HONORABLE CÁMARA DE SENADORES

ENTRE RÍOS

LEY N° 10885

LA LEGISLATURA DE LA PROVINCIA DE ENTRE RÍOS SANCIONA CON FUERZA DE

LEY:

ARTÍCULO 1°.- La provincia de Entre Ríos, en lo que respecta a su competencia, dispone su adhesión a la Ley Nacional N° 27.411, por la cual se aprueba el CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, adoptado en la ciudad de BUDAPEST, HUNGRÍA, El 23 de noviembre de 2001.

ARTICULO 2°.- Apruébese los puntos 2.5 (2.5.1; 2.5.2; 2.5.3; 2.5.4) del capítulo sobre Recolección de Evidencias Digitales del "Protocolo Unificado de los Ministerios Públicos de la República Argentina: Guía para el Levantamiento y Conservación de la Evidencia" el que como ANEXO I forma parte de la presente.

ARTICULO 3°.- Comuníquese el contenido del documento mencionado en el artículo precedente al Superior Tribunal de Justicia de Entre Ríos y al Ministerio Público Fiscal de la provincia de Entre Ríos.

ARTÍCULO 4°.- Comuníquese, etcétera.

PARANÁ, SALA DE SESIONES, 7 de abril de 2021.

Dr. Ángel GIANO
Presidente H. C. de Diputados

Lic. María Laura STRATTA
Presidenta H. C. Senadores

Dr. Carlos SABOLDELLI
Secretario H. C. de Diputados

Dr. Lautaro SCHIAVONI
Secretario H. C. de Senadores

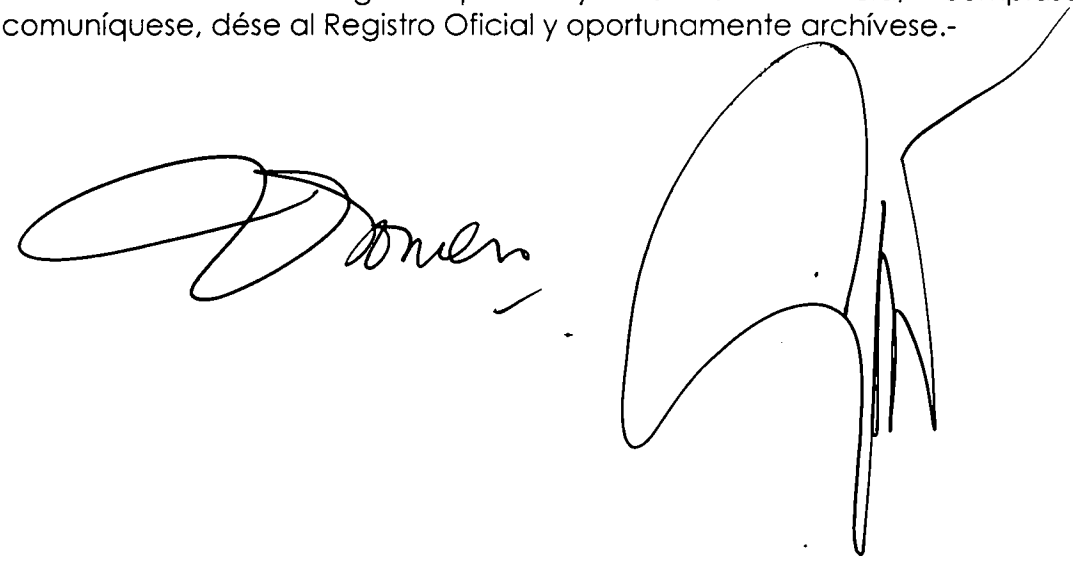
ES COPIA AUTENTICA

LEONARDO M CENTURIÓN
PROSECRETARIO
H. CÁMARA DE SENADORES
ENTRE RÍOS

PARANÁ, 16 ABR. 2021

POR TANTO:

Téngase por Ley de la Provincia, cúmplase, comuníquese, dése al Registro Oficial y oportunamente archívese.-



MINISTERIO DE GOBIERNO Y JUSTICIA 16 ABR. 2021

Registrada en la fecha bajo el N° 10885 .- CONSTE.-

ANEXO 1

Se anexa la parte pertinente del Protocolo unificado de los ministerios públicos de la República Argentina: guía para el levantamiento y conservación de la evidencia:

2.5. Evidencias digitales

2.5.1. Principios generales

Las evidencias digitales son elementos tecnológicos que pueden poseer información almacenada en formato digital, como PC, notebook, netbook, tablets, celulares, pendrive, CD, DVD, discos rígidos, servidores, etc. Para aquellas situaciones que involucren procedimientos judiciales en empresas o instituciones de gran envergadura a priori se procurará obtener información tendiente a conocer las características generales de la infraestructura tecnológica y hardware existente en el lugar del hecho. Las actividades operativas corresponden al personal policial y deben ser efectuadas siguiendo las indicaciones del presente protocolo. La actuación profesional del perito es, principalmente, una actividad de laboratorio y de asesoramiento científico al operador judicial que es responsable de la investigación penal. La pericia informática conlleva tiempos elevados de trabajo y no es posible realizarla sobre grandes cantidades de elementos. Debe evitarse el secuestro masivo de elementos informáticos, en especial CD y DVD, los que solo han de ser enviados a peritaje únicamente si se tienen presunciones con un alto grado de verosimilitud de poseer la evidencia buscada. Cabe aclarar que, de ser posible,

se sugiere realizar, previo al allanamiento, una investigación minuciosa con el objeto de identificar con precisión la ubicación y características técnicas generales de los elementos a secuestrar por medio de inteligencia policial. Respecto a la evidencia digital se deberá identificar claramente qué dispositivos móviles están en uso y a quiénes pertenecen, como así también los que se encontraron apagados, guardados o en aparente desuso. A continuación, se describen los principios generales para la recolección y embalaje de las evidencias digitales halladas en la escena del crimen.

1) Registrar lo que es visible en los dispositivos de salida como pantallas e impresoras y no intentar explorar los contenidos ni recuperar información de una computadora u otro dispositivo electrónico (cámara de fotos, celular, etc.) sin contar con los conocimientos técnicos para realizarlo.

2) No presionar cualquier tecla ni hacer clic del mouse.

3) Verificar si existen discos o CD puestos en unidades.

4) Identificar claramente qué dispositivos móviles están en uso y a quién pertenecen, dar cuenta también de los dispositivos que se encontraron apagados, guardados o en aparente desuso.

5) No encender si se encuentra apagado.

6) Dejar encendido hasta agotar batería.

7) Para apagar, desconectar el enchufe directamente de la red de energía, después desconectar el resto de cables, como la red de datos, monitores, etc.

8) No desarmar el equipo dejándolo sin batería. 9) No abrir la tapa de una computadora portátil si está cerrada.

10) Se realiza algún cambio, registrarlo y justificar.

11) Respetar el orden de volatilidad, estableciendo como criterio preservar la muestra más volátil al principio —como registros, cachés, memoria de periféricos, memoria (kernel, física), estado de las conexiones de red, procesos que se están ejecutando—.

12) Indicar si el material recolectado se encuentra contaminado con residuos biológicos o peligrosos de cualquier tipo.

2.5.2. Pasos en el lugar del hecho, escena del crimen o en allanamiento

1) Separar a las personas que trabajen sobre los equipos informáticos lo antes posible y no permitirles volver a utilizarlos. Si es una empresa, se debe identificar al personal informático interno (administradores de sistemas, programadores, etc.) o a los usuarios de aplicaciones específicas que deban someterse a peritaje. Dejar registrado el nombre del dueño o usuarios del equipamiento informático, ya que luego pueden ser de utilidad para la pericia.

2) Obtener, siempre que sea posible, las contraseñas y/o patrones de bloqueo de aplicaciones, tabletas, celulares, etc. para registrar.

3) Fotografiar todos los equipos informáticos antes de moverlos o desconectarlos. Esto es, fotografiar una toma completa del lugar donde se encuentren los equipos informáticos y de las pantallas de las computadoras, si están encendidas. Excepcionalmente, si se debiera inspeccionar los equipos informáticos o material tecnológico en el lugar del hecho, puede ser

conveniente realizar una filmación o bien una descripción del trabajo que se lleva a cabo ante los testigos.

4) Levantar el material informático con guantes descartables, ya que el teclado, monitores, mouse, CD, DVD, etc., pueden ser utilizados para análisis de huellas dactilares, ADN, etc.

5) Si los equipos están apagados, deben quedar apagados; si están prendidos, deben quedar prendidos y consultar con un especialista la modalidad de apagado (en caso de no contar con asesoramiento, proceder a apagarlos desenchufando el cable de corriente desde el extremo que conecta al gabinete informático). Si los equipos están apagados, desconectarlos desde su respectiva toma eléctrica y no del enchufe de la pared. Si son notebooks o netbooks, es necesario quitarles la o las baterías y proceder a secuestrar los cables y la fuente de alimentación. Para el caso de celulares, retirar la batería. En caso de no poder extraer la batería, apagarlo y proteger el botón de encendido con un cartón pegado con cinta para evitar el encendido accidental. Como medida extra de seguridad, se puede activar el "modo avión" antes de apagarlo.

6) De ser necesario, dejar el dispositivo encendido por algún requerimiento específico —por ejemplo: para no perder información volátil colocarlo en una bolsa de Faraday o envolverlo con, al menos, tres capas de papel aluminio—.

7) Identificar si existen equipos que estén conectados a una línea telefónica y, en su caso, el número telefónico para registrarlo en el acta de allanamiento.

8) No realizar búsquedas sobre directorios ni ver la información almacenada en los dispositivos, ya que es posible que se altere y destruya evidencia digital (esto incluye intentar hacer una "copia" sin tener software forense específico y sin que quede documentado en el expediente judicial el procedimiento realizado).

9) Identificar correctamente todo el material tecnológico a secuestrar:

a) Siempre debe preferirse secuestrar únicamente los dispositivos informáticos que almacenan grandes volúmenes de información digital (computadoras, notebooks y discos rígidos externos). Respecto a DVD, CD, pendrives, etc., atento a que pueden encontrarse cantidades importantes, debe evitarse el secuestro de este material si no se tiene una fuerte presunción de hallar la evidencia en estos medios de almacenamiento.

b) Rotular el hardware que se va a secuestrar con los siguientes datos:

i) Para computadoras, notebooks, netbooks, celulares, cámaras digitales, etc.: número del expediente judicial, fecha y hora, número de serie, fabricante, modelo.

ii) Para DVD, CD, pendrives, etc.: almacenarlos en conjunto en un sobre antiestático, indicando número del expediente judicial, tipo (DVD, CD, pendrives, etc.) y cantidad.

c) Cuando haya periféricos muy específicos conectados a los equipos informáticos y se deban secuestrar, deben identificarse con etiquetas con números los cables para indicar dónde se deben conectar. Así como también, fotografiar los equipos con sus respectivos cables de conexión etiquetados.

2.5.3. Registros activos y volátiles de las PC, netbooks y notebooks

Estado de la memoria RAM	Capacidad de los programas cargados. Bloqueos. Porcentaje de uso		
Procesos activos	Uso de CPU. Dependencias de procesos y componentes		
Conexiones de red	Conexiones actuales con otras PC y servidores	Identificación de elementos con respaldo de impresiones, fotografías y actas	No instalar programas en las PC. Realizar las operaciones con los equipos encendidos y cables conectados
Impresiones activas	Cola de impresión local. Documentos sin imprimir. Estado y descripción de los documentos que se están imprimiendo		
Fecha y hora del sistema operativo	Fecha y hora del sistema operativo. Zona horaria. Sincronizaciones con servidores de hora en Internet		
Red de la empresa u organización	Características. Tráfico. Congestión. Bloqueos. Snifers activos. Virus de red		
Papeles impresos	Recolección de papeles impresos en el lugar	Identificación de elementos con respaldo de fotografías y actas	
Conexiones físicas de red	Cableados existentes. Hubs. Suitchs	Identificación de elementos con respaldo de fotografías y actas	No desconectar hasta tanto se recolecte y documente la evidencia

2.5.4. Medios de almacenamiento

Discos duros de PC	Descripción del gabinete en el cual está contenido (marca, color, número de serie). Marca y número de serie. Capacidad	Rotulado. Embalaje en bolsas especiales tipo Faraday o en sobres de papel madera. Precinto de seguridad. Identificación de elementos con respaldo de impresiones, fotografías y actas	Capturar datos volátiles antes de apagar
Discos duros externos	Marca y número de serie. Capacidad		
Pendrives, CD, DVD, disquetes, otros dispositivos similares	Marca. Capacidad. Color		
Netbooks, notebooks, tablets			
Cámaras fotográficas, celulares, mp3, mp4, ipods			

Fuente: Protocolo unificado de los ministerios públicos de la República Argentina: guía para el levantamiento y conservación de la evidencia / Anónimo. - 1a ed . - Ciudad Autónoma de Buenos Aires: Ediciones SAIJ, 2017. Libro digital, EPUB.