PROTOCOLO DE ACTUACIONES PARA INFORMATICA FORENSE

MINISTERIO PÚBLICO FISCAL DE LA PROVINCIA DE CORRIENTES

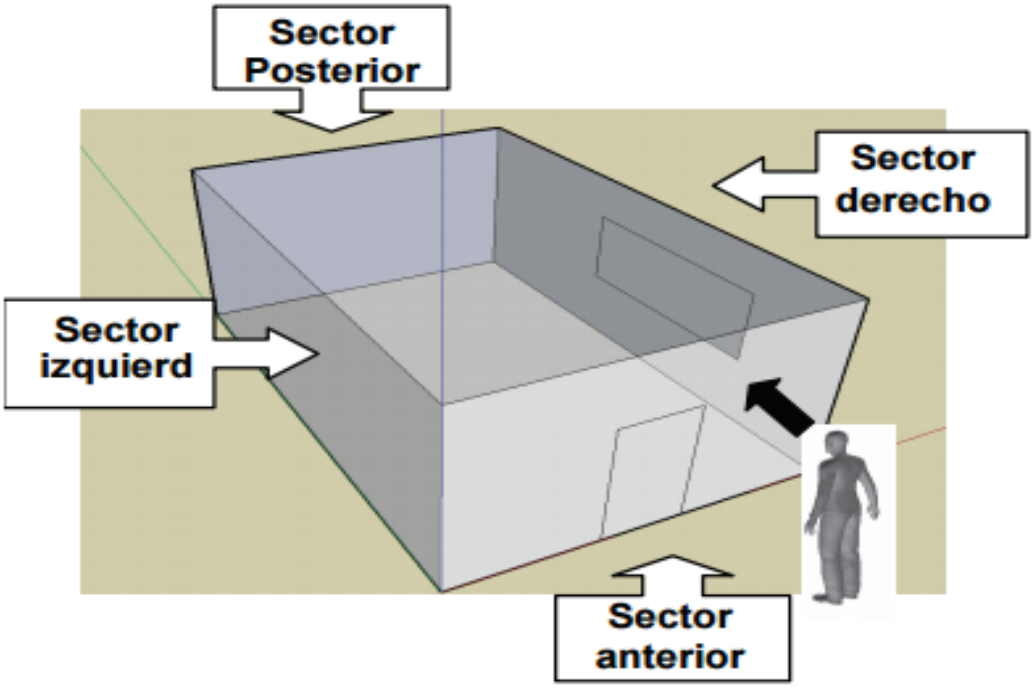
Contenidos

1. Objetivos

- ✓ Formalizar con procedimientos estandarizados, las actuaciones en materia de informática forense.
- ✓ Especificar las tareas referentes a la informática forense.
- ✓ Lograr eficiencia en la labor diaria alcanzado resultados eficaces.
- ✓ Priorizar la cadena de custodia.

2. Preservación del lugar de hecho en un allanamiento o procedimiento en la vía publica

El funcionario policial o de fuerza de seguridad que intervenga inicialmente debe extremar recaudos a fin de preservar la intangibilidad del lugar del hecho, para lo cual deberá cumplir los presupuestos abajo descriptos, los que no necesariamente requieren un seguimiento secuencial, dado que definen actividades que pueden cumplirse simultáneamente:



a) Coordinar el allanamiento con personal policial.

b) En el lugar del hecho retirar a toda persona ajena al procedimiento y restringir el acceso al lugar.

c) Definir los límites del lugar del hecho a fin de protegerlo y asegurarlo, estableciendo un perímetro amplio.

d) Utilizar cordeles, cintas, vehículos, al propio personal o cualquier otro medio existente a su alcance para la demarcación, protección y aislamiento del lugar del hecho, cuando se tratare de lugares abiertos.

e) Clausurar los accesos, cuando se tratare de lugares cerrados, ya sea ubicando personal frente a puertas y ventanas o sellando dichos sectores.

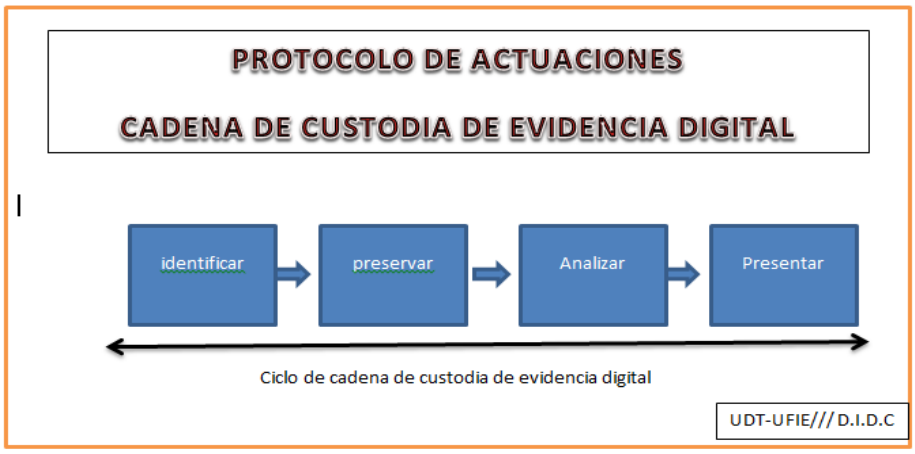
f) Resguardar la integridad y contenido de todo el material, datos, documentos o información, de su destrucción, desaparición o manipulación, los elementos electrónicos, celulares, pendrive, computadoras, impresoras, teléfonos, cámaras fotográficas, filmadoras, fotocopiadoras y todo material de almacenamiento digital.

g) Tomar todas las previsiones ante peligros inminentes para reducir al mínimo la posibilidad de que bienes materiales puedan resultar dañados.

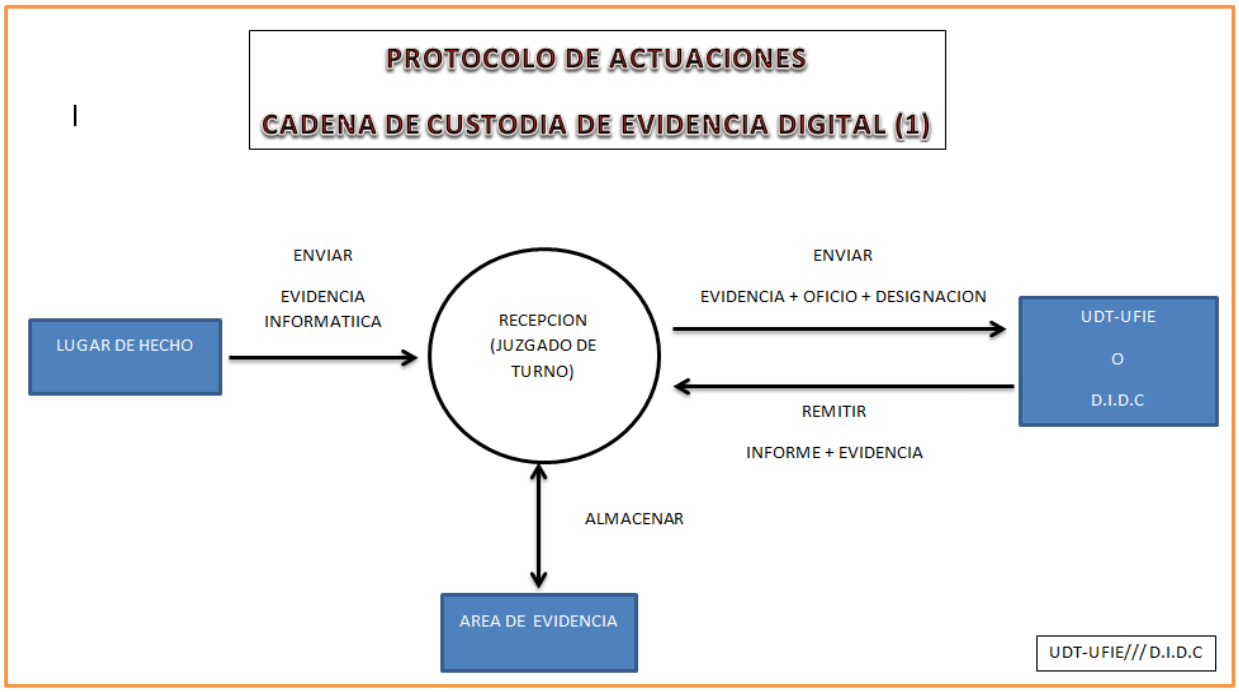
h) Comunicar el conjunto de lo observado y actuado, por la vía más rápida, a la superioridad, a efectos de su intervención para garantizar el orden y la seguridad pública, como así también la dotación de especialistas periciales a intervenir y/o el personal técnico informático de la UFIE (Fiscalía General).

i) Impedir el acceso al LUGAR DEL HECHO de personas no autorizadas con excepción de los servicios de emergencia hasta la llegada de la Policía Científica o Criminalística.

3. El ciclo de la cadena de custodia de evidencia informática



La cadena de custodia tiene como finalidad preservar la prueba. Por tal motivo deben establecerse los procedimientos indicados para garantizar la idoneidad de los métodos aplicados para la obtención de la evidencia informática. Por lo cual es necesario que se eviten suplantaciones, modificaciones, alteraciones, adulteraciones o simplemente su destrucción (común en la evidencia digital, ya sea mediante borrado o denegación de servicio). Procedimiento controlado y supervisarle, la cadena de custodia informático-forense se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, desde su localización hasta su valoración por los encargados de administrar justicia.
La preservación de la cadena de custodia sobre la prueba indiciaria es obligación de la totalidad de los miembros del poder judicial, los operadores del derecho y sus auxiliares directos. Entre estos últimos debemos incluir el personal de las fuerzas de seguridad, la policía judicial y el conjunto de peritos oficiales, de oficio y consultores técnicos o peritos de parte.
Desde el momento de sustracción de evidencia informática, después del lacrado y la colocación de faja de seguridad por el personal idóneo o técnico, ante la presencia de testigos y con las firma de los mismos. La evidencia informática deberá recorrer el ciclo de cadena custodia hasta la realización del análisis técnico pericial (oficinas de UDT-UFIE o D.I.D.C) por el personal designado.



4. Procedimientos

a) Planificación

Ante todo procedimiento judicial en el lugar del hecho, deberá procurarse obtener información tendiente a conocer las características generales de la infraestructura tecnológica existente, tendiente a elaborar una planificación minuciosa para el secuestro de elementos que pudieran contener material probatorio.

Cuando la operación a llevarse a cabo involucre personal ajeno a esta oficina se coordinaran a priori en tiempo y formas, estableciendo los medios necesarios para un trabajo fluido y evitar contratiempos.

b) Identificación de los elementos informáticos

La identificación debe ser precisa en el sentido de incautar solo aquellos materiales tecnológicos que almacenen información y se llevara a cabo conforme la "Guía operativa para el secuestro de tecnología informática" que integra el presente documento.

Se deberá redactar un acta en el lugar del allanamiento donde consten datos esenciales como ser los números de serie, etiquetas del fabricante de software y hardware instalado u otros distintivos particulares de los elementos y sus distintos componentes que lo conformen, si los tuvieran.

c) Preservación de evidencia digital

Se deberá utilizar precintos o fajas de seguridad al momento del secuestro de los elementos informáticos y todo medio necesario para garantizar la autenticidad e integridad de los elementos secuestrados. A tal fin se deben seguir los lineamientos indicados en el "Instructivo para la utilización de etiquetas de seguridad sobre dispositivos informáticos" que complementa el presente protocolo.

d) Requerimiento judicial

Los operadores judiciales realizaran las consultas necesarias para eliminar ambigüedades y establecer de forma concreta los puntos de pericia en el oficio que adjuntara los elementos secuestrados y proveerá toda información necesaria para la realización del análisis forense.

e) Priorización de casos urgentes

Se establecerá exenciones sobre el orden en la lista de espera dando prioridad a aquellas causas con personas detenidas, debiendo ello ser explícitamente indicado en el oficio del requerimiento judicial.

Asimismo, tienen prioridad aquellas causas judiciales por delitos que prevean penas severas por tratarse de bienes jurídicos protegidos de suma relevancia, como la vida o la integridad sexual, en los que el paso del tiempo ponga en riesgo el devenir de la investigación.

En caso de tener dos pericias informáticas con el mismo nivel de urgencia, se dará trámite por orden de ingreso.

El especialista podrá brindar una estimación del tiempo requerido para el inicio de la tarea forense en función de la capacidad operativa disponible, los trabajos en trámite y aquellos que estén en lista de espera.

f) Audiencias

Las audiencias se llevaran a cabo en las condiciones acordadas con el organismo solicitante y de acuerdo al cronograma interno de la oficina.

El solicitante deberá remitir la información necesaria para aminorar incertidumbres sobre la tarea a ejecutar, como ser dispositivo informático a analizar o archivos electrónicos a reproducir, a fin de lograr procedimientos fluidos con resultados agiles y satisfactorios evitando situaciones de demora o improcedencia técnica por factores previsibles.

En virtud de lo anterior, se realizaran las comunicaciones pertinentes para el buen entendimiento y coordinación de todos los intervinientes, antes de la elaboración del oficio requirente.

g) Traslado y recepción del material secuestrado

El traslado de los elementos secuestrados hasta los organismos judiciales es responsabilidad del personal policial por lo cual todo personal interviniente en la cadena de custodia de dichos elementos deberá dejar registrada su intervención en el acta de secuestro y tener presente las sanciones previstas por el art. 254 y 255 del Código Penal Argentino.

La recepción de los elementos secuestrados se realizara cotejando la existencia de los precintos y fajas de seguridad conforme el "Instructivo para la utilización de etiquetas de seguridad sobre dispositivos informáticos", la correcta identificación y estado general de cada elemento. En caso de detectar discrepancias se realizaran las salvedades y observaciones pertinentes dejando constancia en el acta de recepción.

h) Análisis forense

El análisis informático forense se realizara conforme las legislaciones vigentes formales y materiales válidas, estándares actuales y buenas

prácticas, con el objetivo de llegar a resultados eficaces y sustentados técnica y legalmente.

Las tareas operativas en el lugar del hecho resultan dificultosas por las complejidades técnicas y el tiempo que requieren las herramientas forenses para completar su ejecución, por lo cual se deberá determinar la viabilidad de realizarla in situ o se propenderá llevarla a cabo en el laboratorio forense en condiciones ideales y con recursos adecuados, garantizando la evidencia y los resultados.

i) Presentación del informe

El informe será presentado siguiendo los estándares utilizados para la presentación de reportes informáticos forenses.

Se intentará minimizar el volumen de información en soporte papel, suministrando información complementaria en soporte digital.

El lenguaje empleado será técnico y se harán comentarios tendientes a su comprensión por personal no técnico, cuando así se lo considere necesario.

Se imprimirá un informe para presentar al organismo requirente y una copia a fines de resguardo y archivo en esta oficina. Esta última será impresa parcial o total según el volumen y tipo de información.

j) Remisión del material secuestrado

Los elementos secuestrados serán resguardados con los medios adecuados para preservar la integridad y la autenticidad de la evidencia digital hasta finalizar el proceso judicial por si fuera necesario repetir o ampliar el análisis forense y serán remitidos al organismo de origen junto al correspondiente informe.

5. Guía operativa para el secuestro de tecnología informática

Destinatarios: Personal policial, técnicos y personal informático de la UFIE.
Principios básicos
Siempre que los tiempos lo permitan se debe 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.
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 de la presente Guía. 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 CDs, DVDs, los que sólo han de ser enviados a peritaje únicamente si se tienen presunciones con un alto grado de verosimilitud de poseer la evidencia buscada.

Pasos durante el allanamiento

a) Se deben separar 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. Siempre que sea posible obtener contraseñas de aplicaciones, dejarlas registradas en el acta de allanamiento.

b) Se deben procurar fotografiar todos los equipos informáticos antes de moverlos o desconectarlos. Fotografiar una toma completa del lugar donde se encuentren los equipos informáticos, y fotos 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.

c) Evitar tocar el material informático sin uso de guantes descartables. Dependiendo el objeto de la investigación, el teclado, monitores, mouse, CDs, DVDs, etc., pueden ser utilizados para análisis de huellas dactilares, ADN, etc. Si se conoce que no se realizarán este tipo de pericias puede procederse sin guantes.

d) 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.

e) 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.

f) Impedir que nadie realice búsquedas sobre directorios o intente 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).

g) Identificar correctamente todo el material tecnológico a secuestrar:

g.1) Siempre debe preferirse secuestrar únicamente los dispositivos informáticos que almacenen grandes volúmenes de información digital (computadoras, notebooks y discos rígidos externos). Respecto a DVD, CDs, 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.

g.2) Rotular el hardware que se va a secuestrar con los siguientes datos:

- ✓ Para computadoras, notebooks, notebooks, celulares, cámaras digitales, etc.: N° del Expediente Judicial, Fecha y Hora, Número de Serie, Fabricante, Modelo.
- ✓ Para DVDs, CDs, Pendrives, etc.: almacenarlos en conjunto en un sobre antiestático, indicando N° del Expediente Judicial, Tipo (DVDs, CDs, Pendrives, etc.) y Cantidad.

g.3) Cuando haya periféricos muy específicos conectados a los equipos informáticos y se deban secuestrar, se deben identificar con etiquetas con números los cables para indicar dónde se deben conectar. Fotografiar los equipos con sus respectivos cables de conexión etiquetados.

h) Usar bolsas especiales antiestática para almacenar discos rígidos y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.

i) Precintar cada equipo informático en todas sus entradas eléctricas y todas las partes que puedan ser abiertas o removidas. Es responsabilidad del personal policial que participa en el procedimiento el transporte sin daños ni alteraciones de todo el material informático hasta que sea peritado.

j) Resguardar el material informático en un lugar limpio para evitar la ruptura o falla de componentes. No deberán exponerse los elementos secuestrados a altas temperaturas o campos electromagnéticos. Los elementos informáticos son frágiles y deben manipularse con cautela.

k) Mantener la cadena de custodia del material informático transportado. Es responsabilidad del personal policial la alteración de la evidencia antes de que sea objeto de una pericia informática en sede judicial. No se podrá asegurar la integridad de la evidencia digital (por lo tanto se pierde la posibilidad de utilizar el medio de prueba) si el material informático tiene rotos los precintos al momento de ser entregado, siempre que no esté descripta en el expediente judicial la intervención realizada utilizando una metodología y herramientas forenses por profesionales calificados.

6. Instructivo para la utilización de etiquetas de seguridad sobre dispositivos informáticos

Destinatarios: Personal Policial, Policía Judicial y Técnicos Informáticos de la UFIE (Fiscalía General).

Objetivo

Mantener la cadena de custodia de los elementos probatorios, desde su secuestro hasta la finalización del proceso judicial, a fin de garantizar la autenticidad e integridad de la evidencia.

Es imposible atribuir responsabilidades por el faltante de elementos si no se identifica y asegura el material que se envía a peritaje "desde el momento del allanamiento". Estas etiquetas de seguridad evitan fallas en el procedimiento de secuestro/transporte de los elementos probatorios.

Distribución

Las etiquetas se distribuyen a todos los organismos judiciales encargados de la Investigación penal en toda la provincia.

Este material puede ser requerido a la División Suministros como cualquier otro insumo, con la salvedad de que deberá mantenerse un estricto control en la entrega de las etiquetas por cuestiones de costos y demora en el reaprovisionamiento.

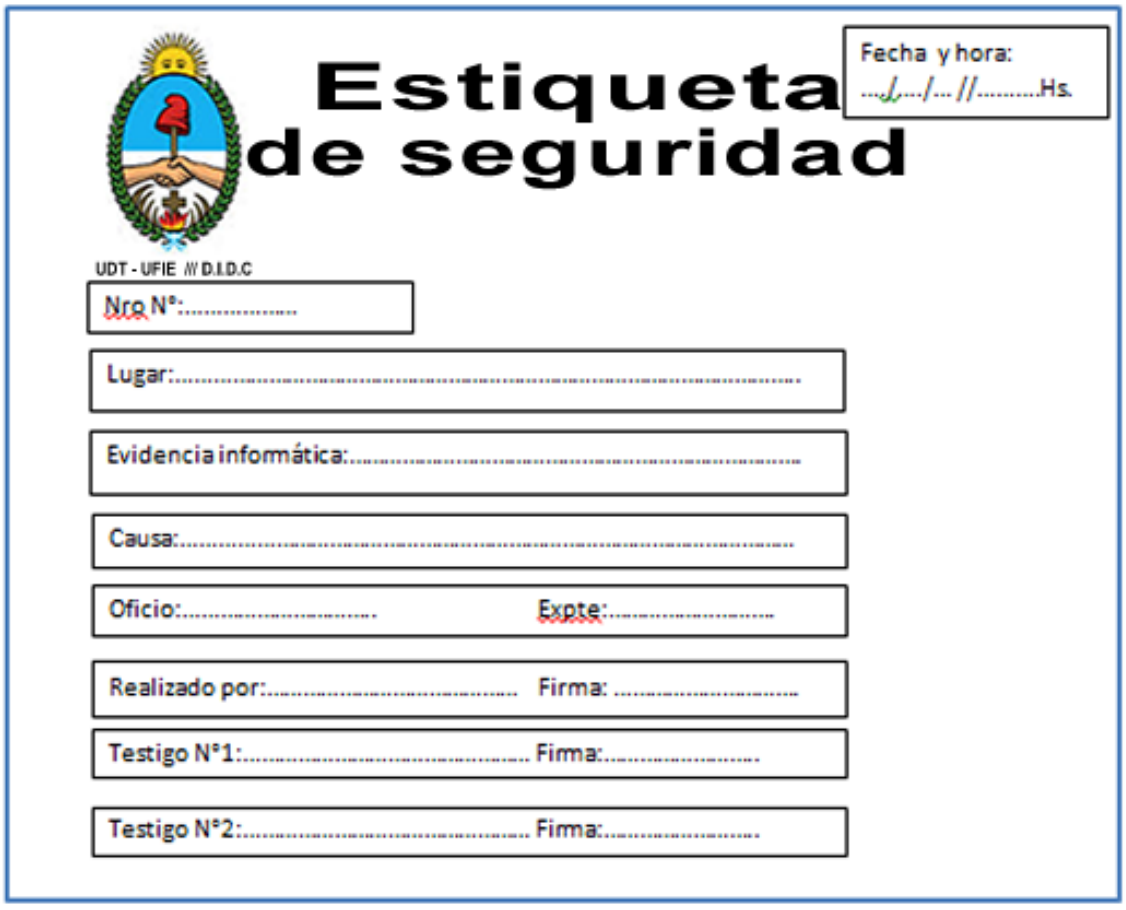
El personal de la División Suministros de la Administración General del Poder Judicial registrará los números de serie entregados a cada dependencia judicial. Por costos y dificultades en el reaprovisionamiento, las etiquetas de seguridad deberán estar bajo custodia de un funcionario judicial en cada organismo judicial que haga uso de las mismas.

Utilización

Las etiquetas de seguridad deberán ser entregadas al Fiscal a cargo de la investigación o al Oficial actuario de la Policía al momento de expedir una orden de allanamiento (en una cantidad razonable a la magnitud del procedimiento). Se adjuntará al acta de allanamiento una copia de la "Guía operativa para el secuestro de tecnología informática".

Durante el procedimiento judicial, las etiquetas serán colocadas por el personal policial en todos aquellos lugares que permitan la apertura de un equipo informático, bloqueando cualquier conector de energía eléctrica o que permita el acceso al dispositivo. El personal policial registrará en el acta de allanamiento todos los números de serie de las etiquetas de seguridad utilizadas.

Al finalizar el procedimiento, deberán reintegrarse al organismo judicial las etiquetas de seguridad que no hayan sido utilizadas, las que serán resguardadas por un funcionario para usos posteriores.
Una vez que los objetos secuestrados ingresen al laboratorio pericial, se realizará una inspección general, dejando constancia de cualquier alteración o ausencia de etiquetas de seguridad.
Finalizada la pericia, se colocarán nuevas etiquetas de seguridad, detallando los números de serie en el dictamen y se remitirán los secuestros a la dependencia de origen.



Detalle para llenado de la etiqueta de seguridad

A. Número de serie: un identificador único e irrepetible que debe registrarse al colocar la etiqueta de seguridad en un dispositivo informático (se detalla en el acta de allanamiento, oficio elaborado por un funcionario judicial o dictamen del perito).
B. Fecha y hora: la fecha y hora que se realizar el secuestro de la evidencia informática.
C. **Lugar**: se debe especificar en lugar donde hecho.
D. **Evidencia informática**: descripción de los elementos informático.
E. **Causa**: Nombre de la causa si es que existe al momento de realizar el procedimiento.
F. **Nro. de Oficio y Nro. de Expte**: si coloca el número de oficio y/o Expediente si existe al momento de realizar el procedimiento.
G. **Realizado por y Firma** : se colocara el nombre y apellido del que coloco el etiqueta de seguridad seguido de su firma.
H. **Testigo N°1 y Firma**: se colocara el nombre y apellido seguido de su firma de aquella persona que estuvieron al momento de reguardar evidencia digital.
I. **Testigo N°2 y Firma**: se colocara el nombre y apellido seguido de su firma de aquella persona que estuvieron al momento de reguardar evidencia digital.

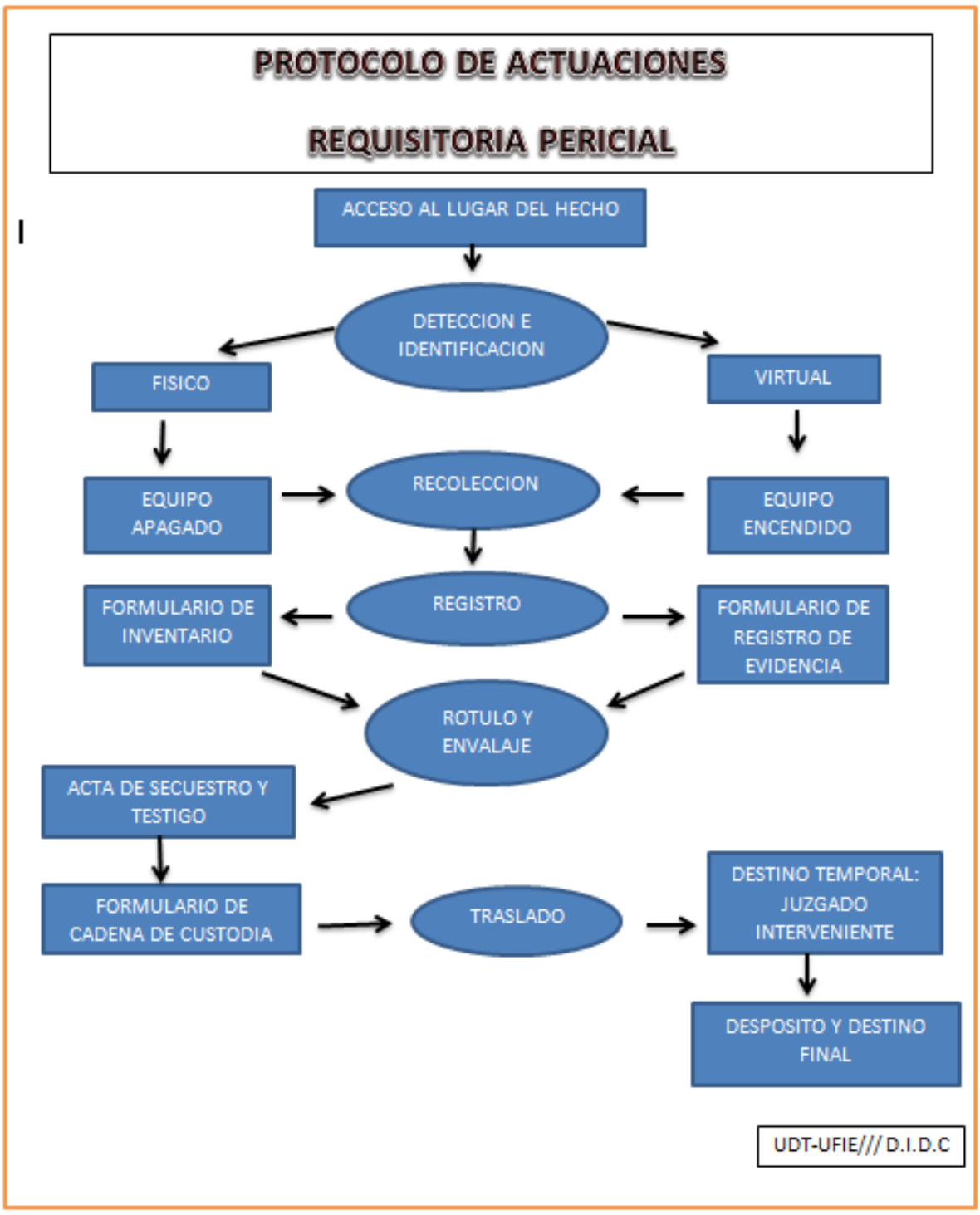
7. Requisitoria pericial

El perito informático forense deberá recolectar la evidencia procediendo de manera acorde al origen del requerimiento de la pericia informático-forense, a saber:

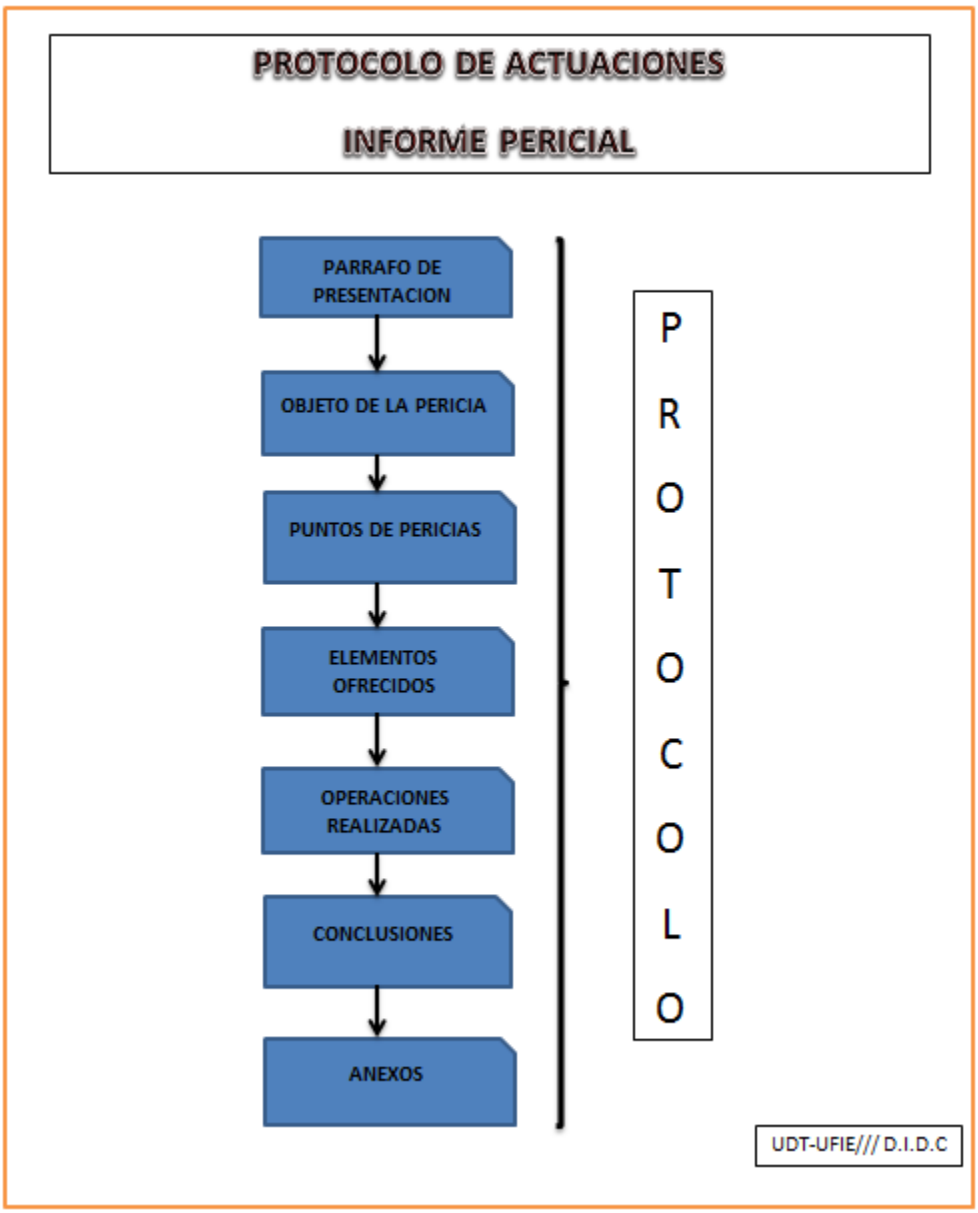
1. Por orden judicial, cuyo texto indica:

a. Secuestrar la evidencia para su posterior análisis en el laboratorio, el perito informático-forense procederá a:

a) Certificar matemáticamente la evidencia.
b) Identificar y registrar la evidencia.
c) Elaborar un acta ante testigos.
d) Iniciar la cadena de custodia.
e) Transportar la evidencia al hasta las oficinas del Juzgado Interviniente.


PROTOCOLO DE ACTUACIONES
REQUISITORIA PERICIAL
ACCESO AL LUGAR DEL HECHO
DETECCION E IDENTIFICACION
FISICO
VIRTUAL
EQUIPO APAGADO
RECOLECCION
EQUIPO ENCENDIDO
FORMULARIO DE INVENTARIO
REGISTRO
FORMULARIO DE REGISTRO DE EVIDENCIA
ROTULO Y ENVALAJE
ACTA DE SECUESTRO Y TESTIGO
FORMULARIO DE CADENA DE CUSTODIA
TRASLADO
DESTINO TEMPORAL: JUZGADO INTERVENIENTE
DESPOSITO Y DESTINO FINAL
UDT-UFIE/// D.I.D.C

8. Protocolo para Informes Técnicos e Informes Periciales



Párrafo de Presentación: En este apartado cuenta con un encabezado solo en la primer página, el cual posee el escudo de la provincia de Corrientes y los datos del área; seguidamente se describe lugar y la fecha de entrega del informe; datos del requirente (nombre del Juez o Fiscal, Juzgado o Fiscalía requirente y ciudad); se detalla el carácter de la pericia a realizar, informando número de Oficio, expediente y carátula.
Objeto de la pericia: Se detalla textual la requisitoria de la solicitud pericial solicitada por el Juzgado o Fiscalías.

Puntos de pericia: Aquí se especifican los procedimientos a realizar en todo el ciclo de vida de la evidencia. (Identificación, Preservación, Análisis y Presentación).
Elementos ofrecidos: Se describe detalladamente todos los elementos secuestrados, aportados por el tribunal requirente. Esta descripción es un cuadro analítico y minucioso de todos los elementos que se peritaran, dejándose constancia el estado de los mismos.
Operaciones realizadas: Este es uno de los puntos más extensos del informe, donde se detalla la metodología implementada y procedimientos llevados a cabo en la pericia. Comenzando a describir las operaciones realizadas en cada etapa del ciclo de vida de la evidencia, cuales son resultados obtenidos en la "Identificación" individualizando su cadena de custodia como así también las imágenes obtenidas en dicha etapa; se describe los procedimientos y resultados obtenidos en la "Preservación" (imagen forense y validación de la misma). Se explicitan los procedimientos, técnicas y herramientas implementadas en el "Análisis" y por último se desbroza la etapa de "Presentación" donde se deja constancia el procedimiento de cadena de custodia y la manera en que es entrega la evidencia al ente requirente (CD, DVD, N° de faja de seguridad, anexos, manuales operativos, entre otros).
Conclusiones: En este punto se dilucidan las herramientas y sus versiones utilizadas en la pericia, las técnicas implementadas, los resultados obtenidos, detallándose los anexos adjuntados y por último se informa que las imágenes forenses utilizadas en la pericia, son eliminadas transcurrido un tiempo determinado, haciendo saber que si por alguna razón es necesario devolver la prueba original, se tomen los recaudos necesarios para su resguardo.
Recomendaciones: Este factor es utilizado en los informes técnicos, luego de haberse brindado en las conclusiones el domicilio desde donde se produjo el supuesto hecho investigado, se detalla los procedimientos de cadena de custodia que se debería llevar a cabo, si el magistrado o funcionario toma la determinación del allanamiento en dicho domicilio. Junto a esos procedimientos se hace mención de todos los elementos Informáticos que se deberían tener en cuenta para secuestrar, según el hecho a investigar.
Anexos: donde se colocar demás documentaciones que se estime agregar sobre el informe pericial.

9. Organización interna de las oficinas de análisis