetity Module). De la tarjeta SIM se puede obtener Identificador de área local (identifica donde esta ubicado actualmente el Celular), Numero de serie, Numero de Cliente (se refiere al IMSI (International Mobile Subscriber Identity) que es el número de identificación del cliente que permitirá, junto al la ayuda del proveedor del servicio, identificar al cliente propietario del celular), y por último el numero de teléfono del celular (MSISDN Mobile Subscriber Integrated Services Digital Network).

También se puede obtener de la tarjeta SIM, mensajes de textos, mensajes borrados, contactos y últimos números marcados.

- Generar una clonación de la SIM o leer la información digital de dicho dispositivo.
- utilizando un lector de SIM protegido contra escritura.
- Si el SIM está bloqueado por PIN, se deja constancia o se utiliza el PUK en caso de estar disponible. (PUK es la clave o password de 8 dígitos de longitud para

desbloquear la tarjeta SIM del equipo celular cuando se ha olvidado el PIN o bien se ha bloqueado totalmente el teléfono).

- Si el SIM no está bloqueado, se extrae la información digital relevante al caso.

**g)** Aislar el dispositivo de la red de telefonía celular previamente a la extracción de información digital y si es posible, durante todo el proceso.

**h)** Realizar una extracción física de la memoria del teléfono celular o bien una extracción lógica utilizando todas las herramientas forenses apropiadas, tanto de hardware como de software.

**i)** Verificar los resultados obtenidos.

**j)** Validando mediante valores hash distintos artefactos digitales del teléfono celular.

**3) Análisis**

En esta etapa se analizara la evidencia digital con las diferentes herramientas de software forenses para obtener los datos especificados en los puntos de pericias propuestos por Magistrado o Funcionario. Aplicándose técnicas especificas de análisis forense.

**4) Presentación**

Se elaborara el informe pericial final mediante los resultados obtenidos y remitirlo junto a los elementos probatorios, acorde a lo establecido en los puntos 5 y 6 de la acordada N° 8 del 2012.

**----------o0o----------**