Guía de Buenas Prácticas para el secuestro, preservación y envío de elementos de informática

Reglas generales

1.- Asegurar el lugar y preservar la evidencia electrónica, impidiendo el acercamiento de toda persona ajena al equipo criminalístico.

2.- La evidencia solo debe ser manipulada por expertos o por la persona a cargo del procedimiento. Usar guantes de látex para no contaminar las improntas dactilares o palmares, o evidencia biológica cuya recolección puede ser útil para el esclarecimiento del caso.

3.- Fotografiar todos los equipos (informáticos, de comunicación o almacenamiento), sus alrededores y conexiones. Asimismo si el dispositivo se encuentra encendido, fotografiar el contenido que refleja la pantalla. Si el equipo se encuentra en stanby (monitor encendido con su pantalla en negro) mover el Mouse y cuando la pantalla muestre el contenido, fotografiarla.

4.- Preservación de equipos (informáticos, de comunicación o almacenamiento). Si al momento de la diligencia de secuestro se encuentran húmedos o sumergidos en algún líquido se deberá proceder del siguiente modo:
a.- equipos de telefonía celular sumergirlos en alcohol isopropílico.
b.- equipos DVR, abrirlos, y luego, sumergirlos en alcohol isopropílico.
c.- computadoras de escritorio, notebooks y netbooks, extraer el disco rígido del dispositivo y luego sumergirlos en alcohol isopropílico.

En todos los casos de no contarse con alcohol isopropílico deberá sumergirse en alcohol etílico.-

5.- Si por razones de urgencia el experto en informática decide manipular el elemento en el lugar para extraer información, será obligatorio realizar una filmación de este proceso y dejar constancia en el acta de las tareas que se realizaron.

Reglas particulares

1.- **Computadoras personales de escritorio**. Proceder del siguiente modo:
a.- Si el equipo se encuentra apagado, nunca encenderlo.
b.- De encontrarse encendido no apagarlo con los métodos convencionales. En este caso dar aviso inmediato al experto en informática forense o, de no ser posible, proceder desconectando directamente la alimentación desde la parte trasera del gabinete del equipo.
c.- Si hay indicios o sospechas que el equipo esta corriendo algún tipo de programa de borrado, desconectar directamente la alimentación.

2.- En caso de secuestro de notebooks y/o netbooks extraer la batería del dispositivo. Si el mismo se encuentra encendido no apagarlo de forma

tradicional, sino que directamente extraer la batería. Cuando no puedan ser extraídas las baterías como por ejemplo con los dispositivos de Apple, presionar el botón de encendido durante 10" (diez segundos), con lo cual pasado ese lapso el mismo se apagara.

3.- Cuando se hallen periféricos de almacenamiento (discos externos, sistemas NAS, etc.) conectados a los equipos informáticos y se disponga su secuestro, se procederá del siguiente modo:
a) identificar con etiquetas numeradas los cables para indicar donde estaban conectados,
b) fotografiar los equipos con sus respectivos cables de conexión etiquetados.

4.- Tratándose de computadoras de escritorio solo secuestrar el Gabinete (CPU). Evitar el secuestro de elementos innecesarios, tales como dispositivos que no tengan algún tipo de memoria, cables de alimentación genéricos, cables usb de impresoras, monitores, scanners, teclados, mouses, parlantes, UPS, etc. Salvo caso que alguno de estos elementos tenga relación con el caso que se investiga.

5.- Los dispositivos que tienen capacidad de almacenamiento suelen contener información valiosa para la investigación, por ejemplo: Pendrives, Tarjetas de Memoria, Cámaras Digitales, GPS, Equipos DV-R, Celulares, Tablets, Notebooks, Netbooks, Discos Externos, etc.. En consecuencia es recomendable el secuestro y envío al Equipo Técnico Multidisciplinario para su análisis.-

6.- Precintar todos los equipos informáticos en sus entradas y todas las partes que pudieren ser movidas o extraídas.

7.- Usar bolsas especiales antiestáticas para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos. Si no se cuenta con este tipo de envoltorio, pueden utilizarse bolsas de papel madera. Evitar siempre el uso de bolsas plásticas, puesto que se corre el riesgo de generar una descarga de electricidad estática y destruir datos almacenados.

8.- **Equipos de telefonía celular**. En caso de secuestro proceder del siguiente modo:
a) si el mismo se encuentra apagado no encenderlo;
b) si se encuentra encendido no apagarlo. El apagarlo puede activar medidas de seguridad como la solicitud de PIN o PUK , activar sistemas de bloqueo del teléfono u otros sistemas mas complejos de bloqueo, encriptación o borrado masivo. Todo lo cual dificulta o imposibilita la pericia técnica.
c) Es recomendable individualizar el equipo por el número de identificación IMEI. Para obtenerlo:
1.- si el dispositivo se halla encendido digitar en el teclado *#06# para revelar el numero de identificación IMEI,
2.- si se encuentra apagado sacar esta identificación de la etiqueta que se encuentra en el interior del dispositivo en el compartimiento para la batería.

También anotar el "SIM card Number" ubicado en la parte superior de la "SIM card" oCHIP.

9.- Medidas de conservación de equipos de telefonía celular. Se sugiere:
a) de ser posible poner el celular en modo avión para el ahorro de energía,
b) utilizar bolsas especiales que aíslan el equipo de la red. De no contar con ellas utilizar bolsas de papel madera
c) colocar el equipo con un cargador especial, para incrementar su autonomía

10.- Los equipos de telefonía celular deben ser peritados de inmediato o en el mas breve lapso para evitar que se agote la fuente de alimentación y las consecuencias que de ellas se derivan descriptas en el pto.8 b.

11.- **Equipos DV-R** (equipos de grabación de cámaras de seguridad) el mismo debe ser secuestrado con su cable de alimentación y control remoto, si el equipo se encuentra funcionando y es factible, constatar y dejar mención en el acta si la fecha y la hora coinciden con la actual, de no ser así, dejar constancia del tiempo de discrepancia.