

ADM 9042/20

PROTOCOLO DE ACUERDOS 2020

ACUERDO N° 205.- En la Provincia de San Luis, a TREINTA días del mes de ABRIL de DOS MIL VEINTE, los Señores Ministros del Superior Tribunal de Justicia, Dres. LILIA ANA NOVILLO, CARLOS ALBERTO COBO y MARTHA RAQUEL CORVALAN;

DIJERON: Vista la Resolución de Procuración General N° 168/20 y su Anexo A, remitida para su homologación mediante ESC 760/20, y los informes al respecto de Secretaría de Informática Judicial -actuación 13768740/20- y de la Oficina de Secuestros Judiciales -actuación 13851633/20, efectuados con motivo de la vista que de tal Resolución y Anexo se confiriera en fecha 25/03/2020 -actuación 13720999/20. Por ello:

ACORDARON: I) HOMOLOGAR en todas sus partes la Resolución de Procuración General N° 168/20, actuación 13708794/20, que dispone que la Guía de procedimiento para recolección de muestras, preservación y transporte, que la integra como ANEXO A, constituya el protocolo de actuación obligatoria para el Departamento de Investigaciones de Delitos Complejos del Poder Judicial de la Provincia, la que como anexo forma parte del presente Acuerdo, DETERMINANDO, a esos efectos, que el referido Departamento deberá tener presente el informe de Secretaría de Informática Judicial -actuación 13768740/20, todo lo que obra en el ESC 760/20.-

II) REMITIR al Departamento de Investigaciones de Delitos Complejos y a los Departamentos de Medicina Forense del Poder Judicial de la Provincia, copia de lo planteado por la Oficina de Secuestros Judiciales en actuación 13851633/20, que obra en el ESC 760/20, a fin de que comuniquen a la mencionada Oficina de Secuestros las especificaciones técnicas requeridas, para

la oportuna actualización del Reglamento de la Oficina de Secuestros Judiciales, aprobado por Acuerdo N° 414/2017.-

III) DISPONER que por Secretaría Administrativa se publique el presente Acuerdo en Boletín Oficial y Judicial de la Provincia de San Luis, por un (1) día, y en el link “Acuerdos” del sitio web institucional del Poder Judicial.-

Con lo que se dio por terminado el acto, disponiendo se comuniquen a todos los Organismos del Poder Judicial. –

Poder Judicial San Luis

ESC 760/20

"PROCURACION DICTA PROTOCOLO DE PROCEDIMIENTO PARA RECOLECCIÓN DE MUESTRAS, PRESERVACIÓN Y TRASPORTE."

13708794

RESOLUCIÓN 168/20

San Luis, 19 de marzo de 2020

VISTO:

La necesidad de implementar una guía sobre secuestro, recolección, custodia y traslado de evidencia digital y muestras de residuos de disparo con arma de fuego para la provincia de San Luis, y

CONSIDERANDO:

Las funciones asignadas al Departamento de Investigación de Delitos Complejos y la necesidad y urgencia de establecer lineamientos generales para la unificación de criterios para la recolección de evidencias en el lugar del hecho y su posterior análisis en laboratorio. Ello, en razón de la creciente demanda, dado el cambio de paradigma con respecto a la importancia de las nuevas tecnologías aportadas a la investigación penal.

Que se torna imprescindible contar con guías de actuación para el esclarecimiento de hechos criminales investigados. Ello en procura de la correcta recolección de evidencias, dado que la investigación del hecho puede verse seriamente afectada si las evidencias iniciales que se encuentran en el lugar del hecho no son correctamente recolectadas y preservadas para su posterior análisis. Que, por todo ello, resulta prioritaria y estratégica la aprobación de la

Poder Judicial San Luis

presente guía para su uso por los operadores del sistema en general, auxiliares de la Justicia, funcionarios del Poder Judicial y fuerzas de seguridad.

En uso de las facultades que me otorga la constitución de la Provincia y la ley Orgánica del poder judicial de la Provincia

RESUELVO:

ARTICULO 1.- Disponer que la Guía De Procedimiento Para Recolección De Muestras, Preservación Y Transporte la cual integra el presente como ANEXO A, constituya el protocolo de actuación obligatoria para el Departamento de Investigaciones de Delitos Complejos dependiente de la Procuración General de la Provincia.

ARTICULO 2.- Notificar y hacer saber al Superior Tribunal de Justicia, a fin de que despache las medidas necesarias para la aplicación inmediata del presente protocolo, como así también la armonización con todos los agentes y miembros del Poder Judicial y los de los demás poderes constituidos de la Provincia.

ARTICULO 3.- Protocolizar, notificar y oportunamente archivar.-

La presente actuación se encuentra firmada digitalmente en sistema de gestión informático Iurix por el Dr. Fernando Oscar Estrada, no siendo necesaria la firma ológrafa (Reglamento General del Expediente Electrónico vigente).

ANEXO A

Procuración General de La Provincia de San Luis

GUIA DE PROCEDIMIENTO PARA RECOLECCIÓN DE MUESTRAS, PRESERVACIÓN Y TRANSPORTE.-

La presente guía de actuación tiene como objetivo trazar los lineamientos para el correcto levantamiento, preservación y transporte de los indicios que es de vital importancia para una correcta investigación criminal.

En este sentido, se adecuó esta guía de procedimiento que toma como referencia a varios Ministerios Públicos de la República Argentina, como así también normas internacionales, razón por la cual se redactó el siguiente, para la aplicación en el territorio de la Provincia de San Luis de acuerdo a su geografía, su idiosincrasia, sus procedimientos legales, etc, considerando tales cuestiones al momento de la elaboración del presente documento.

Se pretende realizar un manual de buenas prácticas, donde todas las evidencias que sean susceptibles de análisis pericial dentro del laboratorio del Departamento de Investigación de Delitos Complejos (DIDC) dependiente de Procurador General, contemplen o guarden ciertos parámetros y transparencia para el correcto tratamiento de las mismas y así fortalecer las instituciones que se aúnen para proyectar una excelencia en la calidad de las investigaciones.

Autores:

Líc. Carina Bernal

Ing. David Fuentes



Esquema general del material tratado en la presente guía



Contenido

Tabla de contenido

CAPITULO I	3
INTRODUCCIÓN A LA GUIA SOBRE EVIDENCIA DIGITAL	3
1.1 Contenido.....	3
1.2 El por qué de la Guía de procedimiento de Actuación del Departamento de Investigación de Delitos Complejos.....	4
1.3 Objetivos de esta Guía	4
1.4 Definiciones.....	5
CAPITULO II	6
GUIA OPERATIVA PARA EL SECUESTRO DE DISPOSITIVOS TECNOLÓGICOS	6
2.1 Principios básicos	6
2.2 Criterio	6
2.3 Pasos durante el allanamiento.....	7
CAPITULO III	9
CADENA DE CUSTODIA	9
3.1 Concepto de Cadena de Custodia	9
3.2 Rotulo de Evidencia.....	9
3.3 Modelo rótulo de evidencia de Cadena de Custodia	10
3.4 Planilla de Cadena de Custodia para Transporte	10
3.5 Modelo planilla Cadena de Custodia - Transporte.....	11
CAPITULO IV	12
PROCEDIMIENTO INTERNO PARA PERICIAS INFORMÁTICAS	12



4.1	Procedimiento general de investigación judicial con tecnología informática	12
4.2	Lineamientos y recomendaciones para una optima utilización del servicio de laboratorio	14
CAPITULO V.....		18
EVIDENCIA BALISTICA.....		18
5.1	Muestras de residuos de disparo con arma de fuego.....	18
5.2	Recaudos.....	19
5.3	Procedimiento.....	19
CAPITULO VI.....		21
TRASLADO Y CUSTODIA DE MUESTRAS DE RESIDUOS DE DISPARO CON ARMA DE FUEGO		21
6.1	Protocolo de actuación de traslado y custodia de muestras de residuo de disparo	21
Bibliografía Consultada:		22

CAPITULO I

INTRODUCCIÓN A LA GUIA SOBRE EVIDENCIA DIGITAL

1.1 Contenido

Tomando como referencias diversos protocolos internacionales y siguiendo el camino recorrido por otras provincias con sus **protocolos de procedimientos** ya aprobados por Neuquén, Río Negro, Corrientes, se elaboró el propio para la Provincia de San Luis. Esta guía de procedimiento pretende mostrar de modo cronológico y secuencial las sugerencias y guías para el manejo de evidencia digital y dar a conocer el proceder y el actuar del departamento a los fines de incrementar los niveles de formalidad de la materia, recuperación de evidencia digital, fortaleciendo y mejorado los modelos. Se detallarán



modalidades de recepción de elementos, trabajos internos, envío de material informático al laboratorio, lineamientos del alcance del servicio profesional, resguardo de la cadena de custodia de la prueba pericial desde el momento mismo del secuestro, entrada y salida del laboratorio, adecuación del trabajo pericial al requerimiento judicial y recomendaciones para el secuestro del material tecnológico. Asimismo se intenta que a través del impulso del S. T. J, éste haga extensiva la sugerencia de implementación a los diferentes operadores del Derecho y Fuerza Policial para la pronta puesta en marcha o funcionamiento del efectivo control del tratamiento de la evidencia.

1.2 El por qué de la Guía de procedimiento de Actuación del Departamento de Investigación de Delitos Complejos

Tecnología Aplicada perteneciente del DIDC (Departamento de Investigaciones de Delitos Complejos) es un área que surge de la necesidad de dar respuesta a la demanda de la justicia respecto de la recolección de evidencias significativas o determinantes para ser presentadas como pruebas en un proceso judicial y que permita la identificar a los responsable/s de delito/s tanto informáticos como otros contemplados en el Código Penal y cuya prueba se encuentra conservada en dispositivos de Tecnología de Información (TI).

La amplia diversidad y complejidad de la prueba digital, suele avasallar y sorprender, generando una sensación de desconocimiento sobre la tecnología, es por esto que es importante la consulta por parte del magistrado para con DIDC, acompañando en la dificultad para especificar los puntos de pericia desde el vocabulario técnico, surge la necesidad de formalizar los procedimientos para la recolección de la prueba y cadena de custodia, análisis y diagnóstico tecnológico, y la elaboración del informe técnico de pericia. Esta formalización permite ajustar el procedimiento a una norma que garantice la utilización de criterios metodológicos y buenas prácticas en la actividad de incautación de la evidencia digital. Es de suma importancia tratar de individualizar acciones adecuadas que puedan llevarse a cabo cuando se trata de recuperar potenciales fuentes de evidencias digitales.

1.3 Objetivos de esta Guía

- Formalizar el procedimiento de actuación pericial en materia tecnológica.
- Definir el alcance de los servicios del área de Tecnología Aplicada.
- Minimizar demoras de la comunicación y lograr eficiencia en la labor diaria a raíz de la comprensión de los protocolos.



- Alfabetización tecnológica sobre la evidencia digital.
- Evitar la contaminación de la prueba durante el proceso judicial.
- Priorización de la cadena de custodia.

1.4 Definiciones

La **Evidencia digital** es la información que se encuentra en los dispositivos tecnológicos. De acuerdo con el HB:171 2003 "Guidelines for Managment of IT Evidence" evidencia digital es cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" o "también es considerada evidencia digital a cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal".

El informático forense es "la persona que permitirá avanzar en la búsqueda de la verdad, en el análisis de la información residente en los dispositivos tecnológicos y realizar una reconstrucción de los hechos en base a la evidencia digital analizada"

La Informática Forense consiste en métodos científicos comprobables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar la evidencia digitales procedentes de fuentes digitales con el propósito de hacer posible la construcción de hechos considerados delictivos.

La Prueba indiciaria así lo define la ciencia de la criminalística, al conjunto de huellas de cualquier tipo y naturaleza, que se hayan producido como resultado de una acción cualquiera y que al ser metodológicamente investigados, permiten reconstruir los hechos acaecidos. En General, pero no de manera excluyente, se relacionan con actos delictivos.



CAPITULO II

GUIA OPERATIVA PARA EL SECUESTRO DE DISPOSITIVOS TECNOLÓGICOS

2.1 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. 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 magistrado 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.

2.2 Criterio

Cualquier sistema informático no se deberá identificar como evidencia sólo porque se encuentran en el lugar. La recolección de los elementos debe ser justificada por autoridad competente, por lo que la autoridad que ordenó la búsqueda debe tomar una decisión consciente de que si un artículo está siendo recolectado, este, debe tener una sospecha razonable o evidencia suficiente que justifique el hecho, para así evitar atestar los laboratorios con evidencias no pertinentes. Debe evitarse salvo orden expresa, el secuestro masivo de elementos, en especial CDs, DVDs, móviles rotos, viejos, guardados o en aparente estado de desuso. Tampoco partes de computadoras que no posean almacenamiento de información. Hay que primar la recolección de los artículos tecnológicos personales y de uso diario.



2.3 Pasos durante el allanamiento

- 2.3.1 Se deben separar las personas que trabajen sobre los dispositivos tecnológicos 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 y dejarlas registradas en el acta de allanamiento.
- 2.3.2 Se deben procurar fotografiar todos los equipos informáticos antes de moverlos o desconectarlos. Realizar una toma fotográfica 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.
- 2.3.3 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.
- 2.3.4 Para evitar que los dispositivos sigan recibiendo datos de comunicaciones, o cualquier otro tipo de instrucción remota que pueda alterar la información, tener en cuenta que: 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 son notebooks o netbooks, es necesario removerle la batería. Para el caso de dispositivos móviles, como medida de seguridad, activar el “modo avión” antes de apagarlo y luego remover la batería. En caso de no poder remover la batería, apagarlo y proteger el botón de encendido con un cartón pegado con cinta para evitar el encendido accidental.
- 2.3.5 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).



- 2.3.6 Se debe realizar una descripción en el acta de los elementos de tal modo que sean diferenciadores, mencionando características individuales de los dispositivos, se deberá determinar por ejemplo, números de serie, marca, modelo, IMEI (cuando es un smartphone, estos datos se encuentran en etiqueta pegado detrás de la batería) y una breve descripción de lo que se observa como estado general. Completar el rótulo de la evidencia según modelo proporcionado en esta guía y el posterior llenado de la Cadena de Custodia-Transporte.
- 2.3.7 Cuando se trate de discos rígidos y otros dispositivos de almacenamiento informáticos que sean sensibles o sus circuitos electrónicos estén expuestos al contacto debe utilizarse una buena cantidad de papel madera para embalarlo sin temor a exagerar en el envoltorio.
- 2.3.8 Resguardar de cada equipo informático todas sus entradas eléctricas y todas las partes que puedan ser abiertas o removidas. Pudiendo utilizar para ello hoja de papel firmada y pegada con cinta. Es responsabilidad del personal capacitado que participa en el procedimiento el transporte sin daños ni alteraciones de todo el material informático hasta que sea peritado.
- 2.3.9 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.
- 2.3.10 Completar y mantener la cadena de custodia del material informático transportado. Es responsabilidad del personal asignado, el traslado de la evidencia que sea objeto de pericia informática en sede judicial. No se podrá asegurar la integridad de la evidencia digital si el material informático tiene roto fajas o precintos al momento de ser entregado, se deberá dejar asentado en la guía de transporte de la cadena de custodia.
- 2.3.11 Cuando haya equipos muy específicos (equipos electrónicos de salud, mediciones, fiscales, etc) y que tengan relación directa al hecho que se investiga y se deban secuestrar, deben identificarse con etiquetas con números los cables para indicar dónde se deben conectar. Así también, se deberán fotografiar los equipos con sus respectivos cables de conexión etiquetados.



CAPITULO III

CADENA DE CUSTODIA

3.1 Concepto de Cadena de Custodia

La CoC (Cadena de Custodia por sus siglas en Inglés) se entiende como “el control que se efectúa tanto de las personas que recogen la evidencia como cada persona o entidad que posteriormente tiene la custodia de la misma”. Este control es un registro que permite conocer el o los movimientos de la evidencia en el proceso, observaciones de cambio e identificar a los responsables que tomaron contacto con la misma.

Este registro debe contar con elementos identificadores mínimos y particulares que pueden ser los siguientes:

- Un identificador univoco de la evidencia.
- Quién accede a la prueba o evidencia, en qué momento y en qué ubicación física.
- El pasaje de la prueba o evidencia de un sitio a otro y la razón.
- Cualquier cambio inevitable potencial en la prueba o evidencia será registrado con el nombre del responsable y la justificación de sus acciones.

3.2 Rotulo de Evidencia

Cada muestra recolectada, debe llegar al laboratorio correctamente identificada y debidamente acondicionada en su contenedor a los fines de garantizar la autenticidad e integridad de la misma; esto es lo que se denomina rotular.

La información de cada rótulo de evidencia debe contener al menos:

- Lugar, hora y fecha donde fue colectada.



- Carátula y número de causa y/o actuación policial.
- Descripción de la evidencia.
- Autoridad/Juez interviniente.
- Tipo de diligencia o pericia.
- Nombre, apellido, DNI y rango de quien recolectó y acompañante.
- Número único asignado a rótulo, coincidente con su planilla de transporte.

Este rótulo debe estar pegado en el elemento secuestrado o sobre, caja o envase que lo contenga.

3.3 Modelo rótulo de evidencia de Cadena de Custodia

Pegado en Sobre

Rótulo de evidencia de Cadena de Custodia		
		Numero Único:
Procedimiento:		
Fecha:	Hora:	Dirección del Secuestro:
Descripción del Paquete:		
Descripción de la evidencia:		
Juzgado/Dependencia policial:		
Levantado por: (nombre completo, DNI)		Cargo:
Levantado por: (nombre completo, DNI)		Cargo:
Observaciones (Indicaciones Juez):		

3.4 Planilla de Cadena de Custodia para Transporte

Deberá confeccionarse además del rótulo de evidencia, una planilla de cadena de custodia (para transporte), esto debe acompañar a cada paquete de cada elemento secuestrado, debe estar completa y firmada por cada uno de los actores intervinientes de las etapas.

En cada línea del registro de continuidad del elemento materia de prueba o evidencia física (CoC-Transporte), debe contener:

- La descripción del elemento contenido dentro del sobre.



- El número único que debe coincidir con el rotulo del sobre.
- Sección indicando DE (quien transporta) y sección indicando PARA (quien recibe)
- En las secciones indicar la fecha de izquierda a derecha consignando el día, mes y año en los cuales se realiza el traslado y/o traspaso del elemento materia de prueba o evidencia.
- El campo con el organismo que envía o recibe (DE, PARA)
- Nombre, apellido, DNI y firma de quien transporta y recibe.
- Notificar en calidad de qué actúa, pudiendo ser custodio, perito o transportador.
- Indicar el propósito del traspaso de la evidencia, pudiendo ser estudio o análisis, desplazamiento de un lugar a otro, presentación en audiencia o disposición final.
- Indicar que autoridad dispuso el traslado, consignando firma y nombre.
- Indicar si hay novedades con respecto al estado general de la evidencia o sobre.

3.5 Modelo planilla Cadena de Custodia - Transporte

Lo que se muestra a continuación es un ejemplo para un solo movimiento de la evidencia, es recomendable que la planilla tenga para cuatro movimientos.

Acompaña a Sobre

Cadena de custodia - TRANSPORTE									
Descripción elementos:							Numero Único:		
DE:	FECHA		ORGANISMO		NOMBRE Y APELLIDO		Firma		
	D	D	M	M	A	A			
	Hora:				DNI:				
	Calidad en la que actúa:		Propósito del traspaso:		Autoridad que autoriza el traslado				
	A) Custodio B) Perito C) Transportador		1) Estudio o Análisis 2) Desplazamiento de un lugar a otro 3) Presentación en audiencia 4) Disposición final		FIRMA:				
Estado general de la evidencia/Sobre: (Observaciones)									
PARA:	FECHA		ORGANISMO		NOMBRE Y APELLIDO		Firma		
	D	D	M	M	A	A			
	Hora:				DNI:				



CAPITULO IV

PROCEDIMIENTO INTERNO PARA PERICIAS INFORMÁTICAS

4.1 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 fases principales:

Fase 1) **Incautación confiable de la prueba y mantenimiento de la Cadena de Custodia.**

La primera fase debe ser llevada a cabo por personal capacitado junto a Secretario o Juez responsable del control o de la ejecución de la medida, siguiendo "La Guía Operativa Para El Secuestro De Dispositivos Tecnológicos" descrita en el Capítulo II.

Fase 2) **Preservación, adquisición, análisis de la información disponible y redacción del informe pericial.**

La segunda fase 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 Magistrados y Funcionarios.



4.1.1 Preservación

También denominada como etapa de resguardo, es la obtención de la información a analizar. En esta etapa se debe garantizar que no se pierden indicios y evidencias que deben obtenerse para su análisis, siendo un requisito necesario para el inicio de la cadena de custodia del material informático intervenido que es recibido en el laboratorio. Es importante corroborar que la descripción del material informático recibido coincida y el estado del mismo. Personal del departamento actuará como fedatario en el momento de apertura de embalajes y



dejando asentado en el sistema informático de registro de evidencias lo actuado, las descripciones y características del material y registro fotográfico de todas las partes incluida la documentación que acompaña, asignándole en esta instancia una etiqueta numerada para su individualización durante la estadía en el departamento y depósito en un lugar adecuado para su correcta preservación.

4.1.2 Adquisición

Realización de Copia forense de la evidencia y cálculo de la clave “hash” a los fines de salvaguardar la información. La copia forense es la copia bit a bit del material incautado (un bit es la porción más pequeña de la información almacenada) realizada con técnicas forenses que garantiza la no alteración del material original y certificando mediante un código alfanumérico de dicha información (el denominado hash, que vendría a ser el ADN del archivo o conjunto de estos ya tratado). En este punto es importante resaltar la aplicación de métodos que reza la norma de la práctica de informática forense a nivel internacional ISO/IEC 27037:2012 y que dice: La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.

4.1.3 Análisis

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. Se utilizarán en esta etapa, tanto hardware como software analíticos para la revisión de documentos, todo esto específicamente diseñados para el análisis forense. Siempre que la realidad de las etapas anteriores lo permitan, se trabajará únicamente sobre las copias forenses.

4.1.4 Informe

En el informe, el lenguaje empleado será técnico y se harán comentarios tendientes a su comprensión por personal no técnico, cuando así se lo considere necesario. No se entregará ninguna parte del mismo impreso, todo se elevará por sistema o por el soporte adecuado a su tamaño. El informe contará con la siguiente información:

- 4.1.4.1. Párrafo de Presentación: Se detallan los datos del numero de oficio y autos.
- 4.1.4.2. Objeto de la Pericia y los puntos de pericia: Se especifican los objetivos y los puntos de pericias establecidos por el Organismo interviniente.
- 4.1.4.3. Elementos Ofrecidos: En este apartado se detalla todos los elementos ofrecidos por el Juzgado (elementos informáticos “evidencia digital”, prueba documental, otros informes periciales y demás pruebas por el organismo que sirvan para la investigación).
- 4.1.4.4. Operaciones Realizadas: A partir de los Puntos de Pericias y los elementos ofrecidos, se detallará la metodología de trabajo, técnicas, y procedimientos que llevo a realizar la pericia encomendada.



- 4.1.4.5. Conclusión: con el desarrollo de las operaciones realizadas, se especificará los resultados obtenidos, especificando Anexos, elementos que serán entregados junto al informe pericial, entre otros.
- 4.1.4.6. Observaciones: Informar del estado de cómo fue recepcionada la evidencia o su envoltorio si esta fuere algo fuera de lo común.
- 4.1.4.7. Recomendaciones: Si fuese necesario se especificaran pasos a seguir como ser: medidas de secuestros, oficios a empresas prestadoras de servicios de internet, lo que ayude a una ampliación o u obtención de mayores pruebas que pueda ser útil a la investigación.

El objetivo es utilizar un estándar de informe claro y preciso, suministrando toda la información complementaria que sea necesaria para el objeto de la pericia en soporte digital.

4.2 Lineamientos y recomendaciones para una optima utilización del servicio de laboratorio

4.2.1 Del requerimiento judicial y procedimiento de consulta al magistrado

Cuando sea requerido, el perito estará a disposición para las consultas de los magistrados a los fines de eliminar ambigüedades y definir el alcance de los puntos de pericia en lo que respecta a los servicios de informática forense. La información necesaria a proveer para una optima tarea puede ser: fijaciones de ordenes de relevancia, determinación de cuando es suficiente lo hallado para un determinado propósito investigativo o probatorio, proporcionar criterio para el filtrado de datos, periodos temporales de análisis, entre otros.

Sólo se podrán requerir informes periciales cuando para descubrir o valorar alguna evidencia sea necesario poseer conocimientos especiales en informática forense y la utilización del hardware y software específico.

Se debe tramitar el oficio relacionado con los puntos de pericia o tarea encomendada la cual deberá enviarse desde el organismo requirente indefectiblemente junto con el material probatorio que será sometido a análisis forense.

4.2.2 De las Tareas Excluidas

Quedan excluidas del servicio del laboratorio 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).



4.2.3 De la asignación de turnos

Recibido el oficio para la realización de la pericia, salvo casos urgentes con habilitaciones (explicado en el próximo punto) se asignará turno en función de la cantidad de material probatorio provisto dividiéndose en 3 plazos de tiempos.

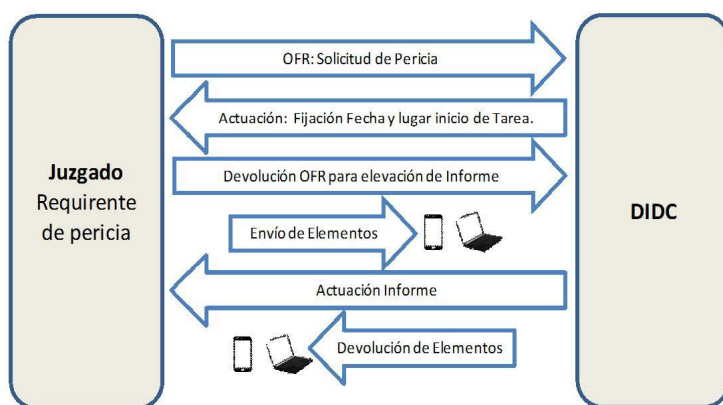
Corto plazo, cuando se provea de 1 a 2 elementos

Mediano plazo, cuando provean de 3 a 5 elementos

Largo plazo, cuando se provean de 6 a más elementos

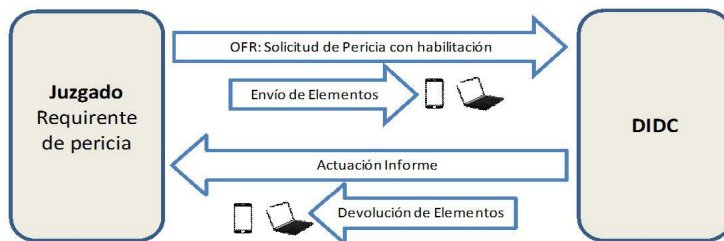
El esquema de Protocolo de Actuaciones de Solicitud de Pericias, se presenta en la siguiente figura, todos los pases están habilitados en el sistema de gestión de expedientes.

4.2.4 Esquema sin habilitación





4.2.5 Esquema con habilitación



4.2.6 De la priorización de casos urgentes

Se establecerá exenciones sobre el orden en la lista de asignaciones de turno 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 solicitudes de pericias informáticas con el mismo nivel de urgencia, se dará trámite por orden de ingreso.

4.2.7 De la cancelación y/o reasignación del turno pericial

En caso de que el juzgado requirente de la pericia no envió los elementos secuestrados en tiempo, o la persona citada no se hace presente, se le devolverá el oficio indicando el motivo y será responsabilidad del juzgado la nueva solicitud de turno ajustándose al régimen de asignación de turnos descripto anteriormente.

4.2.8 Del almacenamiento de la información post entrega de informe

Este departamento no realiza resguardo de datos obtenidos tras la recuperación mediante técnicas forenses. Luego de la entrega del informe al juzgado solicitante al finalizar la pericia, si esta se perdiera o dañara se deberá solicitar una nueva pericia, aportando nuevamente los elementos secuestrados.

4.2.9 De la audiencias post pericia

Las audiencias, rectificatorias, aclaratorias, etc, solicitadas a los miembros del departamento, se deberán notificar con un mínimo de 48 hs de anticipación, debiendo ser estas siempre posteriores al acto de revisión de los informes periciales y/o análisis por parte del personal del juzgado solicitante. Las audiencias que sean en el interior provincial se sugiere puedan ser realizadas mediante el sistema de videoconferencia con que cuenta actualmente el Poder Judicial.

4.2.10 Del traslado y recepción del material secuestrado



El requirente arbitrará los medios necesarios para el envío de los elementos probatorios al Laboratorio del Departamento Pericial. Allí se cotejará, la cadena de custodia y la correcta identificación de los elementos enviados a peritaje. En caso de detectarse la alteración o ausencia del envoltorio de los elementos se dejará constancia, como así también los datos del responsable que haya trasladado los elementos probatorios.

4.2.11 De la remisión del material secuestrado

Una vez finalizada la pericia, se remitirá el dictamen por sistema y el material secuestrado al organismo de origen. El material que fuera secuestrado y remitido por el departamento contara con envoltorio nuevo, dentro del mismo se encontrará el material y ensobrado anterior, todo esto rotulado con los datos de interés y su respectiva cadena de custodia de transporte, la cual tendrá asentado el nuevo traslado indicando la persona responsable de dicho pase.



CAPITULO V

EVIDENCIA BALISTICA

5.1 Muestras de residuos de disparo con arma de fuego

Luego de efectuar un disparo con arma de fuego, algunos residuos —compuestos por pólvora y restos de material del proyectil— pueden depositarse sobre la/las manos del tirador y prendas de vestir. Este residuo varía en función del tipo de arma y la munición utilizada. En el análisis por GSR (gunshot residue), se detectan principalmente pequeñas trazas de residuo del fulminante. Los residuos depositados sobre las manos disminuyen rápidamente durante la primera hora posterior al disparo. En la práctica no es esperable encontrar residuos de disparo después de las doce horas posteriores, cuando se trata de un individuo vivo. Sin embargo, en caso de suicidios, los GSR pueden durar varias horas después del hecho. Preferentemente, las muestras deben ser tomadas inmediatamente después del contacto con el sujeto en el campo.

Este procedimiento es necesario para todas las muestras que tengan que ser colectadas, ya sea en prendas, personas o cosas en el lugar del hecho o en el laboratorio.

- 5.1.1 **Operador:** serán estos quienes, utilizando las instrucciones adjuntas en el presente documento, llevarán adelante la toma de muestras en cadáveres y personas vivas.
- 5.1.2 **GSR (Gunshot residue):** Los residuos de disparo o residuos GSR “son los residuos depositados en las manos y la ropa de algún individuo que se encuentra en el entorno cercano a un punto geográfico donde se ha disparado o detonado un arma de fuego”.
- 5.1.3 **STUBS:** soporte contenedor compuesto por un adhesivo disco de carbono, que permite la adherencia de las partículas a analizar, dentro de un recipiente herméticamente cerrado.



5.1.4 MEB: Microscopia Electrónica De Barrido

5.2 Recaudos

Para este tipo de muestras, el operador debe tener los siguientes recaudos:

- 5.2.1 Utilizar, al menos, un muestreador por mano, quedando a criterio del perito la toma de otras muestras.
- 5.2.2 Realizar, antes de cualquier recolección de GSR, un examen visual de las manos y muñecas del sujeto que recolecta la muestra de los involucrados en el hecho.
- 5.2.3 Tomar fotografías de las manos y, especialmente, de las zonas que presenten ennegrecimiento.
- 5.2.4 Lavar cuidadosamente las manos y antebrazos antes de manipular los materiales para evitar contaminación de las muestras.
- 5.2.5 Evitar en lo posible tomar contacto con las manos del sujeto.
- 5.2.6 No desplazar o manipular a la persona sospechosa de haber accionado un arma de fuego.
- 5.2.7 Evitar que el sujeto se lave o frote las manos antes del muestreo.
- 5.2.8 No tomar las impresiones digitales antes del muestreo.
- 5.2.9 No esposar las manos del sujeto detrás de la espalda.
- 5.2.10 Las muestras en sospechosos vivos deben ser tomadas antes de las 12 h posteriores a ocurrido el hecho.

5.3 Procedimiento

Para el levantamiento de la muestra, se sugiere seguir el siguiente procedimiento:

- 5.3.1 Seleccionar un disco muestreador, destaparlo y mantenerlo con el disco adhesivo hacia abajo.
 - 5.3.1.1. Mano derecha (utilice un muestreador para palma y dorso): zona A.
 - 5.3.1.2. Mano izquierda (utilice un muestreador para palma y dorso): zona B.
 - 5.3.1.3. Cara y cabello (utilice un porta muestras para esta colecta): zona C.
 - 5.3.1.4. Mangas de la prenda utilizada en el momento de ocurrido el hecho (un porta muestra para ambas mangas): zona D.
 - 5.3.1.5. Zona anterior de la prenda, utilizada en el momento de ocurrido el hecho o cualquier otro elemento que el Operador pueda inferir la existencia de residuos de disparo de acuerdo a los lineamientos establecidos en el presente. zona E.



- 5.3.2 Retirar el film protector del disco de elemento carbono, en caso que lo tuviera, con una pinza de punta fina. Asegurarse de no tocar ninguna cosa con el adhesivo, solo tocar las manos de la persona sospechosa.
- 5.3.3 Tomar el disco adhesivo con el soporte (stubs) y presionar firmemente sin deslizar contra las manos del sospechoso o detenido siguiendo el patrón sistemático, hasta que se pierda la adherencia del disco.
- 5.3.4 Repetir los pasos utilizando un stubs por cada mano.
- 5.3.5 Una vez terminada la recolección, colocar la tapa al stubs y rotular.
- 5.3.6 Respetar los mismos pasos por cada muestreo y preservar los stubs junto a una planilla de datos en lugar seco y al abrigo del calor.
- 5.3.7 En caso de prendas de vestir, siempre deberá enviarse al LABORATORIO la ropa intacta, separadamente, en bolsas de papel, sin doblar o separando las porciones de género con un papel, con la menor manipulación posible, acompañada de una breve descripción del hecho (número y localización de los daños aparentes).
- 5.3.8 Cuando se está en presencia de un cadáver con sospecha de suicidio, al efectuar la recolección se requiere determinar un desnivel de distribución de residuos para concluir la existencia o no de suicidio.
- 5.3.1.6. Se deben realizar colectas distintas en: dorso de la mano derecha, palma de la mano derecha, dorso de la mano izquierda y palma de la mano izquierda.

En lo que respecta al operador, en virtud de contar el Poder Judicial de San Luis, con un cuerpo Médico Forense en sus tres circunscripciones dotadas de Médicos, Ayudantes médicos e idóneos, es conveniente que sean estos los que realicen la toma de muestras en personas vivas y en cadáveres. Con respecto a los cadáveres, de acuerdo a los lineamientos trazados aquí, el Operador a su criterio profesional decidirá el lugar para realizar la toma de muestra (lugar del hecho/hallazgo o Morgue Judicial). Y si de personas vivas se trata, S. S. a sabiendas de la presente técnica puesta a disposición para la investigación científica del hecho, tendrá a su criterio el uso y aplicación con el Operador propiamente dicho.-



CAPITULO VI

TRASLADO Y CUSTODIA DE MUESTRAS DE RESIDUOS DE DISPARO CON ARMA DE FUEGO

6.1 Protocolo de actuación de traslado y custodia de muestras de residuo de disparo

A los fines de garantizar el correcto traslado y custodia de la/s evidencias que surgieran del levantamiento de muestras de residuos de disparo para ser analizadas en el Laboratorio de Microscopia Electrónica de Barrido del Cuerpo Médico Forense y Criminalístico de la Provincia De Mendoza cuyo Laboratorio Regional de Investigación Forense está a disposición de los miembros del Consejo de Procuradores, Fiscales, Defensores y Asesores Generales de la República Argentina, es necesario establecer lo siguiente:

- 6.1.1 Que de acuerdo a la naturaleza de la causa, resulte disponer de los resultados periciales en un plazo perentorio, se arbitren los medios a fin de obtener los resultados de la prueba tratando que dicho plazo no sea mayor de 24 horas. Se solicita al Superior Tribunal de Justicia de San Luis que arbitren las medidas necesarias para el cumplimiento de lo cometido.
- 6.1.2 De no mediar la urgencia en la ocasión, se fijará fecha de realización de Pericia previo mandamiento judicial que así lo ordene, para llevar las muestras acumuladas, ello a fin de evitar gastos innecesarios y al solo fin de optimizar los recursos materiales.
- 6.1.3 Para el cumplimiento de la Prueba Pericial y en resguardo de la cadena de custodia y a fin de evitar nulidades procesales, el traslado de las muestras será asignación del Departamento de



Investigación de Delitos Complejos exclusivamente o a quien los responsables designen previa homologación de Procuración General..-

Bibliografía Consultada:

El material bibliográfico de referencia que se utilizó para la elaboración de la “guía de procedimiento para recolección de muestras, preservación y transporte” es el siguiente:

1. Poder Judicial de la Provincia de Neuquén (2013). *Protocolo de actuación para pericias Informáticas*. Neuquén: Gómez.
2. Poder Judicial de la Provincia de Río Negro (2014). *Protocolo de Actuación del Departamento de Informática Forense*. Río Negro: Semprini G.
3. Normas Internacionales ISO/IEC 27.042.2015 (2015). *Guía para Análisis e Interpretación de Evidencia Digital*.
4. Gómez, L. (2006). *Guía Operativa para Procedimientos Judiciales con secuestro de Tecnología Informática*.
5. Poder Judicial de Río Negro (2016). *Lineamientos para la creación de laboratorios informáticos forenses*. Río Negro: Semprini G
6. Consejo federal de Política Criminal (2017). *Protocolo unificado de los ministerios públicos de la República Argentina*. CABA: Libro digital, EPUB.
7. Ministerio de Seguridad de Santa Fe (2016). *Guía de Manipulación y secuestro de dispositivos electrónicos, investigación de la escena del crimen electrónica*. Rosario.
8. Ministerio Público Fiscal de la Provincia de Corrientes (2016). *Protocolo de Actuaciones para Informática Forense*. Corrientes.
9. Facultad de Ingeniería de La Universidad Católica de Salta (2015). *Plan estratégico para la implementación de un Centro de Servicios de Informática Forense*. Salta: Appendino, Aprile, De Gallo.
10. Bielli, G. y Ordoñez, C. (2019). *La Prueba electrónica. Teoría y Práctica*. Buenos Aires: Tomson Reuters.