Ministerio de Seguridad

BUENOS AIRES,

VISTO el Expediente CUDAP: EXP-SEG: N° 0003372 /2016, las Leyes Nº 26.388 del 25 de junio de 2008, y Nº 26.904 del 11 de diciembre de 2013 y,

CONSIDERANDO

Que en el marco de la lucha contra el narcotráfico y el crimen organizado que ha asumido este gobierno resulta menester realizar todos los esfuerzos y contar con los elementos necesarios para lograr una mayor eficiencia y eficacia.

Que a nivel mundial ha tomado gran relevancia el fenómeno de la cibercriminalidad teniendo ésta una gran relación con el crimen organizado, en especial el narcotráfico, la pornografía infantil, los delitos sexuales y la venta ilegal de armas entre otros.

Que el incremento de los delitos cometidos a través de las nuevas Tecnologías de la Información y Comunicaciones (TICs) en la última década deviene en una necesidad de capacitar y dotar a las Fuerzas de Seguridad y Policiales con herramientas, métodos y procedimientos a fin de mejorar su investigación y conservar la prueba digital.

Que los delitos informáticos o ciberdelitos son actividades delictivas en donde las TICs se utilizan como medio para la comisión (estafas, extorsiones, corrupción de menores, etc.), o bien, son objetos del delito (acceso ilegítimo a sistemas o datos restringidos, daño informático, denegación de servicios, etc.).

Que los llamados ciberdelitos se encuentran contemplados en la Ley Nº 26.388 sancionada en junio del año 2008 y el delito de *grooming* fue incorporado al Código Penal de la Nación por la ley Nº 26.904 en el año 2013.

Que el anonimato que provee la utilización de Internet y las redes sociales dificulta la persecución de los delitos cibernéticos.

Que la prueba digital se diferencia de la prueba tradicional por su volatilidad, la capacidad de duplicación de la misma, la facilidad para alterarla y la cantidad de metadatos que posee.

Que la investigación de la delincuencia informática se dificulta debido a la intangibilidad y volatilidad de la evidencia digital, por lo que su adecuada preservación es fundamental para que las mismas sean admitidas judicialmente.

Que la prueba digital, en su estado natural, no permite entrever qué información es la que contiene en su interior, por lo que resulta para ello ineludible, examinarla a través de instrumentos y procesos forenses específicos.

Que la prueba digital es fundamental para la investigación por la información y datos de valor que pueden extraerse de los distintos dispositivos electrónicos, tanto aquellos aportados por el denunciante como los que se encuentren en el lugar de allanamiento.

Que dicha prueba puede ser en ciertos delitos de extrema preponderancia y en algunos casos, la única evidencia que se puede obtener para el esclarecimiento del delito investigado.

Que la adecuada obtención, conservación y tratamiento de la evidencia digital es un elemento clave para asegurar el éxito de las investigaciones.

Que las Fuerzas de Seguridad y Policiales deben estar capacitadas para operar con prueba digital teniendo en cuenta su fragilidad ya que las altas temperaturas, la humedad y cualquier error en su manejo puede acarrear la destrucción de la misma.

Que incluso el valor de las pruebas obtenidas con el mayor esmero puede perderse si no se respeta debidamente la cadena de custodia, las precauciones especiales al momento de recolectar, manipular, documentar y examinar la evidencia digital ya que de no hacerlo, podrían generarse nulidades judiciales o resultar imprecisa a efectos de esclarecer el hecho delictivo.

Que es necesario asistir y capacitar a las Fuerzas de Seguridad y Policiales dado que son las encargadas de auxiliar en la investigación de estos delitos, y que dicha investigación requiere de una experiencia, herramientas y actuación distinta que en los delitos convencionales.

Que es fundamental que las Fuerzas de Seguridad y Policiales sean capaces de reconocer qué tipo de dispositivos pueden contener información vital para la investigación del delito para su posterior secuestro.

Que resulta necesario que se trabaje mancomunadamente con Organizaciones No Gubernamentales que tienen finalidad de prevención y erradicación de delitos como el Grooming, siendo estas una fuente de datos importantes, por su rol protagónico frente delitos de esta índole.

Que el presente protocolo tiene por objeto concientizar sobre las prácticas a seguir en la investigación del delito estableciendo los principios a tener en cuenta al momento de la investigación, además de abarcar la índole, pertinencia, modo de obtención, conservación y tratamiento de las evidencias digitales, desde la actuación de los agentes de prevención hasta la entrega de las mismas para su análisis;

Que además, pretende que los agentes de las Fuerzas Policiales y de Seguridad, comprendan la importancia de su labor y las consecuencias que se generan al no aplicar los principios que aquí establecidos.

Ministerio de Seguridad

Que la SUBSECRETARÍA DE ASUNTOS JURÍDICOS ha tomado la intervención de su competencia.

Por ello,

LA MINISTRA DE SEGURIDAD

RESUELVE:

ARTÍCULO 1°.- Apruébese el "PROTOCOLO GENERAL DE ACTUACIÓN PARA LAS FUERZAS POLICIALES Y DE SEGURIDAD EN LA INVESTIGACIÓN Y PROCESO DE RECOLECCIÓN DE PRUEBAS EN CIBERDELITOS" que, como ANEXO forma parte integrante de la presente resolución.

ARTÍCULO 2°.- Invítese a las Provincias y a la CIUDAD AUTÓNOMA DE BUENOS AIRES a adherir al presente Protocolo.

ARTÍCULO 3°.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

RESOLUCION N°:

Ministerio de Seguridad

ANEXO

PROTOCOLO GENERAL DE ACTUACIÓN PARA LAS FUERZAS POLICIALES Y DE SEGURIDAD EN LA INVESTIGACIÓN Y PROCESO DE RECOLECCIÓN DE PRUEBAS EN CIBERDELITOS.

I. REGLAS GENERALES, DEFINICIONES Y PRINCIPIOS

1. Objeto: El presente PROTOCOLO GENERAL DE ACTUACIÓN (en adelante "PGA") tiene por objeto establecer las pautas y el procedimiento al que deberán atenerse los miembros de las Fuerzas Policiales y de Seguridad al momento de la investigación y proceso de recolección de pruebas en el marco de los ciberdelitos y en especial en el delito de *grooming* contemplado en el artículo 131 del Código Penal de la Nación.

2. Generalidades: El presente PGA es de aplicación obligatoria en todo el país para todo el personal de GENDARMERÍA NACIONAL ARGENTINA, PREFECTURA NAVAL ARGENTINA, POLICÍA FEDERAL ARGENTINA Y POLICÍA DE SEGURIDAD AEROPORTUARIA, debiéndose tener en cuenta que su accionar debe ajustarse en un todo a la Constitución Nacional, las leyes penales, las pautas procesales y los protocolos vigentes.

3. Definiciones: A los fines del presente PGA se entiende por:

3.1 Ciberdelito: todo delito en donde las Tecnologías de la Información y las Comunicaciones (TICs) sean utilizadas como medio para la comisión del mismo o bien sean el objeto.

3.2 *Grooming*: delito que se configura cuando por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, se contac-

ta a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

3.3 Copia Forense: réplica en forma completa (por sector, bit a bit) de la estructura y contenido de un dispositivo de almacenamiento. Se conecta un dispositivo externo al dispositivo y se hace la copia idéntica. Puede realizarse por medio de un copiador de hardware o un software.

3.4 Hash: es una función matemática que permite representar datos de longitud variable como un dato de longitud fija y donde pequeñas diferencias en los datos de entrada generan una gran diferencia en los datos de salida. Los valores resultados también se denominan hash (singular) o hashes y permiten identificar con gran nivel de precisión los datos originales, sin revelar el contenido real de los mismos a través de una función unidireccional. Tiene como funciones primordiales la identificación y el control de la integridad de los datos, resultando de vital importancia a los fines de controlar la preservación de la cadena de custodia y evitar planteos de nulidad.

3.5 Evidencia digital: es la prueba fundamental en los ciberdelitos. Información y datos de valor en una investigación que se encuentra almacenada, es recibida o transmitida por un dispositivo electrónico. Dicha prueba se adquiere cuando se secuestra y asegura para su posterior examen. Normalmente las pruebas consisten en archivos digitales de texto, vídeo o imagen, que se localizan en ordenadores y todo tipo de dispositivos electrónicos.

3.6 Allanamiento: es el acto procesal que implica el ingreso a un domicilio, recinto de acceso restringido u otro lugar dentro del marco de una investigación criminal, consistente en el registro del mismo. Este acto se realiza mediante el uso de la fuerza pública en horario hábil y con las excepciones horarias que autoriza la ley, procurando minimi-

zar los riesgos a la integridad física de la totalidad de los actores y procurando la preservación de los medios de prueba buscados.

3.7 Requisa Personal: es una medida procesal de coerción real por medio de la cual se procura examinar el cuerpo de una persona y las cosas que lleva en sí, consigo, dentro de su ámbito personal o en vehículos, aeronaves o buques, con la finalidad de proceder a su secuestro o inspección por estar relacionadas con un delito.

3.8 Secuestro: es una medida procesal por el cual se procede a la retención de lo que se hallare en virtud de un allanamiento o de una requisa personal dejando constancia de ello en el acta respectiva y dando cuenta inmediata del procedimiento realizado al juez o fiscal intervinientes.

Los elementos de prueba serán recolectados según las reglas aplicables al tipo de objeto, garantizando la cadena de custodia

3.9 Cadena de Custodia: es el control que se efectúa tanto de las personas que recogen la evidencia como de cada persona o entidad que posteriormente tiene la custodia de la misma. La cadena de custodia debe contener un identificador unívoco de la evidencia, de las fechas en las que los artículos fueron recogidos o transferidos, datos sobre el responsable que realizó la recolección, datos sobre la persona que recibe la evidencia y los datos de las personas que acceden, el momento y la ubicación física, número del caso, y una breve descripción de cada elemento. El pasaje de la evidencia de un sitio a otro y las tareas realizadas, cualquier cambio inevitable potencial en evidencia digital será registrado con el nombre del responsable y la justificación de sus acciones. El objetivo de la cadena de custodia es garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso.

3.10 Dirección IP: La dirección IP, acrónimo para Internet Protocolo, es un número único e irrepetible con el cual se puede identificar el acceso a internet de cualquier dispositivo con conectividad.

II. PRINCIPIOS GENERALES DE INTERVENCIÓN

1. Accesibilidad y respeto: Los agentes de las Fuerzas Policiales y de Seguridad están obligados a tratar a la víctima con absoluto respeto por sus derechos y garantías constitucionales, otorgándole especial atención y seguridad al tratarse de víctimas en situación de vulnerabilidad y sensibilidad.

2. Interés superior del niño: Cuando se trate de víctimas menores de 18 años, el vector de actuación de las Fuerzas Policiales y de Seguridad debe velar siempre por el interés superior del niño.

Por interés superior del niño se entenderá al conjunto de acciones y procesos tendientes a garantizar un desarrollo integral y una vida digna, así como las condiciones materiales y afectivas que les permitan vivir plenamente y alcanzar el máximo de bienestar posible.

3. Confidencialidad y privacidad: En todo momento, debe respetarse la privacidad de la víctima, no pudiendo dar publicidad de sus circunstancias personales, declaraciones y/o fotografías.

III. PRINCIPIOS ESPECÍFICOS DE INTERVENCIÓN

1. Recolección, Aseguramiento y Transporte: Los procesos de recolección, aseguramiento y transporte de la prueba no pueden en ningún caso modificar la original.

2. Examen por Expertos: La evidencia digital sólo debe ser examinada y analizada por personal idóneo, entrenado y capacitado para ese propósito.

3. Documentación de las Actuaciones: Todo lo actuado durante el proceso de recolección, transporte y almacenamiento de la prueba tiene que estar completamente documentado, preservado y disponible para un posterior examen.

4. Prevención: A los fines de la investigación de los ciberdelitos alcanzados por el presente protocolo las Fuerzas Policiales y de Seguridad podrán hacer y solicitar el uso de las técnicas de investigación establecidas en los Códigos de Fondo, Procedimentales y leyes especiales de la jurisdicción correspondiente, .

IV. PAUTAS ESPECÍFICAS DE ACTUACIÓN

1. Denuncia

1.1 Recepción : Las denuncias en materia de ciberdelitos, deben cumplir con lo establecido en el Código Procesal Penal de la Nación, los Códigos Procesales de cada provincia y de la CIUDAD AUTÓNOMA DE BUENOS AIRES, en cuanto a su recepción, forma, contenido.

La denuncia puede ser receptada por cualquiera de los canales de recepción de denuncias existentes siguiendo el procedimiento normal para el trámite de la misma.

Respecto de la comunicación y procedimiento de la denuncia, las Fuerzas Policiales y de Seguridad deberán incluir obligatoriamente:

A) Lugar y fecha en que fueron iniciadas.

B) Los datos personales de quienes en ellas intervinieron.

C) Las declaraciones recibidas, los informes que se hubieran producido y el resultado de todas las diligencias practicadas.

Recibida la denuncia por cualquiera de los canales existentes, los miembros de las Fuerzas Policiales y de Seguridad deberán comunicar de inmediato al Ministerio Pú-

blico Fiscal quienes a su vez, pondrán en conocimiento la denuncia en caso de tratarse del delito de grooming o pornografía infantil a la "Red 24/7".

Al momento de la recepción de la denuncia los miembros de las Fuerzas Policiales y de Seguridad deben procurar el aseguramiento de la prueba aportada por el denunciante o solicitar la misma, la cual podrá verse contenida en correos electrónicos, dispositivos electrónicos tales como computadoras, dispositivos móviles, chats de mensajería instantánea, redes sociales, páginas de internet, etc.

La conservación de la prueba por parte del denunciante consiste en el almacenamiento de las conversaciones, mensajes, imágenes, videos y cualquier otra prueba que se relacione con el hecho. Es necesaria su custodia y cuidado conforme las reglas establecidas en el presente Protocolo, a fin de que queden a disposición de la Justicia.

Si la misma consiste en correos electrónicos, se deben guardar los mismos o ser reenviados a una casilla oficial como archivo adjunto. La impresión en papel de los mismos impide rastrear el remitente original del material probatorio.

Si la prueba se encuentra almacenada en un dispositivo de telefonía celular, quien reciba la denuncia deberá tomar los recaudos necesarios para que un informático forense realice una copia forense del dispositivo móvil para su análisis y posterior estudio.

Es imprescindible que si el material probatorio se encuentra en páginas de internet, redes sociales, etc. se solicite inmediatamente a los responsables la preservación de la evidencia digital allí contenida hasta tanto se obtenga la orden judicial pertinente.

1.2 Denuncia realizada por víctima menor de edad: En el caso que las víctimas de un ciberdelito sean menores de edad, deberán ser interrogadas por un psicólogo especialista en niños, niñas y adolescentes.

El interrogatorio se realizará en un ambiente acondicionado a la edad y la etapa evolutiva del menor, contando con el equipamiento e implementos que sean necesarios.

En el tratamiento de las víctimas, debe evitarse cualquier conducta o actitud que tienda a la re-victimización de las mismas.

La re-victimización tiene lugar cuando a los daños que sufre una persona como consecuencia del delito del que fue víctima se suman aquellos generados por el proceso legal. Para evitar esto, no se debe juzgar y/o inferir algún grado de responsabilidad por parte de la misma. Es decir, a los daños causados a la víctima por los delitos de los que fue objeto, no se le debe sumar el maltrato institucional.

2. Allanamiento

2.1 Reglas Generales y Cuestiones Preliminares: Previo a la práctica de la diligencia procesal, las Fuerzas Policiales y de Seguridad deberán realizar investigaciones preliminares a fin de identificar la dirección IP, números de teléfonos celulares de los dispositivos electrónicos que se utilicen para la comisión del delito denunciado y, principalmente, al supuesto autor del delito objeto de la investigación.

Identificado el presunto autor, se procurará practicar el allanamiento previendo la presencia del mismo en el lugar, para así poder practicar requisas y secuestro de los elementos que éste tenga encima, siempre y cuando la orden del juez lo contemple.

2.2 Procedimiento: El allanamiento debe ser practicado de acuerdo a lo establecido en el Código Procesal Penal de la Nación, los Códigos Procesales correspondientes a cada una de las provincias y la CIUDAD AUTÓNOMA DE BUENOS AIRES.

Una vez dentro del lugar objeto del allanamiento, los agentes deberán visualizar la escena y fotografiar el estado en el que se encuentra, dándole especial relevancia a los dispositivos electrónicos que estén a la vista y cualquier otra anotación que pudiera re-

sultar útil al momento de analizar la evidencia recolectada en el lugar. Deberán reconocer e identificar todos los dispositivos que se encuentran en la escena. Realizado esto, deberán documentar toda la escena especificando el lugar exacto donde se encontraron los dispositivos, el estado en el que se encontraron y el tipo de dispositivo por la relevancia que éstos datos tendrán al momento de reconstruir la escena y se haga la extracción de la prueba digital.

Se deberá poner especial atención en intentar determinar quién o quiénes son los usuarios de los dispositivos.

El personal que manipule la evidencia digital deberá estar especialmente capacitado y entrenado para dicho propósito y deberá utilizar para la recolección guantes de látex, cajas de cartón y bolsas de papel o plásticas según corresponda, debidamente selladas para la recolección de los objetos secuestrados. De esta manera, se evita la contaminación de la posible prueba biológica (ADN, huellas digitales en teclados, mouse etc.) que pueda encontrarse en dichos dispositivos.

Es importante que se registre la marca, modelo y números de serie, así como también cualquier otro tipo de dato de identificación de la computadora y demás dispositivos encontrados en la escena.

2.3 Objetos Susceptibles de Secuestro:

A) Computadoras: Gabinetes, motherboards, microprocesadores, discos rígidos, tarjetas de memoria, laptops, baterías.

B) Dispositivos periféricos: Hardware que puede ser conectado a una computadora para mejorar y expandir las funciones de la máquina: Monitores, teclados, parlantes, discos externos, mouse, módems, routers, impresoras, escáners, faxes, micrófonos.

Estos son importantes dados que contienen pruebas biológicas (ADN, huellas digitales…), así como también documentos recientemente escaneados, números entrantes y salientes de fax.

C) Dispositivos de almacenamiento de datos: Disquetes, CD, DVD, Pendrives (pueden estar conectados a la computadora, venir en diferentes tamaños y formas, estar disfrazados u ocultos dentro de otros objetos), Tarjetas de memoria, Micro SD, Discos rígidos, Discos externos.

D) Dispositivos de mano: Celulares, smartphones, tablets, GPS, videocámaras, equipos de vigilancia, consolas de video juegos.

E) Cualquier otro dispositivo que pueda ser susceptible de contener evidencia digital. *Potencial prueba que pueden contener:* Documentos, imágenes, fotos, emails, bases de datos, información financiera, historial de navegación, log de los chats, discos externos, geo localización.

2.4 Pautas Generales

Los agentes que actúen en el allanamiento deberán:

A) Fotografiar el estado en el que se encuentra el dispositivo y documentar, el estado en el que se lo encontró y el estado en el que se secuestra en caso que haya habido un cambio en la pantalla del dispositivo.

B) Documentar, fotografiar y hacer un esquema de todos los cables y otros dispositivos que estén conectados a la computadora.

C) Desconectar y etiquetar el cable de suministro y los demás cables, alambres o dispositivos USB conectados a la computadora.

D) No encender nunca un equipo apagado y si está encendido no apagarlo inmediatamente para evitar la pérdida de información volátil, dependiendo si es necesario para el caso realizar la adquisición de memoria volátil en el lugar del hecho.

E) No desconectar el equipo si el mismo es una estación de trabajo o servidor (conectado en red) o está en un negocio. El desconectarla puede acarrear daño permanente al equipo. Anotar los números de conexión IP y consultar con un técnico experto en redes.

F) Documentar la existencia de cámaras web y si éstas se encuentran activas.

G) Cuando se tengan dudas acerca de si un dispositivo electrónico se encuentra encendido o apagado, mirar y escuchar si existe algún sonido o luz que indique que se encuentra encendido, como ser el ruido de los ventiladores, o las luces led del gabinete si se trata de una computadora.

H) Verificar lo que muestra la pantalla del dispositivo para detectar si se está accediendo a ella remotamente o bien si la información en ella está siendo destruida. Buscar palabras claves tales como borrando, moviendo, limpiando.

I) Buscar señales de actividad de comunicación con otro dispositivo o usuarios a través de ventanas emergentes de chats, de mensajería instantánea, etc.

2.5 Procedimientos especiales

A) Computadora de Escritorio

i) Si el monitor está prendido sacarle una fotografía a la pantalla y anotar la información que se ve.

ii) Si el monitor está prendido pero se ve el protector de pantalla, mover ligeramente el mouse sin tocar ningún botón ni mover la rueda. Fotografiar el estado en el que se encontró, anotando y fotografiando lo que aparece posteriormente.

iii) Si el monitor está apagado pero el gabinete está encendido, prender el monitor, fotografiar la pantalla y registrar la información que aparezca.

iv) Si el monitor está prendido pero la pantalla está en blanco como si estuviese apagada, mover ligeramente el mouse sin tocar ningún botón ni mover la rueda. En el caso que aparezca la pantalla, anotar el cambio de la pantalla, registrar la información y fotografiar el antes y después. Si la pantalla no aparece, confirmar que el gabinete se encuentre encendido, de lo contrario la computadora está apagada. Fotografiar y de ser posible, filmar la escena y documentar el estado en el que se encuentra.

B) Laptop o computadora portátil: Remover el cable de alimentación, localice y remueva la batería, la cual por lo general se localiza debajo del equipo. Seguir los mismos pasos que si se trata de una computadora de escritorio.

C) Dispositivos móviles y celulares:

i) Si el aparato está encendido, no lo apague. Si el aparato está apagado, déjelo apagado.

ii) Si lo apaga puede iniciarse el bloqueo del aparato. Transcribir toda la información que aparece en la pantalla y fotografiar el estado en el que se encontró y lo que apareció luego en la pantalla.

iii) Revisar los dispositivos de almacenamiento removibles. (Algunos aparatos contienen en su interior dispositivos de almacenamiento removibles tales como Tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.)

2.6 Embalaje, Transporte y Almacenamiento

A) Embalaje: Tener en cuenta que la prueba digital es frágil y sensible a altas temperaturas, humedad, electricidad estática y campos magnéticos.

i) Embalar toda la evidencia digital en bolsas antiestáticas. Solo utilizar bolsas de papel, sobres o cajas de cartón. No deben utilizarse materiales plásticos ya que pueden producir electricidad estática, lo que hace que penetre la humedad.

ii) Todo lo que pertenezca a una misma computadora será identificado (etiquetado), embalado y transportado en su conjunto, para evitar que se mezcle con las partes de otros dispositivos y poder luego reconfigurar el sistema.

iii) Fajar con fajas de papel y pegamento los puertos y todas las entradas. Sellar cada entrada o puerto de información, tornillos del sistema de manera que no se puedan remover o reemplazar las piezas internas del mismo con cinta de evidencia. Asegurarse que las bandejas de CD o DVD estén cerradas y anotar si estaban vacías o no y fajarlos con cinta adhesiva.

iv) Desconectar el cable de suministro.

v) Guardar las baterías de forma separada al equipo.

vi) Embalar toda la evidencia teniendo cuidado de no dañar ni alterar nada durante el transporte y almacenamiento.

B) Transporte: Documentar quiénes participaron del empaquetamiento y transporte para registrar la cadena de custodia.

Mantener la prueba alejada de campos magnéticos como transmisores de radios, parlantes.

Evitar mantener la prueba por tiempo prolongado en el vehículo que la transporte.

C) Almacenamiento:

i) Inventariar correctamente toda la prueba.

ii) Almacenarla en un ambiente seguro y con un clima controlado para evitar altas temperaturas y humedad.

iii) Asegurarse que no esté expuesta a campos magnéticos, humedad, polvo, vibración u otros elementos que puedan dañarla o destruirla.

iv) Si se secuestró más de una computadora, almacenar cada una con sus respectivos cables y dispositivos electrónicos por separado.

3. Extracción de la Prueba: Una parte es extraída mediante procedimientos forenses de la propia terminal de la víctima y de los elementos secuestrados.

Otra es facilitada por los proveedores del servicio de Internet, quienes son depositarios de la mayoría de los datos de tráfico válidos para la investigación. Para poder acceder a esta información se requiere de una autorización judicial.

No se debe trabajar con la prueba original si no realizar una copia forense del dispositivo.

En el caso de trabajar con computadoras, se debe realizar primero una copia del disco duro, y luego precintarlo debidamente.

La copia forense puede realizarse por medio de un copiador de hardware o un software.

Es obligatorio para este procedimiento:

A) Utilizar un bloqueador de escritura al momento de realizar la copia forense ya que este dispositivo permite operar la computadora asegurando que no se modifique absolutamente la más mínima información, por ejemplo, nos restringirá la mera lectura y copiado de los archivos.

B) Por otro lado, una vez finalizado el copiado, el agente debe realizar el cálculo hash de dicha copia forense.

3.1 Procedimiento: Se recomienda hacer dos copias por cualquier eventualidad. Asegurarse que la copia es exacta al original y que durante el proceso del mismo el original permanezca inalterado.

Obtener un código (hash) que identifique al disco y corroborar que el mismo sea igual al código de la copia. Por lo tanto, ante el mínimo cambio tanto en el original como en la copia, se daría como resultado un código distinto.

3.2 Potencial Prueba Extraíble:

A) Registros de chats y blogs

B) Software de reproducción, captura y edición de video

C) Imágenes y videos de contenido sexual

D) Juegos infantiles o de contenido sexual

E) Registros de actividad en internet

F) Directorios de archivos encriptados o no visibles mediante los cuales clasifica el contenido de las distintas víctimas.

G) Correos electrónicos, notas y cartas varias

H) Papeles con contraseñas anotadas, notas, manuales de hardware y software, calendarios, material pornográfico, DVD, CD, Disquetes, etc.

3.3 Cadena de Custodia. La cadena de custodia debe contener:

A) una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, identificación del encargado de custodia, identificaciones, cargo, y firmas de quien recibe y quien entrega.

B) Rótulos que van pegados a los envases de la prueba.

C) Etiquetas con la misma información de los rótulos que van atadas con cuerda al paquete de la prueba que corresponda.

D) Libros de registros de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios.

4. Capacitaciones

El MINISTERIO DE SEGURIDAD se compromete a realizar capacitaciones para los agentes de la POLICÍA FEDERAL ARGENTINA, GENDARMERÍA NACIONAL, PREFECTURA NAVAL, Y POLICÍA DE SEGURIDAD AEROPORTUARIA en temas vinculados a los ciberdelitos y la investigación y prevención de los mismos, mediante el dictado de cursos, talleres y seminarios diseñados a tal fin.

El contenido y programa de las capacitaciones versará sobre definiciones, lineamientos, protocolos de actuación, herramientas de investigación de los delitos y tratamiento de las víctimas. Dicho contenido será establecido por el Ministerio.