80

COLECCIÓN CRIMINALÍSTICA

5

Manual básico de **cateo y aseguramiento de evidencia digital**

Gabriel Andrés Cámpoli

Instituto Nacional de Ciencias Penales

Gabriel Andrés Cámpoli

Es Abogado por la Universidad Nacional de la Patagónica *San Juan Bosco* (Provincia del Chubut, Argentina).

Cuenta con especializaciones en: Contratos Telemáticos, Contratos informáticos y Régimen Jurídico de los Bancos de Datos (Universidad de Buenos Aires, Argentina) y Propiedad Intelectual en la Sociedad de la Información (Universidad de Castilla-La Mancha, Toledo, España).

Fue conferencista en el primer Congreso Mundial de Derecho Informático (Quito, Ecuador, Octubre de 2001) y coautor del libro *Propiedad Intelectual en Internet* (editado por la Universidad de Curitiba, Brasil).

Es autor de los libros *Derecho Penal Informático en México*, INACIPE, 2004 y *Delitos informáticos en la legislación mexicana*, INACIPE, 2005; de diversos artículos de la Revista *Iter Criminis* y del libro *La firma electrónica en el régimen comercial mexicano*, Porrúa, 2004.

En el área docente, se ha desempeñado en el Consejo de la Judicatura Federal (México, D.F.) y en el diplomado Derecho y nuevas Tecnologías (ITAM, México), entre otros.

Ha sido profesor de los cursos del INACIPE sobre Cibercriminalidad, Prevención de la Cibercriminalidad en el sector financiero, del Diplomado de Delitos Fiscales y Financieros, Delincuentes Informáticos y Lavado de Dinero por medios electrónicos. Actualmente es investigador del INACIPE.

Fotografía y diseño: Francisco Javier Quintanilla

Manual Básico de Cateo y Aseguramiento de Evidencia Digital

Instituto Nacional de Ciencias Penales
México, 2006

Manual Básico de Cateo y Aseguramiento de Evidencia Digital

Publicado por el Instituto Nacional de Ciencias Penales
Magisterio Nacional núm. 113, Col. Tlalpan
Delegación Tlalpan
C.P. 14000, México, D.F.

ISBN: 970-768-077-6

Edición y distribución a cargo
del Instituto Nacional de Ciencias Penales

Impreso y hecho en México
Made and printed in Mexico

http//:www.inacipe.gob.mx
Correo electrónico (e-mail): publicaciones@inacipe.gob.mx

Manual Básico de Cateo y Aseguramiento de Evidencia Digital

México, 2006

DIRECTORIO

Eduardo Medina Mora
Procurador General de la República y Presidente de la H. Junta de Gobierno del INACIPE

Gerardo Laveaga
Director General del INACIPE

Álvaro Vizcaíno Zamora
Secretario General Académico

Rafael Ruiz Mena
Secretario General de Profesionalización y Extensión

Karmen Thereza Silva Fajardo
Directora de Publicaciones

Contenido

Introducción

El presente manual tiene la finalidad de servir como una guía de las acciones y mecanismos mínimos a aplicar durante el cateo o aseguramiento de los equipos electrónicos que se hallen en la escena del crimen a fin de que la evidencia que de ellos surja, luego de realizar las pruebas periciales y medidas de investigación que para cada caso se crean convenientes, se pueda utilizar en la averiguación previa para descubrir o formar los elementos del delito o conocer la identidad del sujeto activo. Luego, en su caso, aportar la evidencia al proceso penal a fin de obtener la condena del inculpado sin sufrir las consecuencias de la nulidad de las pruebas o su simple inadmisibilidad en juicio por no llevar los recaudos necesarios que la ley y la Constitución de los Estados Unidos Mexicanos requiere para que se respeten las garantías del debido proceso penal.

La evidencia digital es muy frágil y puede perderse o modificarse con demasiada facilidad, aun por la simple inacción de quien tiene a su cargo el cateo o aseguramiento de los bienes, lo que implica la utilización de medidas especiales para su conservación en estado original para poder ser aportada como prueba válida en cualquier proceso penal.

---

* N.E. Una versión preliminar de este manual se publicó, en octubre de 2006, en la página Web de la revista de derecho informático Alfa Redi. (<http://www.alfa-redi.org/rdi-articulo.shtml?x=7693>).

La verdad es que un mal aseguramiento de los bienes electrónicos (prefiero esa terminología por ser más abierta que informático) produce, al poco tiempo, una disminución de la credibilidad en el sistema pero sobre todo, una alta tasa de impunidad basada en sentencias contrarias que nacen del principio conocido como "los frutos del árbol de raíces amargas o de raíces envenenadas".

Principio del árbol de raíces envenenadas

El principio utilizado en Derecho Penal, y sobre todo en Derecho Procesal Penal, indica por comparación que un árbol que adquiere un veneno por sus raíces, lo distribuirá a su tronco, sus ramas, sus flores e incluso sus frutos, que a la larga resultan también envenenados por la distribución interna de la savia, cuya función es la de llevar a todo el conjunto vegetal los nutrientes y demás compuestos que ingresan por la raíz.

Este ejemplo asume que un proceso penal es como un árbol cuya raíz contiene las primeras aportaciones o indicios probatorios. Luego crece su tronco, que equivaldría a la averiguación previa y las declaraciones iniciales, para llegar a las hojas, flores y frutos, que son las medidas probatorias de la relación del sujeto con los hechos.

¿Qué impacto real tiene esta situación en un proceso penal? Pues bien, si seguimos la relación probatoria y de investigación del proceso penal, veremos que la evidencia se construye desde la raíz hacia los frutos, y si la raíz está envenenada, los frutos del proceso penal también lo estarán a la larga.

¿Cómo puede envenenarse un proceso penal? Es muy simple, si aplico al inicio o en cualquier etapa procedi-

mental pruebas nulas, de dudosa obtención o que afecten garantías constitucionales como la privacidad, el no ser obligado a declarar contra sí mismo o cualquier otra garantía, la investigación y el proceso tendrán el mismo defecto desde su génesis, es decir, las pruebas o medidas que le dieron origen serán nulas o inadmisibles en juicio por sus propios vicios.

¿Qué tiene esto que ver con la evidencia digital? La respuesta es obvia: Si la obtención de la evidencia digital en un proceso penal no es adecuada al cumplimiento de las garantías del debido proceso o afecta cualquier otro derecho constitucional, jamás podrán ser usadas en juicio contra el sujeto activo, lo que aumentaría la situación de impunidad que actualmente existe en materia de delitos informáticos, o cometidos por medios informáticos, e incluso de delitos comunes donde la evidencia digital contenida en elementos electrónicos pudiere apoyar la investigación o condena de los criminales.

Garantías a cubrir

A estas alturas podemos preguntarnos cuáles son las garantías necesarias a cubrir para no afectar derechos constitucionales y lograr una plena admisibilidad de las evidencias digitales en los procesos penales.

Para cubrir esas garantías se elaboró este manual de la etapa previa para la obtención y aseguramiento de los medios de soporte de la información digital que podrá utilizarse como evidencia en caso de ser requerida o necesaria.

Si estas etapas no satisfacen las garantías implicadas, la evidencia que se obtenga en las posteriores mediante

peritajes o extracción de datos de los equipos no podrá utilizarse por las razones teóricas que hemos planteado, lo cual implicaría que un sujeto responsable de una acción antijurídica, típica y culpable no resulte punible por no contar con los medios probatorios idóneos.

Privacidad

La primer garantía que entra en juego en cualquier proceso donde se involucre información contenida en equipos electrónicos, es la de privacidad, pues si el sujeto titular de la información, y (en su caso) propietario o poseedor del medio de soporte, la colocó en ese formato es para que no pueda obtenerse con facilidad y sin su autorización expresa.

Debemos tener presente que la privacidad es una garantía relativa, pues puede caer ante la orden expresa de un juez, pero siempre que se respeten los principios que le dan sustento; por ejemplo, para la apertura de un correo electrónico deben respetarse las garantías que atañen a la comunicación postal; para una intervención de equipos que poseen mecanismos de *sniffing*[1] deben respetarse los derechos de terceros involucrados, de igual manera que con las intervenciones telefónicas y cualquier otra violación posible de privacidad, siempre por orden expresa de un juez, ya que en la mayoría de los procesos se recogen los equipos del imputado o presunto responsable y se

[1] Mecanismos, técnicas o programas que permiten interceptar, grabar o, en algunos casos, modificar la información que se transmite de una computadora a otra, ya sea por medio del agregado de programas o por la intervención física en las líneas (cables) o en las conexiones inalámbricas que las unen con las demás.

abren de manera indiscriminada archivos, correos y comunicaciones privadas a las que no se debe tener acceso sin la autorización expresa del juez que interviene en la causa como garante de la constitucionalidad del proceso.

Valor probatorio

En los procesos penales, el valor probatorio depende, tal como lo exponen los códigos de procedimiento penal, de la valoración que dé el juez interviniente a las evidencias digitales que se aporten a la causa, de manera que cuanto mayor sea la información que pueda obtenerse de los equipos electrónicos en cateo y aseguramiento, mayor será la relevancia para una sentencia absolutoria o condenatoria, según el caso.

En realidad, el valor probatorio depende de un segundo factor que es la credibilidad que pueda tenerse en la obtención y conservación de los equipos y la evidencia en ellos contenida, así como en la inviolabilidad o no adulteración de esos contenidos a favor o en contra del sujeto a proceso.

Inviolabilidad de los contenidos

Tal inviolabilidad es el punto medular del proceso probatorio, ya que si la evidencia es manipulada u obtenida de forma ilegal, no sólo corre el riesgo de resultar inadmisible sino también de que con ella caigan partes importantes del proceso que provoquen que un sujeto obtenga su libertad aun cuando sea claramente responsable del hecho que se le imputa, teniendo en cuenta que es la representación social quien debe probar la culpabilidad (obviamente ba-

sado en el principio constitucional de inocencia e *in dubio pro reo*), y sin las pruebas necesarias, o bien con pruebas inadmisibles, la parte acusadora verá disolverse sus posibilidades de ganar el proceso, de manera directa al grado de errores que se hayan dado en el cateo y aseguramiento de bienes electrónicos.

Son estos errores los que producen la inadmisibilidad judicial de las pruebas que podrían condenar o absolver a los indiciados, y el objetivo del presente manual es tratar de reducirlos al mínimo para que los elementos que puedan ser usados como prueba y la información que ellos contienen adquieran relevancia a la hora en que el decidor deba pronunciarse a través de la sentencia.

¿Qué es lo que se debe probar?

Entramos en un segundo tema de conflicto en el momento de la presentación de las pruebas en el proceso, habida cuenta de que la mayoría de las veces se trata de demostrar cuestiones irrelevantes o que en el fondo nada aportan en la discusión del proceso.

La mayoría de las veces lo que se intenta probar equivocadamente en los procesos es que desde determinado domicilio o desde determinado equipo se ha cometido la acción típica, lo que es cierto y presenta alguna relevancia, pero en realidad el que comete el delito no es el equipo informático sino la persona que lo opera, razón por la cual la simple prueba de que desde un equipo determinado se cometió el hecho no es suficiente para condenar al titular del equipo informático, ya que se debe ubicar al sujeto activo en tiempo y lugar con el mismo equipo desde

el cual se comete el ilícito, para que de esta manera se encuentren constituidos todos los extremos del cuerpo del delito.

Enfrentamos entonces la manera de relacionar los equipos con los usuarios que los operan, lo que implica necesariamente ubicar, como se dijo, a una persona en tiempo y lugar con un equipo, lo que requiere, en algunos casos, de evidencia digital contenida en el equipo, como el *blog* de inicio de sesión, las contraseñas o cualquier otra marca digital de quien era el supuesto operador del equipo en ese espacio temporal, lo que no implica tampoco un 100% de certeza, ya que si el mismo operador comparte sus claves de usuario con otros, o bien alguien más tuvo acceso a ellas, nos encontraríamos ante una evidencia circunstancial.

De esta manera adquieren entonces relevancia otras pruebas, como por ejemplo, la dactiloscopía practicada sobre los equipos, las filmaciones de los lugares de trabajo con cámaras de seguridad, las fotografías o incluso los testimonios de personas que pudieran dar fe de quién era el usuario de ese equipo a una hora y en una fecha determinadas.

Es fundamental comprender este concepto de integración de la prueba en la evidencia digital, ya que si no se llevan los recaudos necesarios en el momento del aseguramiento podría ocurrir que se pruebe desde qué equipo se cometió el delito o se apoyó la comisión de un delito, pero no saber quién operaba ese sistema, lo que nos pondría ante la ridícula situación de poder "condenar" a un equipo, mas no a un probable responsable.

En algunos casos excepcionales puede pensarse en la posibilidad de efectuar pruebas de ADN sobre los residuos epiteriales contenidos entre y sobre los espacios del teclado para demostrar que no existe evidencia de que el mismo haya sido utilizado por personas ajenas a los titulares de las claves de usuario o los inicios de sesión.

En conclusión, siempre que se trabaje sobre la obtención de evidencia digital se deben tener los recaudos necesarios para poder realizar sobre el equipo cualquier otro medio probatorio que pueda apoyar el hecho de que es una persona en particular la que está relacionada con la utilización del equipo que se pretende inspeccionar.

Procedimiento jurídico previo

Aunque sea obvio, el procedimiento jurídico previo debe aclararse a efecto de no generar la posibilidad de que se dictaminen nulidades procedimentales por los mismos errores comentados anteriormente en la referencia al principio del árbol de raíces envenenadas.

Es absolutamente indispensable que para el cateo y aseguramiento de los bienes informáticos exista orden judicial expresa, ya que, al no compartir las características de los demás bienes, no se puede tomar una orden de cateo genérico como suficiente para inspeccionar los sistemas electrónicos o, en su caso, asegurarlos.

La apertura de un equipo informático o bien su aseguramiento implican la posibilidad de violentar garantías constitucionales, lo que en definitiva debe ser siempre ordenado y controlado por un juez competente.

Conocidos estos "frenos" procedimentales, es de buena práctica que, al solicitar un cateo, el Ministerio Público pida expresamente el aseguramiento de los medios y equipos electrónicos (ya que requerir el cateo de equipos no necesariamente autorizaría el aseguramiento de soportes como CDs o de 3 1/2 pulgadas, que no son parte del equipo) que pudieran contener información a fin de evitar que el agente conozca datos para los cuales no está autorizado por el titular de los mismos o, en su caso, por alguien que lo represente, o el juez.

Con estas previsiones, la evidencia contenida en los equipos o en los medios asegurados podrá ser incorporada correctamente al expediente (averiguación previa o proceso judicial) sin objeciones sobre la legalidad de su obtención, ya que se encontrarían plenamente respetadas las garantías constitucionales involucradas en el proceso.

Debe tenerse siempre presente, pero sobre todo en el momento de la solicitud, que es indispensable utilizar la expresión *medios y bienes electrónicos*, ya que un PDA o un teléfono celular pueden contener mucha información y, si lo analizamos en detalle, no son estrictamente bienes informáticos, aunque sí bienes o equipos electrónicos.[2]

El problema es que si las facultades solicitadas no incluyen expresamente la recolección de información o el vaciado de datos (o clonación de discos), puede ocurrir que el aseguramiento resulte físicamente imposible, ya que muchos de los equipos no pueden ser movidos por su tamaño

[2] Véase Cámpoli, Gabriel Andrés, *Derecho penal informático en México*, INACIPE, México, 2004, por lo que respecta a las definiciones sobre delitos informáticos y delitos electrónicos.

o porque, de ser retirados, podría perderse información de los registros que se están procesando en el momento del operativo, de manera que debe tenerse el recaudo de también solicitar al juez la facultad de fotografiar (si es necesario) o bien de extraer datos de la escena del crimen para que los peritos que acompañan al Ministerio Público en el acto puedan tomar los cuidados necesarios para el caso.

Estas solicitudes incluyen, según el caso, la posibilidad de apertura de claves por procedimientos informáticos, si éstas existen y el equipo no puede ser retirado, o bien el retiro parcial de algunas partes del equipo para que éstas sean objeto de las pruebas periciales que se requieran.

¿Qué debe buscarse en un cateo completo?

En un cateo de equipos y sistemas completo e integrativo, tal como se describe en el presente trabajo, se deben buscar las evidencias necesarias, electrónicas o no, de la existencia de vínculos entre el sujeto y el equipo, para lo cual se recomienda buscar, además de los bienes en sí mismos, los siguientes comprobantes de posible existencia en el domicilio a registrar:

a) Comprobantes de pago y/o facturas de servicio de internet.

b) Comprobantes de pago y/o facturas del servicio de luz.

c) Comprobantes de pago y/o facturas del servicio de teléfono.

d) Anotaciones de claves de usuario o de correos que pudieran encontrarse en soportes distintos a los electrónicos (papeles o *post it,* por ejemplo).

e) Comprobantes de pago y/o facturas del servicio de conexión satelital (teléfono y/o internet).

f) Comprobantes de pago y/o facturas de pago del servicio de telefonía celular.

g) Comprobantes de pago y/o facturas del servicio de gas.

h) Comprobantes de pago y/o facturas del servicio de agua.

i) Comprobantes de pago de prediales.

j) Comprobantes de pago de tenencias vehiculares.

k) Comprobantes de pago y/o facturas de tarjetas de crédito.

l) Comprobantes de operaciones realizadas con tarjetas de crédito o débito.

m) Comprobantes emitidos por cajeros automáticos.

n) Listados de estados de cuentas bancarias.

o) Plásticos o tarjetas de crédito o débito.

p) Plásticos de tarjetas de hoteles u otras con banda magnética.

q) Comprobantes de pago y/o facturas de servicios de localizador (*pager* o *bipper*).

r) Facturas de pago de cualquier comercio o institución que puedan relacionarse con la persona o con los números de tarjetas que utiliza o, en su caso, con las cuentas bancarias, telefónicas o de Internet que se investigan.

s) Mecanismos de almacenamiento de imagen de video o estática (fotografía), como cintas VHS, fotografías en papel, CD, memorias tipo tarjeta o cualquier otro que pueda eventualmente aportar dicha información, los cuales pueden estar en el mismo lugar de los hechos o bien en habitaciones separadas, como cuartos de video o vigilancia, que incluso pueden ser externos a la empresa misma, de manera que si existen cámaras de cualquier tipo, necesariamente habrá un respaldo de lo que esos equipos obtienen, por lo que si no se encuentran en el lugar se debe cuestionar detalladamente a los presentes sobre la existencia y ubicación de dichos medios de almacenamiento de video e imágenes.

Procedimiento en el lugar de los hechos

Como primera medida, lo que se debe es no alterar o perder ninguna de las evidencias, digitales o físicas, encontradas en el lugar de los hechos, a fin de poder relacionar las mismas entre sí o, en su caso, con el probable responsable.

Por ello siempre se deben tomar las precauciones habituales en cualquier escena de crimen, por ejemplo:

1) No tome los objetos sin guantes de hule, pues podría alterar, encubrir o desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.

2) Proteger en la medida de lo posible la zona de posibles interacciones humanas o animales.

3) Tener extrema precaución de no tropezar, jalar o cortar cables de conexión de equipos, periféricos o conexiones de entrada o salida de datos.

4) Asegurar la zona y los equipos de acceso remoto, lo cual debe hacerse con extremo cuidado si se trata de servidores que deben ser intervenidos, ya que éstos, por su propia naturaleza, están especialmente preparados para ser *accesados* en forma remota.

5) Controlar que los presuntos responsables o la persona que estaba a cargo de los equipos no tenga en su poder un control remoto o cualquier otro dispositivo electrónico que pueda alterar el contenido o el estado de los equipos o periféricos, ya estén éstos conectados o no al servidor o sistema central. Esta precaución se aplica a todos los presentes en el acto.

6) Retirar los teléfonos celulares o dispositivos tipo *blue berry* o similares (dispositivos que conjuntan las PDA con teléfonos celulares), ya que con ellos pueden realizarse en ciertos casos modificaciones sobre los equipos en distancias cortas.

7) Asegurar el acceso y control de los suministros de luz, ya que existen muchos equipos que si son apa-

gados de manera incorrecta pueden dañarse (lo que haría irrecuperable la información) o bien pueden perder información, como por ejemplo la de inicio de sesión.

8) Si en el momento de ingresar al lugar alguien se encuentra operando el sistema, tomar nota (en forma legal) de la situación, y de ser posible fotografiarlo cuando aún está sentado en posición de operador.

9) De igual manera, ordenar a la persona que se encuentra en el equipo que suspenda de manera inmediata lo que está haciendo y tratar de tener control de las actividades que realiza hasta que se encuentre separado del equipo y los periféricos.

10) Una vez garantizado el cierre del área, debe procederse a tomar fotografías del estado y posición de los equipos, así como de sus puertos (conectores de cables, lectores de CD, lectores de disquete y cualquier otro punto de contacto del equipo con el exterior) y de igual manera de la pantalla en el estado en que se encuentre, incluyéndose los cables, conectores externos e, incluso, todos los periféricos que se hallan en el área o los que pudieran estar conectados de forma remota si ello es posible (por ejemplo, impresoras comunes en una sala de impresión), con las debidas identificaciones, ya sea de marca o cualquier otra que pueda dar certeza sobre el equipo. Es ideal tomar fotografías de los números de serie de todos ellos.

11) Fotografiar la existencia de cámaras de video o de fotografía instaladas en el sitio de los hechos para tener plena certeza de la obtención de pruebas adicionales de la relación usuario-equipo.

12) Al manipular los equipos recuérdese hacerlo siempre con guantes de hule para evitar la contaminación.

13) Otorgue la intervención debida a los peritos en dactiloscopía para que se pueda determinar la existencia de huellas dactilares sobre el equipo o bien, en su caso, sobre los periféricos o soportes de cualquier índole que existan en el lugar de los hechos.

14) Una vez terminado el proceso de levantamiento de huellas dactilares, puede comenzar la tarea de los peritos en informática.

Aseguramiento de los equipos, bienes y soportes informáticos

Es importante aclarar que con o sin la presencia de los peritos en informática, sean de la AFI o profesionales de la PGR, deben respetarse los pasos del procedimiento para que de esta manera se otorgue plena garantía de un correcto aseguramiento de la evidencia y de la imparcialidad de la misma, tanto como su integridad posterior.

En el momento de comenzar el cateo, y si fueron debidamente aplicadas las medias anteriores, debe tomarse nota y fotografía del estado de los equipos y sus componentes (centrales y periféricos), según se ha detallado en los pasos de aseguramiento del lugar de los hechos.

A partir de ahí, los pasos a seguir son:

General

1) Levantar individualmente todos los medios de soporte (CD, tarjetas, discos de 3 1/2, memorias USB o cualquier otro según los listados anteriores) que se encuentren separados del equipo.

2) Si está encendido, primero debe aislarse de intrusiones externas, para lo cual es necesario verificar la existencia de puertos de red o conexiones inalámbricas que pudieran ser fuente de acceso para modificar los contenidos.

3) En caso de existir alguna conexión (cable de red o inalámbrica, que en muchos equipos es interna, por lo que no tendríamos acceso inmediato a la misma) se debe aislar de manera inmediata el equipo, preferentemente con la asistencia del experto en informática y precintando las conexiones que se retiren.

4) Si existiere en el lugar de los hechos más de un equipo, identificar de manera clara cada uno de ellos por medio de números con etiquetas engomadas y firmadas, y en cada pieza que se retire de cada uno de ellos colocar el número que se asignó al equipo.

5) Identificar en las fotografías el número asignado a cada equipo.

6) Bajo ninguna circunstancia desmontar o desconectar más de un equipo a la vez, lo cual debe hacerse siempre conforme a los procedimientos indicados en

los puntos posteriores, para evitar confundir las piezas o cables de cada uno de ellos.

7) Cuando un equipo está completamente desmontado, retirarlo del lugar de los hechos antes de comenzar con el siguiente equipo.

8) Bajo ninguna circunstancia desconectar o retirar elemento alguno del equipo (ni discos de 3 1/2, ni CD, ni memoria USB, ni cables, ni tarjetas de memoria de cualquier tipo). Sólo fotografiar su posición y estado.

9) Verificar si los equipos se encuentran apagados o encendidos, y asentar en el acta su estado.

10) Si están apagados, no encenderlos por ningún motivo.

11) Por el contrario, si están encendidos, no apagarlos por ningún motivo.

12) Tomar de inmediato fotografía detallada de la imagen de la pantalla. Si se tratare de un protector de pantalla o el monitor estuviese en descanso, con la utilización de guantes de hule mover lentamente el ratón hasta que aparezca la imagen del programa en proceso en el momento anterior al inicio del ahorro de energía del equipo.

13) Fotografiar inmediatamente la imagen de la pantalla que aparece luego de esa operación.

14) Asentar inmediatamente en las actas de cateo la hora en que fueron realizadas las tres operaciones, es de-

cir, la primera fotografía, el movimiento del ratón y la segunda fotografía de la pantalla.

15) Bajo ninguna circunstancia continuar con las operaciones hasta que no se persone el especialista en informática forense.

16) En ese momento el especialista debe realizar, bajo condiciones normales, la extracción original de datos de las unidades de disco y la memoria RAM (clonación de discos y de memoria) del equipo para evitar la pérdida de la información volátil o la modificación de datos o registros de entrada al equipo.

17) De encontrarse apagado el equipo, puede procederse a su desconexión para retirarlo del lugar de los hechos.

18) Para la desconexión debe procederse según los pasos siguientes:

19) Desconectar el cable que conecta el equipo a la energía eléctrica de la pared o, en su caso, al UPS (también conocido como *no-break*) e inmediatamente colocar un precinto de papel engomado firmado por el interviniente en el sitio del *no-break*, y, en su caso, los testigos del acto, sobre el lugar del conector que se retira.

20) Desconectar el otro extremo del mismo cable que se encuentra en la computadora y repetir la operación de precintado con papel engomado y firmado.

21) Identificar el cable retirado, por medio de etiquetas firmadas, y colocar el mismo en las bolsas de evidencia, de ser posible por separado.

22) Desconectar el cable de energía eléctrica del monitor (pantalla) bajo las mismas mecánicas y cuidados del anterior.

23) Identificar el cable de energía eléctrica del monitor con etiqueta y colocarlo en bolsa de evidencia del mismo modo.

24) Identificar el cable que conecta el monitor con el CPU (cajón central de la computadora).

25) Desconectar el cable que une al CPU con el monitor y precintar el lugar del que se retira el cable con el procedimiento del papel engomado y firmado.

26) Identificar el monitor con el mismo procedimiento del papel engomado y firmado, asegurando que el mismo no pueda ser abierto, para lo cual se recomienda colocar el precinto de papel engomado sobre los bordes de apertura del monitor, para evitar que pueda retirarse cualquier pieza del exterior o interior del mismo sin que ello pudiera ser detectado en revisiones posteriores.

27) Proceder al retiro del teclado, precintando luego el sitio donde el mismo estaba conectado por medio del procedimiento del papel engomado y firmado.

28) Precintar asimismo el extremo del conector del teclado por el mismo procedimiento, o bien, de resultar muy complejo, con una bolsa de polietileno que se pega al cable a través del papel engomado.

29) Colocar, de ser posible, el teclado en bolsa separada a fin de practicar luego las medidas forenses de ADN o huellas dactilares, si se requieren en momentos posteriores del proceso.

30) Proceder luego, de igual manera que con el teclado, con el ratón de la computadora, tomando las precauciones de precintado ya descritas.

31) Apagar los periféricos que estén encendidos, previa anotación en el acta respectiva del estado en que se encontraban al inicio del procedimiento, dejando constancia de los números de serie de cada equipo para luego diferenciar uno del otro en el momento de los trabajos periciales o la sentencia.

32) Proceder a la desconexión de todos los periféricos, como impresoras, escáneres, lectores de disco, grabadoras o cualquier otro que se encuentre conectado al equipo, previa fotografía del lugar de conexión y posterior precintado en cada caso de los lugares donde se encuentran conectados, dejando constancia de ello en el acta y en el precinto de papel engomado, donde, además de las firmas, se debe agregar una leyenda como esta: "conexión de impresora marca..., modelo..., número de serie...," para luego, de ser necesario, poder reconstruir la conformación original del equipo.

33) Etiquetar cada equipo al momento de su desconexión, dejando constancia de la computadora a la que se encontraba conectado.

34) Luego de desconectados y etiquetados sus cables de conexión, precintar cualquier punto de entrada o salida de datos (es decir, cualquier conector que pudiera tener el equipo) y los accesos de corriente eléctrica.

35) Si se trata de unidades de lectura de tarjetas, de discos de 3 1/2 o de CD, precintar los accesos a la misma.

36) Si se trata de cualquier unidad de almacenamiento (discos duros externos, por ejemplo) precintar de igual manera los tornillos de acceso para evitar que los discos internos puedan ser cambiados o modificados.

37) Colocar cada periférico en bolsas o cajas individuales e identificadas de ser posible, e incluso si se hallan las cajas originales, colocarlos en ellas.

38) Una vez retirados todos los periféricos se procede al precintado del CPU, sellando con los papeles engomados todos los accesos posibles, como puertos USB, lectores de CD, lectores de discos de 3 1/2, puertos de impresora, teclados, conexiones de red, o cualquier otro que se encuentre luego de una exhaustiva revisión del mismo.

39) Como los equipos siempre tienen unidades de almacenamiento internas (discos duros) debe procederse también al precintado de los tornillos externos de acceso para evitar que pueda ser abierto y puedan retirase, cambiarse o modificarse piezas, sobre todo las unidades centrales (discos duros).

40) Colocar cada CPU en una caja individual, precintada e identificada, de preferencia en la original (si se halla), para ser retirado del lugar.

Cuando los equipos no pueden ser retirados:

Si los equipos no pudieren ser retirados del lugar por su tamaño, el aseguramiento debe realizarse en el mismo lugar de los hechos, pero bajo el procedimiento de los puntos que siguen:

1) Dejar constancia de si el equipo se encuentra encendido o apagado.

2) Si está encendido, no apagar por ningún motivo.

3) Si está apagado, no encender por ningún motivo.

4) Si se encuentra encendido, primero se debe aislar de intrusiones externas, para lo cual es necesario verificar la existencia de puertos de red o conexiones inalámbricas que pudieran ser fuente de acceso para modificar los contenidos.

5) En caso de existir cable de red o conexión inalámbrica, que en muchos equipos es interna, por lo que no tendríamos acceso inmediato a la misma, se debe aislar de manera inmediata el equipo, preferentemente con la asistencia del experto en informática presente y precintando de manera inmediata las conexiones que se retiren.

6) Una vez aislado, proceder a la extracción de datos (clonación o copia física de los datos contenidos en los equipos).

7) Realizada la extracción de datos, debe procederse al retiro de cualquier periférico que pudiera encontrarse conectado al equipo bajo la metodología explicada en los puntos anteriores para los equipos comunes que sí pueden retirarse, sólo que en este caso se retiran los periféricos debidamente identificados y precintados como se indicó y se sellan los conectores que se dejan libres en esta operación.

8) Luego, y al igual que con los CPU que pueden removerse, se procede al precintado con papel engomado de todos los puertos y conectores que pudieran estar libres.

9) De igual manera deben precintarse los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.

10) En ese momento debe asegurarse la zona para evitar cualquier acceso físico de personas o animales al lugar donde el equipo se encuentra, a fin de mantener la evidencia original intacta.

11) Si el equipo se encuentra apagado, pueden desmontarse en ese acto, por seguridad jurídica y ahorro procedimental, los medios de almacenamiento que se encuentren en el equipo.

12) Para lo anterior se debe contar con la presencia de un técnico informático a fin de evitar daños al equipo o, en su caso, a alguna de las piezas removidas.

13) Una vez desconectados e identificados todos los cables del equipo, se procede a la apertura del mismo por medio de la remoción de su carcaza.

14) Al abrir la carcaza, fotografiar la posición y estado de los medios a extraer.

15) Realizar fotografías de aproximación de cada medio y de sus números de serie, asentando los mismos en el acta respectiva, de manera referenciada a las fotografías de aproximación y la general.

16) Una vez realizado lo anterior, se pueden retirar los medios de almacenamiento, que son los que se deben asegurar.

17) Para lo anterior, al remover los cables de conexión del medio, se debe precintar cada uno de ellos con identificación de la posición que ocupaban en el equipo, haciendo lo mismo con los puntos de conexión del equipo.

18) Terminada esa tarea, se debe proceder a precintar debidamente todos los tornillos del medio extraído.

19) Luego se empaca el medio en caja o bolsa por separado, dejando constancia de todo lo actuado y su orden en el acta respectiva.

20) Terminadas las operaciones se debe colocar nuevamente la carcaza y precintar la misma y sus tornillos de extracción para preservar el resto del equipo por si se presentara la necesidad de pruebas posteriores.

21) Concluida la operación, se debe proceder al aseguramiento físico del lugar de los hechos, como ya se había comentado para opciones anteriores.

*Cuando los equipos son portátiles (*notebook *o* laptop*):*

1) Levantar individualmente todos los medios de soporte (CD, tarjetas, discos de 3 1/2, memorias USB o cualquier otro según los listados anteriores) que se encuentren separados del equipo.

2) Si se encuentra encendido, primero se debe aislar de intrusiones externas, para lo cual es necesario verificar la existencia de puertos de red o conexiones inalámbricas (en muchos casos internas, por lo que no se tendría acceso inmediato a las mismas) que pudieran ser fuente de acceso para modificar los contenidos.

3) En caso de existir, se debe aislar de manera inmediata el equipo, preferentemente con la asistencia del experto en informática presente y precintando de manera inmediata las conexiones que se retiren.

4) Si existe en el equipo una tarjeta de red inalámbrica, retirar de manera inmediata la misma, precintando el lugar de donde se retiró.

5) Colocar la tarjeta retirada, debidamente identificada y fotografiada en bolsa para su aseguramiento.

6) Si la tarjeta fuere interna, localizar la tecla de anulación del servicio inalámbrico y desactivar el mismo de manera inmediata (por lo general la tecla de desactivación tiene una pequeña torre con paréntesis a sus lados en la parte superior).

7) Fotografiar el equipo, su número de serie y el estado de la pantalla. Si la misma estuviese apagada, pasar suavemente el dedo (con guantes) sobre el pad físico del ratón para habilitar la misma a su estado anterior y fotografiar nuevamente lo que aparece en la pantalla.

8) Precintar todos los mecanismos y conexiones de entrada y salida del equipo.

9) Inmediatamente proceder a retirar el equipo para llevarlo al cuerpo forense (si éste no se encuentra presente), aprovechando los tiempos de batería, pero siempre que el equipo se encuentre debidamente precintado, moviendo al menos cada dos minutos el pad físico del ratón para mantener abierta la sesión y evitar que el equipo entre en estado de hibernación, siempre realizando estas acciones con guantes de hule para evitar alterar las huellas dactilares que pudieran existir en esa área del equipo.

10) Al recibirlo en periciales, volver a conectarlo a la corriente para evitar su apagado al consumirse la batería.

11) Si se encuentra apagado, proceder al precintado y retirar los cables eléctricos, identificando dicha actividad, de la cual se deja constancia en el acta.

12) Mantener el equipo asegurado en las mismas condiciones de seguridad que los equipos fijos comentados en el primer apartado del presente.

Cuando se trate de un Asistente Personal Digital (PDA):

1) Si se encuentra encendido, no apagar por ningún motivo.

2) Por el contrario, si se encuentra apagado, no encender por ningún motivo.

3) Fotografiar el estado del aparato y de ser posible lo que se muestra en la pantalla.

4) Fotografiar y asentar en actas la marca, el modelo y el número de serie si es que éstos son visibles.

5) Precintar todas las entradas y salidas.

6) Precintar todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria.

7) Precintar los tornillos para evitar que se puedan retirar o reemplazar piezas internas.

8) Buscar y asegurar el lápiz que lo acompaña.

9) Buscar y asegurar el conector eléctrico.

10) Colocarlo en una bolsa de *faraday* (especial para aislamiento de emisiones electromagnéticas). Si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa.

11) Llevar inmediatamente con los peritos para la extracción de la información correspondiente.

Cuando se trate de teléfonos celulares:

1) Si se encuentra encendido, no apagar por ningún motivo.

2) Si se encuentra apagado, no prender por ningún motivo.

3) Fotografiar el estado del equipo y la pantalla.

4) Fotografiar y asentar en actas la marca, el modelo y el número de serie del equipo si son visibles.

5) Precintar todas las entradas y salidas.

6) Precintar todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria.

7) Precintar los tornillos para evitar que se puedan retirar o reemplazar piezas internas.

8) Buscar y asegurar el conector eléctrico.

9) Colocarlo en una bolsa de *faraday* (especial para aislamiento de emisiones electromagnéticas). Si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa.

10) Llevar de inmediato a los peritos para la extracción de la información correspondiente.

Manual Básico de Cateo y Aseguramiento de Evidencia Digital
edición al cuidado de Olivia Bravo Arvizu y
la Dirección de Publicaciones.
Se terminó de imprimir en el mes de diciembre de 2006 en
los talleres de Impresiones Precisas Alfer S.A. de C.V.
Su composición se hizo en *Times New Roman* 14:16, 12:14 y 9:11 puntos.
Se usó papel ABTB 75 grs.
Tiraje: 1 000 ejemplares.

El actual dominio de las comunicaciones en el ámbito de la documentación y su imparable tendencia como medio fundamental dentro de la investigación criminalística, hacen de la evidencia digital un recurso de utilidad en el suministro de pruebas fehacientes para un determinado incidente telemático.

Sin embargo, que la evidencia digital sea un rubro más de la criminalística lo convierte en un medio tan volátil como lo puede ser, por ejemplo, la investigación en el lugar de los hechos. También se trata de una especialidad pericial donde deben tomarse ciertas medidas y llevarse a cabo procedimientos especiales con la finalidad de no provocar una pérdida irreparable de evidencia, de no causar su inadmisibilidad y, por ende, la errónea liberación del inculpado.

El presente *Manual de cateo y aseguramiento de evidencia digital* pretende servir como guía de las acciones y mecanismos a aplicar durante el cateo o aseguramiento de los equipos electrónicos hallados en la escena del crimen.

Instituto Nacional de Ciencias Penales

30 Aniversario INACIPE 1976-2006

ISBN 970-768-077-6

9 799707 680776