Protocolo de Actuación
para
Pericias Informáticas

Contenidos

Autor: Dr. Leopoldo Sebastián Gómez

Protocolo de Actuación para Pericias Informáticas

El presente documento tiene por objeto dar a conocer el Protocolo de Actuación para Pericias Informáticas utilizado en el Poder Judicial de la Provincia del Neuquén, detallando la modalidad de trabajo interna para el envío de material tecnológico al laboratorio pericial. La adopción de estos lineamientos permite una correcta definición del alcance de los servicios profesionales de informática forense, contribuye a profundizar los resguardos en la cadena de custodia de la prueba, y explicita la modalidad de trabajo interno para una mejor adecuación de los requerimientos judiciales.

1. Objetivos

a) Evitar la contaminación de la prueba durante el proceso judicial.
b) Formalizar el procedimiento de actuación pericial en materia informática.
c) Definir el alcance de los servicios de informática forense.

2. Procedimiento interno para pericias informáticas

a) Descripción general de servicios de informática forense

A los fines de brindar mayores detalles del quehacer pericial, dando a conocer las áreas de competencia de la pericia informática, es oportuno detallar un catálogo de servicios de informática forense.

Este conjunto de categorías no es taxativo sino descriptivo e informativo. No se trata de un número cerrado de servicios forenses sino que dicha enumeración pretende orientar al operador judicial sobre temáticas en las que es posible plantear requerimientos judiciales. Finalmente serán los puntos de pericia los que deberán contener elementos particulares de información objetiva sobre los hechos investigados, para que el especialista pueda aplicar teorías, técnicas y métodos de análisis forense a través de herramientas especializadas. Sin perjuicio de ello, los requerimientos periciales han de procurar la necesidad real de conocimientos especiales en informática forense, siendo esta disciplina una especialidad de las ciencias informáticas como lo es la medicina legal respecto de la medicina.

Catálogo de servicios [1]
• Pericia sobre infracción a la ley de propiedad intelectual del software.
• Pericia sobre control, actualización y adquisición de licencias de software.
• Pericia sobre robo, hurto, borrado intencional o accesos no autorizados a la información de una determinada empresa o institución, procesada y/o generada por los sistemas de informáticos.
• Pericia sobre duplicación no autorizada de datos procesados y/o generados por los sistemas informáticos.
• Pericia sobre métodos y normas a seguir en cuestión de seguridad y privacidad de la información procesada y/o generada por los sistemas informáticos.
• Pericia sobre la realización de auditorias de áreas de sistemas y centros de cómputos así como de los sistemas informáticos utilizados.
• Pericia sobre recupero de datos borrados y rastreo de información en los distintos medios informáticos (magnéticos – ópticos).
• Pericia sobre métodos y normas a seguir en cuestión de salvaguarda y control de los recursos físicos y lógicos de un sistema informático.
• Pericia sobre desarrollo, manejo e implementación de proyectos informáticos.
• Pericia sobre contratos en los que la informática se encuentre involucrada (contratación de servicios, adquisición de equipamiento informático y de sistemas, tercerización de servicios).
• Pericia sobre aspectos laborales vinculados con la informática. Uso de Internet en el trabajo, uso indebido de las facilidades de la organización otorgadas a los empleados (servicio de correo electrónico, acceso a la navegación por Internet, uso de computadoras, entre otros elementos).
• Pericia sobre robos o determinación de identidad a través de correos electrónicos.
• Pericia sobre aspectos vinculados al comercio electrónico y operaciones realizadas a través de Internet.
• Pericia sobre dispositivos de telefonía celular.

[1] Concordante con los servicios ofrecidos por Peritos: Especialidad en Sistemas Informáticos, definida por el Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires, aprobada por acuerdo de la Suprema Corte de Justicia Provincial el 15/08/2007. http://www.cpciba.org.ar/

b) Del procedimiento general de investigación judicial con tecnología informática

En el ámbito penal, el procedimiento general de investigación judicial utilizando servicios de informática forense consta de dos etapas principales:

a) Incautación confiable de la prueba y mantenimiento de la Cadena de Custodia.

b) Análisis de la información disponible con arreglo al incidente investigado y redacción del informe pericial.

La primera etapa debe ser llevada a cabo por personal policial junto al Fiscal responsable del control o de la ejecución de la medida, siguiendo la "Guía operativa para el secuestro de tecnología Informática".

La segunda etapa debe ser efectuada en el laboratorio por un Perito, siguiendo los estándares de la ciencia forense para el manejo de evidencia digital, en función a los puntos de pericia que sean indicados por los operadores judiciales.

c) De la identificación y preservación de evidencia digital

El Fiscal deberá realizar una planificación minuciosa del procedimiento judicial para la incautación de material probatorio.

La identificación de material tecnológico por parte del personal policial debe ser efectuada conforme las pautas de la "Guía operativa para el secuestro de tecnología informática" que integra el presente documento.

Es de especial importancia la utilización de precintos de seguridad desde el momento del secuestro del material, y todos aquellos medios tendientes a garantizar la autenticidad e integridad de la evidencia digital. 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.

Por regla deberá preferirse el secuestro del material tecnológico a cualquier otra alternativa para la preservación de información digital. Es importante tener presente que existen características únicas de determinado material tecnológico que imposibilita la realización de la pericia informática si no se cuenta con los elementos originales.

Las tareas operativas en el lugar del hecho resultan sumamente dificultosas por el tiempo que requieren las herramientas forenses para completar su ejecución, la carencia de personal policial capacitado para dichas tareas, la escasez de

recursos tecnológicos, y las complejidades técnicas y riesgos asociados al trabajo en un entorno bajo presión. Excepcionalmente, si existiese la posibilidad de preservar la información digital en el lugar del hecho, dichos menesteres deberán ser realizados por personal policial capacitado, con los elementos técnicos adecuados y siguiendo una guía de procedimiento. Ello quedará a criterio facultativo del responsable de la operatoria técnica, quien determinará la viabilidad de la tarea.

d) Del requerimiento judicial

Cuando sea requerido, el Perito evacuará las consultas previas de los operadores judiciales para eliminar ambigüedades y definir el alcance de los puntos de pericia en lo que respecta a los servicios de informática forense.

Conforme lo prescripto por el Código Procesal Penal y Correccional, sólo se podrán requerir informes periciales cuando para descubrir o valorar alguna evidencia sea necesario poseer conocimientos especiales en informática forense. Se debe proveer toda la información necesaria para realizar la tarea pericial, de manera clara y precisa.

El oficio con los puntos de pericia deberá enviarse desde el organismo requirente indefectiblemente junto con el material probatorio que será sometido a análisis forense. En dicho oficio deberán constar los números de serie de las etiquetas que resguardan el material probatorio, y que fueran detalladas en el acta de allanamiento. Una vez que se instrumente el Formulario para Requerimiento del Servicio de informática pericial para todas las dependencias judiciales, éste deberá ser completado por el organismo de origen y enviado al laboratorio pericial como condición excluyente para dar ingreso al pedido de pericia.

Sólo se realizarán pericias que involucren la utilización del hardware y software para informática forense y aquellas que requieran la experticia de un profesional. Quedan excluidas del servicio de pericias informáticas toda tarea administrativa o técnica que no sea propia de la disciplina (tareas de transcripción de texto o simplemente dactilográficas, tareas de ordenamiento de información o cruzamiento de datos, tareas de impresión, tareas de escucha, tareas de filmación, elaboración de copias simples conocidas como backups o de resguardo de dispositivos de almacenamiento de información digital).

En función a la metodología de trabajo establecida para la actividad pericial informática, no se realizan backups sino que se generan “imágenes forenses” de los

dispositivos que contienen información digital (copia bit-a-bit de la evidencia digital –en un formato propietario del software forense utilizado- únicamente a los efectos de realizar sobre ella el análisis forense). La imagen forense es el resultado de un procedimiento metodológico que sirve únicamente para prevenir una posible mala praxis del perito, evitando la contaminación de la prueba. Un backup –por si mismo- es un procedimiento invasivo que altera la evidencia digital y no conserva información digital oculta o remanente que es de especial utilidad para la pericia informática. Los “backups” (copia simple de archivos) son medidas de seguridad informática utilizadas por los propietarios de los equipos informáticos para resguardar sus datos, y deben realizarlos con la frecuencia que estimen conveniente, quedando fuera del alcance de la actividad pericial en informática forense. En una empresa, la realización de backups es responsabilidad del área de sistemas o seguridad de la Información de la empresa. En el caso de un particular, es responsabilidad del propietario del equipo informático.

e) De la priorización de casos urgentes

Únicamente se establecerá prioridad en pericias nuevas sobre aquellas que estén en lista de espera cuando se trate de causas con personas detenidas, debiendo ello ser explícitamente ser indicado en el oficio con el 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 con autores ignorados, 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 pericia en función de la capacidad operativa disponible, las pericias en trámite y aquellas que estén en lista de espera, conforme las estadísticas propias de la actividad.

f) Del traslado y recepción del material secuestrado

Es responsabilidad del personal policial el traslado de todo el material secuestrado hasta los organismos judiciales. Posteriormente el requirente arbitrará los medios necesarios para el envío de los elementos probatorios al laboratorio pericial. Todo el

personal policial o judicial que intervenga en el manejo de la Cadena de Custodia, deberá tener presente las sanciones previstas por el art. 254 y 255 del Código Penal Argentino.

Se cotejará la existencia de los precintos sobre los secuestros y la correcta identificación de los elementos enviados a peritaje. En caso de detectarse la alteración o ausencia de precintos de seguridad, se dejará constancia. Cada una de las personas que haya trasladado los elementos probatorios deberá dejar registrada su intervención con los medios que se establezcan.

g) Del análisis forense

Todo el proceso forense está conducido por una metodología de trabajo para el manejo de evidencia digital. Durante el desarrollo de una pericia se utilizan procedimientos operativos estándares con un control de calidad previo realizado en el laboratorio pericial.

El Perito trabaja con un equipo profesional, con funciones específicas asignadas y una organización interna, tanto administrativa como profesional. Las distintas actividades están segmentadas y pueden separarse, permitiendo un análisis autónomo y específico, sin perjuicio de su unión respecto a un resultado.

Existe una clara distinción de roles dentro del laboratorio, a saber: asistente técnico, perito informático auxiliar y perito informático oficial. Se considera la capacitación interna para llevar adelante la actividad forense, la idoneidad y la responsabilidad asignada, y el nivel jerárquico conforme experiencia y experticia. La definición del alcance y líneas de investigación forense, así como la elaboración de dictámenes queda a cargo de los peritos de mayor jerarquía y experiencia.

h) De la presentación del dictamen

El dictamen será presentado siguiendo los estándares utilizados para la presentación de reportes informáticos forenses. Se intentará minimizar el volumen de información en soporte papel, suministrando toda la información complementaria que sea necesaria para el objeto de la pericia en soporte digital.

i) De la remisión del material secuestrado

Una vez finalizada la pericia, se remitirá el dictamen y el material secuestrado al organismo de origen. Los elementos analizados deberán ser resguardados con los

medios adecuados para preservar la integridad y la autenticidad de la evidencia digital.

Los elementos probatorios que contengan evidencia digital deberán resguardarse hasta finalizar el proceso judicial, siendo imprescindible su conservación ya que permite a futuro -y si fuera necesario- repetir o ampliar la pericia.

3. Guía operativa para el secuestro de tecnología informática

Destinatarios: Personal policial y operadores judiciales.

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, netbooks, 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.

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

Destinatarios: Personal Policial y Operadores Judiciales.

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 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 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”.

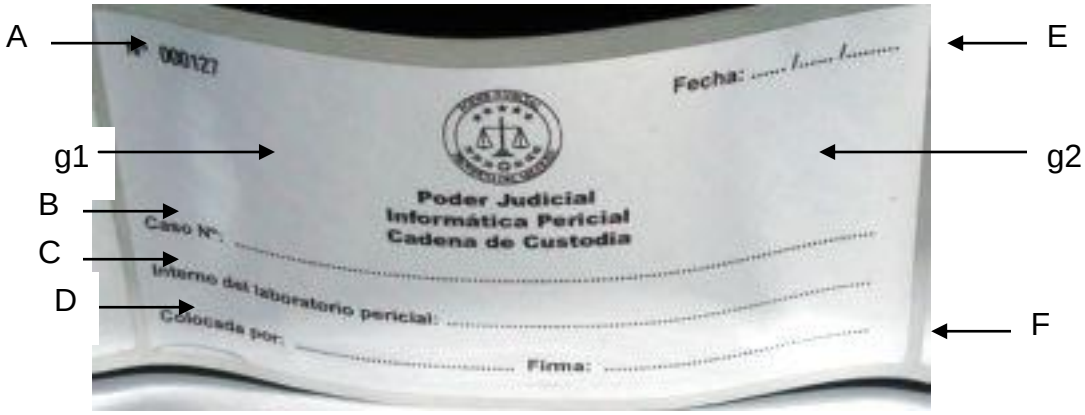
Durante el procedimiento judicial, las etiquetas serán colocadas por el personal policial en todos aquellos lugares que permitan la apertura de un equipo informático, bloqueando cualquier conector de energía eléctrica o que permita el acceso al dispositivo. El personal policial registrará en el acta 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: Número de Expediente-Datos del Juzgado o Fiscalía-Carátula.

Opcional: Lugar donde se encuentra el objeto.

C: Código para uso interno del Laboratorio Pericial (no completar).

D: Nombre y apellido del responsable que colocó la etiqueta de seguridad.

E: Momento en que se realizó el procedimiento judicial. Formato: dd/mm/aaaa

F: Firma del responsable que colocó la etiqueta de seguridad.

g1 y g2: Espacios opcionales para la firma de testigos.