, Poder Judicial - Provincia de Santa Cruz Tribunal Superior de Justicia

TOMO: CVI

REGISTRO: 1J 2?

FOLIO \JboliM

Río Gallegos, de Diciembre de 2.019.- Y VISTO:

El Oficio N° 309/2019 - elevado por la Perito Informático y de Telecomunicaciones “E” Ing. Adriana Laura IBARRETA FAÑANAS, quién desempeña funciones en el Cuerpo Pericial de Informática y Telecomunicaciones dependiente de la Secretaría de Superintendencia y Jurisprudencia del Excmo. Tribunal Superior de Justicia; y,

**CONSIDERANDO:**

Que, mediante dicha presentación remite Protocolo de Actuaciones para Pericias Informáticas en la provincia de Santa Cruz, confeccionado por la dependencia judicial citada precedentemente.-

Que, habiendo tomado intervención S.E. la Señora Secretaria- María Teresa GURUCEAGA, titular de la Secretaría de Superintendencia y Jurisprudencia del Excmo. Tribunal Superior de Justicia, eleva las presentes a consideración del Alto Cuerpo, a los fines de su aprobación; dejando constancia que dicho protocolo fue consensuado con el personal policial especializado en la temática.-

Que, en atención a lo expuesto y lo considerado por los miembros del Excmo. Tribunal en la oportunidad de celebrarse el Acuerdo Ordinario N° 3.528 (30.10.2019) deviene adecuado APROBAR el Protocolo de Actuaciones para Pericias Informáticas en la provincia de Santa Cruz confeccionado por el Cuerpo Pericial de Informática y Telecomunicaciones dependiente de la Secretaría de Superintendencia y Jurisprudencia del Excmo. Tribunal Superior de Justicia .-

Por ello, y atento las atribuciones conferidas por el Artículo 34° de la Ley Provincial N° Uno (según texto ordenado Ley N° 1.600) y lo dispuesto por Resolución asentada T° CCXI, R° 20, Fs. 25/27, S.E. la Señora Presidente del Alto Cuerpo - Dra. Paula E. LUDUEÑA CAMPOS, “Ad-Referéndum” del EXCMO. TRIBUNAL SUPERIOR DE JUSTICIA,

RESUELVE:

1o) APROBAR el Protocolo de Actuaciones para Pericias Informáticas
en la provincia de Santa Cruz, identificado como Anexo I y que forma parte de la presente;
confeccionado por el Cuerpo Pericial de Informática y Telecomunicaciones dependiente de la
Secretaría de Superintendencia y Jurisprudencia del Excmo. Tribunal Superior de Justicia.-

2o) Regístrese.- Comuniqúese.- Tome nota

(Prosecretaría).-

aps

PRESIDENTE

TRIBUNAL SUPERIOR DE JUSTICIA



RESOLUCIÓN REGISTRADA EN PROSECRETARÍA EL DÍA **?.**

JORGE ANTONIO BAQUINSAY

JEFE DE DEPARTAMENTO

PROSECRETARÍA

TRIBUNAL SUPERIOR DE JUSTICIA



ANEXO I

TOMO: CtfJ REGISTRO://3 FOLIO

Protocolo de Actuación
para Pericias
Informáticas en la
Provincia de Santa Cruz



CUERPO PERICIAL DE INFORMÁTICA Y TELECOMUNICACIONES
TRIBUNAL SUPERIOR DE JUSTICIA

2019

PODER JUDICIAL PROVINCIA DE SANTA CRUZ
CUERPO PERICIAL DE INFORMÁTICA Y TELECOMUNICACIONES

**índice**

1. [Objetivos 3](#bookmark3)

Alcances 4

* Delitos informáticos: 4
* Manejo de datos: 5
* Reconocimiento de hardware y software: 5
1. [Del Secuestro de tecnología informática 5](#bookmark4)
2. Identificación de los elementos informáticos 5
3. Buenas prácticas para el secuestro de evidencia digital. 6
4. El ciclo de la cadena de custodia de la evidencia digital. 7
5. Recorrido de la evidencia 8
6. Traslado y recepción del material secuestrado 9
7. [El Requerimiento Judicial 10](#bookmark5)

Solicitud de fecha de pericia informática y en telecomunicaciones al Cuerpo Pericial de Informática y Telecomunicaciones del Poder Judicial 10

1. [El análisis forense 11](#bookmark6)
2. [Informes Técnicos e Informes Periciales 11](#bookmark7)
3. [Bibliografía 13](#bookmark9)

ANEXO I

TOMO: C\J\ REGISTRO: i i 3 FOLIO: i 3o/i2>6



PODER JUDICIAL PROVINCIA DE SANTA CRUZ
CUERPO PERICIAL DE INFORMÁTICA Y TELECOMUNICACIONES

Protocolo de actuación para pericias informáticas en la

provincia de Santa Cruz

En este escrito se presenta el protocolo de actuación respecto a pericias informáticas y en telecomunicaciones propuesto para ser aplicado en la provincia de Santa Cruz.

Ante la apertura del Cuerpo Pericial de Informática y Telecomunicaciones dependiente de Tribunal Superior de Justicia del Poder Judicial de la Provincia (Resolución asentada en Tomo CCXXIV, Registro 07, Folio 09), y dado que esta área debe trabajar en conjunto con los distintos Juzgados, tanto de Instrucción como de Primera Instancia en lo Civil, Comercial y Laboral, de diferentes localidades de la provincia, se detecta la necesidad de contar con una estandarización en lo que respecta a los aspectos que caracterizan a la pericia informática, capaz de ser aplicado en toda la provincia, y al que se pueda acudir para consultas en caso de no poder contar con un especialista en la materia.

Debido a que en la provincia no sólo el Poder Judicial trabaja con evidencia digital, se tiene también presente a la Policía de Santa Cruz, en particular a la División de Apoyo Tecnológico, quienes asisten actualmente en la extracción de información de telefonía celular, debido a que poseen la principal herramienta en lo que respecta a esta materia (Herramienta UFED de la empresa Cellebrite). Es por eso que este protocolo cuenta con ambos actores y pretende que se trabaje conjuntamente para llegar a la verdad.

Se define como pericia informática a la identificación, conservación, análisis y presentación de pruebas electrónicas o digitales, por esta razón es que se hace la distinción respecto a sólo el análisis de información digital. Las pericias informáticas abarcan cada uno de estos procesos estén o no involucrados los mismos actores, y en caso de no contar con un profesional en la materia en cualquiera de los pasos de la pericia informática, se cuenta con protocolo para poder garantizar las buenas prácticas, a lo largo del proceso de pericia, desde que se decide dónde está la información de interés, incluyendo todo el recorrido, hasta llegar a la conclusión del informe pericial.

1. **Objetivos.**

El principal objetivo de este protocolo es comunicar acerca de los procesos realizados por los profesionales de informática forense, no sólo a modo informativo, sino para contribuir a profundizar en las buenas prácticas de todos los actores relacionados con los procesos judiciales, que llevan a la búsqueda de información por medio del análisis de dispositivos informáticos.

Objetivos particulares:

1. Evitar la contaminación de pruebas durante el proceso judicial.
2. Formalizar el procedimiento de actuación pericial en materia informática.
3. Definir el alcance de los servicios de informática forense.
4. Evitar la pérdida de información por mala actuación o desconocimiento.
5. Mantener la comunicación entre las partes conformantes del órgano judicial, para poder acudir al diálogo y asegurar un buen proceder de la información de interés.

Para conocer cuáles son las tareas pertinentes al Cuerpo de Pericias Informáticas y en Telecomunicaciones, se define al Perito informático como “el experto en el área de las tecnologías de la Información que de acuerdo con el tema requerido puede ser seleccionado según su competencia y experiencia para una labor de análisis, capaz de aportar al juez conocimientos, con el finde aclarar el asunto litigioso en revisión”.

Para conocer qué áreas están dentro de las incumbencias del Perito en Informática, se presentan a continuación los temas más relevantes sobre los cuales el especialista podrá dar respuesta.

*Alcances*

> Delitos informáticos:

* Pornografía infantil por Internet u otros medios electrónicos.
* Responsabilidad por contenido. (Contenidos nocivos e ilícitos, responsabilidad de los Proveedores de acceso, tutela de datos y prevención de delitos)
* Violación, apoderamiento y desvío de comunicación electrónica. (También publicación de una comunicación electrónica)
* Hacking. (Utilización abusiva de equipos y terminales de telecomunicación)

Intercepción o captación de comunicaciones electrónicas o telecomunicaciones.

* Intrusión. (Acceso informático sin autorización, en forma individual o grupal, formato de organización criminal)
* Acceso no autorizado a un banco de datos personales. (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)
* Revelación de información registrada en un banco de datos personales.

(Duplicación no autorizada de datos procesados y/o generados por los sistemas informáticos. Delitos contra la intimidad, descubrimiento y revelación de secretos)

* Cracking. Delito de daños. (Sabotaje informático)
* Fraude informático. (También robos o determinación de identidad a través de correos electrónicos y otra aplicación, inserción de datos falsos en un archivo de datos personales)
* Conductas de Cyberpunk. (Vandalismo electrónico, entrada sin consentimiento para destruir datos, implementar virus o bombas lógicas)
* Delitos relativos al mercado y a los consumidores. (Aspectos vinculados al comercio electrónico y operaciones realizadas a través de Internet)
* Estafa informática y hurto informático. (Abuso de Tarjeta de crédito, ficción de crédito, uso de tarjeta caducada, cancelada, falsa o alterada, también utilización de tarjeta ajena y apoderamiento de soportes informáticos)

ANEXO I

TOMO: Oi\ REGISTRO^ b FOLIO: J 2>oj

* Falsedad documental informática. (Simulación de tarjetas, también fabricación o tenencia de programas destinados a la falsedad documental)
* Delitos 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 navegación por Internet, uso de computadoras, entre otros elementos).

> Manejo de datos:

* Extracción de información de todo dispositivo que pueda almacenar datos (Dispositivos de telefonía celular, computadoras, notebook, Tablet, pendrive, discos extraíbles, CDs, DVDs, consolas de juegos con poder de navegación en internet, drones, etc.)
* Recupero de datos borrados y rastreo de información en los distintos medios informáticos entre los que se pueden encontrar archivos, carpetas, objetos, aplicaciones, página visitadas, etc. (también para los medios de almacenamiento nombrados anteriormente)
* Buscar indicios de manipulación de datos como archivos encriptados, comprimidos o escondidos.

> Reconocimiento de hardware y software:

Revelar dónde puede encontrarse información oculta (Aplicaciones(software), Cámaras digitales, impresora, dispositivos de almacenamiento, Emails, Juegos, Imágenes, Chats, Información latente provista por las páginas visitadas, Directorios, archivos y carpeta creadas por el usuario, etc.)

1. **Del Secuestro de tecnología informática.**

El Cuerpo Pericial de Informática y Telecomunicaciones recibe evidencia de toda la provincia. Siempre se aconseja que, en la medida que se pueda, un experto debe estar presente en lo allanamientos, o secuestro de evidencia tecnológica, asegure el resguardo de la evidencia y controle la cadena de custodia. Sin embargo, no siempre se puede contar con personal especializado en cada una de estas tareas, por esta razón es que se propone este protocolo, que considera cada una de estas etapas, permitiendo su consulta ante cualquier duda.

Según el Artículo 245° de Código Procesal Penal, tanto el juez como los peritos procurarán que las cosas a examinar sean en lo posible conservadas, de modo que la pericia pueda repetirse.

1. *Identificación de los elementos informáticos.*

La prueba electrónica no siempre es fácil de identificar, mayormente debido a la cantidad de dispositivos capaces de almacenar información, y la velocidad con que la tecnología evoluciona.

Lo primero que se debe hacer es separar el término electrónico de lo que es evidencia digital. No todo lo electrónico tiene la capacidad de almacenar información y dependiendo de la causa, no todos los dispositivos capaces de almacenar información son útiles.

Por ejemplo, un mouse es un dispositivo que contiene electrónica interna para funcionar, pero que no almacena información, por lo que no es evidencia informática. Ejemplos de dispositivos electrónicos que no poseen información son: mouse, monitores, teclados, lectoras de DVD, impresoras que no son capaces de conectarse a internet sin una PC, parlantes, dispositivos de toma de datos que no posean conexión a PC (ejemplo de estos son, dispositivos médicos, como medidor de glucosa, o accesorios de PC como un UPS o un estabilizador de tensión), etc.

Vale la pena mencionar la importancia de identificar correctamente cada elemento secuestrado en el acta.

Si bien una descripción respecto al tamaño, color y tipo de dispositivo puede ser útil, dado el formato de los dispositivos electrónicos, que suelen ser muy similares entre ellos, es importante remarcar la marca y modelo de cada dispositivo para poder diferenciarlos. ¿Es un pendrive o un mp3? ¿Es una utrabook o una Tablet con teclado? Muchas veces las diferencias externas son ínfimas, pero el proceso de extracción es completamente diferente. En estos casos se aconseja buscar, generalmente en la parte posterior del dispositivo las inscripciones que posean, lo que suelen ser números o una combinación de letras y números, esto es lo que le da la identidad al dispositivo y ayudar a diferenciar uno del otro.





Figural: A\_ Parte Posterior de Notebook. B\_ Detalle de etiqueta remarcada en A

C\_ Etiqueta de Notebook HP Pavillion dv7. D\_ Etiqueta de Notebook Asus K52D

Como conclusión al respecto puede decirse que no cabe la duda que mientras más dispositivos se secuestren existen más probabilidades de encontrar la información que se está buscando, sin embargo, esto podría alargar significativamente los plazos de la pericia y los costos de traslado.

1. *Buenas prácticas para el secuestro de evidencia digital.*

Como se mencionó con anterioridad, muchas veces no se puede contar con un especialista en la materia a la hora de realizar un secuestro que involucre evidencia digital, por esta razón se incluyó en este protocolo un listado de buenas prácticas para el manejo de dispositivos digitales durante el secuestro.

> Ante todo, debe recordarse que cada dispositivo debe manipularse de modo seguro y con medios adecuados como se detalla a continuación.

ANEXO I

TOMO: c>) v REGISTRO: ii'b FOLIO:A2>ol

* Dado que en su mayoría ios dispositivos son electrónicos, es necesario tener presente que una simple descarga estática de una persona con una prenda de nylon puede quemar parte del circuito, para evitar esta exposición y a otras descargas estáticas, se recomienda la utilización de guantes de nitrilo, tanto para el resguardo de los equipos como del personal.
* Recuerde que los gabinetes de las PC de escritorio suelen ser de metal y que uno desconoce el estado de las conexiones con las que cuenta la vivienda donde se realiza el secuestro, si no se tiene precaución el efectivo puede sufrir descargas eléctricas al manipular elementos conectados a la red en el momento del secuestro.
* Si los equipos se encuentran apagados, no deben encenderse, salvo circunstancias justificadas y previa consulta con el especialista.
* También debe desconectarse el cable de red Ethernet (Internet), si hubiera alguno, ya que puede mantener activas algunas funciones del equipo luego del apagado.
* Si el equipo se encuentra encendido deberá desconectarse directamente de la red eléctrica.
* Si no se apaga al ser removido el cable de alimentación, se deberá localizar la batería que lo mantiene encendido y ser removida.
* Si la batería no puede ser removida (como el caso de un celular), deberá recubrirse de papel aluminio o de cualquier otro elemento que asegure que el dispositivo no pueda conectarse a ninguna red (Bolsa, bolso o caja de Faraday, Lata de metal recubierta de nylon).



Figura2: A\_ Bolsa de Faraday B\_ Celular envuelto en Papel Aluminio C\_ Lata de Aluminio

* Las baterías deben ser removidas y guardadas en un lugar seguro y separado de la misma máquina, a fin de prevenir un encendido accidental.
* Si se secuestra un CPU, se recomienda que se anulen (tapen) los puertos de conexión para asegurar la integridad del contenido.
* Se recomienda tomar fotografías de los puestos de trabajo, teniendo presente que pueden encontrarse anotaciones aledañas que pueden contener claves o anotaciones respecto al contenido, que pueden ser útiles para la investigación.
* Recuerde siempre que, de tratarse de un caso especial, donde no se tenga conocimiento del material a secuestrar, debe consultarse a un especialista antes de tomar acciones.
1. *El ciclo de la cadena de custodia de la evidencia digital.*

Algo muy importante es verificar cuál fue el camino que recorrió la evidencia digital una vez secuestrada, hasta el momento de la Pericia Informática. Un error en el seguimiento de la cadena de custodia, alguien que abra o reciba el paquete que no le correspondía, puede poner en riesgo toda la investigación.

Si bien los dispositivos electrónicos son algo físico, tangible, la información, lo que poseen de valor para la investigación, es algo intangible y muchas veces puede borrarse sin que nadie lo note. Al encender un celular o una computadora sólo por verificar si enciende, se están poniendo en funcionamiento tareas internas del equipo que pueden sobrescribir información de interés, como puede ser la memoria volátil.

El hecho que nadie toque la evidencia, no significa que no pueda correr peligro de perderse o ser modificada. Las descargas electrostáticas, campos magnéticos o conexión accidental a redes inalámbricas pueden producir cambios en los equipos, sobre todo si los mismos están encendidos al momento del allanamiento. Para ello, es importante manipularlos y almacenarlos en soportes y lugares adecuados para garantizar su integridad.

De igual manera, el lugar de depósito de los dispositivos electrónicos a todo lo largo del proceso, debe tener las precauciones mínimas para evitar que se filtre agua o humedad a los equipos, polvo y otros agentes externos que puedan dañar al dispositivo.

1. *Recorrido de la evidencia*



|  |  |
| --- | --- |
| **Juzaado 1** | **Cuerpo Pericial 1** |
|  | **de Informática** |
| t |  |

Figura3: Recorrido de la evidencia del lugar de secuestro hacia el Juzgado, luego hacia el Cuerpo Pericial de Informática y finalmente de regreso al Juzgado.

Lugar de

Secuestro

Juzgado

D.A.T. Policía de la Provincia de Santa Cruz

Información

extraída

Cuerpo Pericial de Informática

Figura4: Recorrido alternativo de la evidencia del lugar de secuestro hacia el Juzgado, luego hacia la División de Apoyo Tecnológico. La extracción es enviada al Cuerpo Pericial de Informática y finalmente de regreso al Juzgado.

Generalmente el camino que la evidencia recorre es señalado en la Figura 3. Sin embargo, considerando que no todas las extracciones se realizan en el Cuerpo Pericial de Informática, debido a que la División de Apoyo Tecnológico posee la herramienta UFED, también existe evidencia que sigue el camino señalado en la Figura 4.



ANEXO I

TOMO: ¿'H REGISTRO: U~b FOLIO: iSo/i%e>

De una forma u otra, el tratamiento debe ser el mismo. Siempre se recomienda que el secuestro se haga de forma ordenada, intentando que los dispositivos similares queden juntos. Debido a que esto no siempre se puede asegurar, debido a que cada secuestro se realiza en condiciones diferentes, se recuerda que el único autorizado para separar los elementos secuestrados previo a su envío es el Juzgado, y mediante algún documento que registre cómo fue hecha la redivisión de elementos, para evitar la pérdida de cualquiera de los dispositivos secuestrados.

Por todo lo planteado anteriormente es que se propone adosar a cada paquete que contenga evidencia digital una ficha, que sirva de prueba indubitada que se aseguró integridad de la cadena de custodia.

En el Anexo 1 se adjunta un ejemplo de modelo de cadena de custodia basado en la cadena de custodia que propone el Laboratorio Regional de Investigación Forense del Poder Judicial de la Provincia de Santa Cruz.

1. *Traslado y recepción del material secuestrado.*

Dadas las distancias que separan las localidades de la Provincia de Santa Cruz, es muy común que la evidencia deba ser trasladada. Muchas veces los juzgados cuentan con jurisdicción que abarca a varias localidades, por lo que el traslado desde el lugar de secuestro hasta el Juzgado puede ser de muchos kilómetros, de allí la evidencia debe viajar hasta las oficinas del Cuerpo Pericial para ser analizada.

Cada paquete que se envía entre los determinados entes involucrados en el camino de la evidencia digital debe estar correctamente documentado e identificado, resaltando quién envía y quien recibe en la cadena de custodia.

Para esto existen varias herramientas que pueden tenerse en cuenta, desde rotuladores, etiquetas y bolsones reutilizables con precintos de seguridad.





Figura5: A\_ Precinto de metal B\_ Precinto plástico C\_ Cinta de seguridad con marca D\_ Cinta de seguridad.

1. **El Requerimiento Judicial**

Según el artículo 237° del Código Procesal Penal, “El juez podrá ordenar pericias siempre que para conocer o apreciar algún hecho o circunstancia pertinente a la causa, sean necesarios o convenientes conocimientos especiales en alguna ciencia, arte o técnica”. En particular, sólo se podrán requerir “Pericias Informáticas” cuando se deban intervenir o analizar alguna evidencia digital en el cual sea necesario poseer conocimientos especiales en informática forense.

Al efectuar una consulta, el especialista debe informar la situación suscitada, los posibles cursos de acción (con sus riesgos y probables beneficios) y, cuando lo estimare conveniente o le fuere requerido, formular las sugerencias o recomendaciones que se consideren pertinentes desde la propia incumbencia. Se debe proveer toda la información necesaria para realizar dicha tarea, de manera clara y precisa.

*Solicitud de fecha de pericia informática y en telecomunicaciones al Cuerpo Pericial de Informática y Telecomunicaciones del Poder Judicial*

Ante la creación del Cuerpo Pericial de Informática, considerando a que día a día se reciben pedido de turno de pericia informática de los distintos Juzgados, tanto de Instrucción como de Primera Instancia, de diferentes localidades de la provincia, es que se detecta la necesidad de proponer un formato en particular para la solicitud de turnos. Por ello es que se redacta a continuación las consideraciones que deben tenerse en cuenta, a la hora de realizar un pedido de turno, asegurándose que el instrumento legal que lleve el pedido contenga los siguientes elementos:

* Como primera medida el oficio con pedido de turno de la causa, debe contener los datos necesarios para identificar la causa (nombre y número de expediente) de la que se solicita turno, indicando el tipo tarea que el perito deberá realizar (pericia Informática, en Telecomunicaciones, informe técnico, asistencia técnica, entre otros).
* Debe indicarse qué elemento o elementos serán periciados, sean o no tangibles (puede solicitarse por ejemplo una pericia sobre una casilla de correo electrónico, o sobre un sistema de carga de datos de algún edificio, o sobre la información extraída de un celular por la División de Apoyo Tecnológico).
* Los dispositivos que requieran alimentación deberán ser enviados con sus respectivos cargadores, fuentes o cable de alimentación con los que fueron secuestrados. De no contarse deberá ser especificado en el oficio de solicitud de pedido de fecha de pericia (Por ejemplo, Notebook Sony Vaio C14 sin cargador).
* Por último, deberán indicarse los puntos de pericia solicitados.

Es importante recalcar que cuando se solicita la investigación de “todo punto de interés a la causa que el especialista decida consignar”, se da la oportunidad al perito de considerar otros datos que pueden resultar de interés, pero que no fueron nombrados como punto de pericial. Es por esto que se recomienda agregar siempre este punto.

También debe considerarse que, solicitar dicho punto, conlleva a que el perito deberá tener la mayor información que se pueda dar, ya que esto facilitará el trabajo de peritaje, permitiendo socavar datos que pueden ser de interés para la causa pero que si se desconoce del trasfondo de la causa no serán tomados en cuenta.

Por esto es que se recomiendo el envío del expediente previo a la fecha de pericia ya que hay información que pude ser de interés respecto a la extracción de información de los dispositivos secuestrados, que puede no ser tan fácilmente

ANEXO I

TOMO: CM V REGISTRO: FOLIO: ¿"óoJ

relacionado. Como ejemplo se considera el acta de secuestro, puede que este dato no parezca brindar mucha información, pero la habitación de donde fue secuestrado puede indicar si el elemento era de uso personal o compartido.

La respuesta al pedido de turno es una fecha y un horario en las instalaciones del Cuerpo Pericial de Informática y Telecomunicaciones del Poder Judicial, también se solicitará que la evidencia sea enviada con 48hs de anticipación a la fecha otorgada, para comprobar el correcto estado de los dispositivos.

El perito informático forense, debe ser consciente de sus limitaciones profesionales, y recurrir a equipos de peritos de otras disciplinas, en caso de necesidad, para abarcar todas las áreas de especialización. En importante remarcar que siempre pueden solicitarse la realización de pericias conjuntas con otros Cuerpos Periciales de la misma área o de otras disciplinas ya que muchas veces los delitos involucran diferentes disciplinas.

1. El análisis forense.

La etapa del análisis forense, si bien es un procedimiento interno del Cuerpo Pericial de Informática y Telecomunicaciones, es preciso comunicar su procedimiento debido a que el conocimiento del mismo puede aclarar dudas respecto a cómo solicitar los puntos de pericia por parte de las autoridades judiciales.

A la hora de realizar el análisis de la información recopilada hay que tener presente el tipo de incidente al que se dará respuesta. Aunque nunca se debe caer en el error de descartar lo que pueda parecer obvio, el perito debe ser totalmente objetivo en todo el proceso.

Puede realizarse, entre otros, análisis de:

* De datos (Fechas, horas, modificaciones, creaciones, instalaciones, eliminación, comparaciones).
* De tipos de datos (Imágenes .JPG, archivos .pdf, textos .docx, videos ,mp4, imágenes eliminadas en formato .GIF).
* De contenido (mensajes que contengan la palabra "bomba", Escenas del video X que contengan rostros, Imágenes que contengan niños).
* De aplicaciones (programas que sirvan para encriptar, para ocultar imágenes, descripción del programa, ¿Qué aplicación es la siguiente: ...?, ¿Qué conocimientos se necesitan para utilizarla?).
* De sesiones (Usuarios existentes, ¿Qué hizo el Usuario A en esa fecha?, ¿Cuál fue el último usuario registrado?, Redes Sociales, Almacenamiento en la nube).
* De conexiones (Redes favoritas, tiempo de conexión, páginas que visitó, identificación de dirección IP: o las direcciones IP asignadas a un equipo están registrados en los correos electrónicos enviados y en la navegación efectuada en Internet, proveedor de Internet que brinda el servicio, etc.)
1. **Informes Técnicos e Informes Periciales.**

El informe técnico se confecciona para el dar respuesta a los interrogantes existentes en la causa, relacionados con el contenido de la evidencia digital. Es el resultado de todos los procesos que conlleva la pericia informática, donde se da respuesta a todos los puntos solicitados por el Juez.

Es necesario dejar constancia de la condición de imparcialidad del perito. Posiblemente, el receptor del informe no sea un experto en la materia, por lo que el informe debe ser redactado utilizando métodos pedagógicos que faciliten su comprensión. No debe contener otra información que no sean los resultados objetivos obtenidos durante la investigación.

Particularmente el Cuerpo Pericial de Informática y Telecomunicaciones cuenta con un formato para la realización del Informe pericial con las siguientes partes:

* Solicitud y puntos de pericia: Donde se expone el nombre y expediente de la causa y los puntos a ser contestados a lo largo del desarrollo del informe.
* Elementos Ofrecidos: Donde se enumeran los diferentes elementos recibidos de donde se extraerá la información para dar respuesta a los puntos de pericia. Se suele acompañar de una fotografía de cada elemento para dar constancia del estado y si se encuentra completo o incompleto, como por ejemplo “una notebook HP Pavilion DV6 sin cargador”.
* Operaciones realizadas: Donde se enumeran las operaciones realizadas con la evidencia para extraer la información y realizar el análisis. La evidencia digital presenta características que la diferencian de las restantes clases de evidencia física. Se la puede duplicar de manera exacta (permitiendo manipular la réplica sin alterar el original), por medio de copiadoras bit a bit como la que se posee en el Cuerpo Pericial de Informática y Telecomunicaciones. Esta operación se detalle en cada informe que se utilice. A cada paso de esta sección se irá dando respuesta a cada uno de los puntos de pericia.
* Conclusiones: Se presentan los puntos de pericias solicitados y la respuesta resumida a cada uno de ellos.

Finalmente cabe destacar que los informes pueden estar acompañados de soportes magnéticos que pueden tener información complementaria al informe, como pueden ser imágenes que serán mejor apreciadas en formato digital que impresas en papel. También suelen incluirse los resultados del análisis de contenido de discos en formato de reporte escrito, líneas del tiempo, etc.

Una vez terminado el informe, se procederá a la entrega del mismo y devolución de todo material periciado, por medio de un oficio en el cual se detallan las condiciones en las cuales se remite cada elemento, dando fin a la pericia informática.

iiBW

RieS-aJeso,8$ íexfásnbr i? I&S

^neoXct0PX0toriVat»i»;wa»aj>y«VAarri8^r»á!k«y»»!igmcWcB-

k»joapeu90«tt.-

a tatto a ■» fetey«fai| ¿Ésa fi t/O «nitBBwaJri» a o snxtit

RjMte jí\* itftf jst bfc>'| y- Ivés» Wc&fets \*n b a?»eW|\*fa' 4a w ajeatei.

esa'«> M toteáwta “¡\*«p{¡«tilttm\*i Sarnas
£2¡oja CÍ\*trt'ún\*n¡:»l&SiÍ



t\* «pa ti taima»ta.stt a\* •arta fm ratita ysam. tm

atea amaemila a&rtay\* «x «¡SiS6.eance: ata tm 4t-r-

iiW m» ttaatxsmai «( «sa<e. n pdtnt stnw «a eí\*t. téptat«,aó¡ar¿a <

WMWtenSáffi.V «áéjfcpiciesb i C& <

íte» 5& »jwtoiea»\*'» iw\*



|  |  |  |
| --- | --- | --- |
|  | **1** | 1) ESrtótíCWl\* EOSTEJCU M T3WXMU& VC6CS TSf CIR0»A-»6U..¥MXttZ>OAU.mDft£cú&fcAga$M$ cuate» e.iesjicu»c |
|  |  | ce ndoucs ciBSWCT;«8Sía se. tato. «ostf? w feos ssaAUSYiLHW.mvaMau » u uoqihh ce tos wat» «mhhv «scoas'Caí-MneMUe/K-u» amo\*;-no-seaCMTIlMBMB(13ÍMeSMVIE8S1SieMMRBnULÍ«UK Knos |
|  |  |
|  |  | MUTStfg CÍS «SOCAS QBE »KtM Q£tíKS\*?0Brj<03 KCttDOS t^£n».^4>u^Ki<QH«uonn&tKniso.. • • ■ |
|  |  | .naSMiKma |

Figura 6: Modelo básico de Informe Pericial realizado por el Cuerpo Pericial de Informática y Telecomunicaciones

TOMO: c\J\

ANEXO I

REGISTRO: H'b FOLIO: i Ixoh^S

1. **Bibliografía**
* Dr. Del Pino, Santiago Acurio - “Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0” - Director Nacional de Tecnología de la Información.
* Di lorio, Ana Haydée - “Guía integral de empleo de la informática forense en el proceso penal” - Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. Universidad FASTA.
* Dr. Gómez, Leopoldo Sebastián - “Protocolo de Actuación para Pericias Informáticas” - Poder Judicial Provincia de Neuquén.
* González, Richard M., La cadena de custodia en el proceso penal español, Diario La Ley 8236/2013, Año XXXIV, Número 8187, Viernes, 8 de noviembre de 2013, págs. 3-4.
* Navarro Clérigues, Jorge - “Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico”
* Escola Técnica Superior d’Enginyerialnformática. UniversitatPolitécnica de Valencia.
* Mg.Lic. Piccirilli, Darío A. - "Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia - forensia y cibercrimen)" - Universidad Nacional de La Plata Facultad de Informática.
* Presman, Gustavo - “Estado de la Investigación Forense en la Argentina” - Asociación por los Derechos Civiles.
* Protocolo de Actuación del Departamento de Informática Forense Poder Judicial de Rio Negro - “Procedimientos Internos y Guías Operativas” - Departamento de Informática Forense Poder Judicial de Rio Negro.
* Protocolo unificado de los ministerios públicos de la República Argentina: guía para el levantamiento y conservación de la evidencia / Anónimo. - 1a ed.
* Ciudad Autónoma de Buenos Aires: Ediciones SAIJ, 2017.
* Puig Faura, Sonia «Apuntar a la simple posibilidad de manipulación para entender que la cadena de custodia se ha roto no parece aceptable, ya que debe exigirse la prueba de su manipulación efectiva» (STS 629/2011 de 23 de junio; 776/2001, de 20 de julio).

Cuerpo Pericial de Informática y Telecomunicaciones
**Poder Judicial de la Provincia de Santa Cruz
'w\*\*w «5 - - «fe <wtes#» - swe» cm**



|  |  |  |
| --- | --- | --- |
|  | i | ; pó«§g.e de Réíerenóla |
|  |
| OípawiTse jetew'fweBte;.,. , ,v„ |  | — ----- ™ |
| Oficio Pré«0ft»:, k , | ........ |   |

Carátula:....

Lugar de U vaciamiento,

. . . „ , , ,, . ,,,, • y . ; v .. .. ... y..y. , , , 1 y yy , y, y

;,Ld¿aíáá<fci

Levantada por,. Cargo:.,,.,,:,,,,.,.

**Ctee^feOECUSTOPIA**

|  |
| --- |
| **NesArey Aiptíi^:. Cargo: „ki.**  |
| **Orfawmo:...** | **FitWá v AeJaracite** |
| **Fecha: Itea:,:,.** |
| **Motivo** |
| **Custodia di****PfdMp O Qtre:..****Taswo n.** |
| **Reéeoctón** |
| **Nombre y Apellido:...**  | **OargcK.,. .• ,**  |

enanismos,,,.

'Hora-:.,

Observador»\*:.,,.,.

|  |  |
| --- | --- |
|  |  |
| ttsisegá.dftl Material |
| Notrtbre y-Apelíte:..  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **OrgartistnO':....** |  | **—'**  |  |
| **Fecha:** |  |  |  |
| **ÍSoBMí** |
| **í****j,l «.1**111**;Ó £L** ¥\*\*■ | **LJ****O****Q-** |  |  |

.claraoon

|  |
| --- |
| **Recepción**  |
| **NstrÉa^Apeliáb:,,,** |
| **ÓrganiSfM:**  | **<****|** |
| **Fecha: L,.,., J20....„**  |
| **Oteerw’acfeMs:;,,,** |

ANEXO I

TOMO: cv)v REGISTRO: J 4 $ FOLIO:

**Entrega del Materia!**

Nombre y Apellido:.

............ Cargo:.

|  |  |  |  |
| --- | --- | --- | --- |
| **Organismo:**  |  | **----- : i--;- —** |  |
| **Fecha. ¡L.** | **...720...** | **Hórá:.** |  |
| **Motivó** |  |
| **Custodia** | **O** |  |  |
| **Peritaje** | **□** | **Otra:.., ,**  |  |
| **Traslado** | **n** |  | **Firma v Aclaración** |

|  |  |
| --- | --- |
| **Recepción** |  |
| **Nombre y Apellido:......** |  | **Caigo:........-.: ;**  |

Organismo:.

Fecha: f 720.

Hora:

Observaciones:.

**Firma v Aclaración**

|  |
| --- |
| **Entrega del Material** |
| **Nombre y Apellido: Cargo:**  |
|  |
|  | **Firma v Aclaración** |
|  |
| **Fecha\*** f **Hora:.......:,;-:...** |
| **Motivo** |
| **Custodia L I****Peritaje CU Otro:. ,** **Traslado F I** |
| **Recepción** |
|  |
|  |
| **Organismo: :**  | **Firma v Aclaración** |
| **Fecha: / 720...... Hora?,...,::,—** |
| **Observaciones- „ .**  |
|  |

**Entrega delMaterial**

Nombre y Apellido: . Cargo:.

|  |  |  |  |
| --- | --- | --- | --- |
| **Organismo:,...** |  |  |  |
| **Fecha:**  | **...720.,** | **Hóra:.,** |  |
| **Motivo** |
| **Custodia****Peritaje****Trasladó** | **□****□****n** | **Otro:..** |  |

|  |  |
| --- | --- |
| **Recepción** |  |
| **Nombre y Apellido: ,,**  | **Cargo:.....,,...:**  |
|  |

Organismo:

Fecha: ,./2Q.

Hora:.

Observaciones:.

**Firma y Aclaración**

REFERNCIAS

**c odigo de referencia**

**Colocar ta localidad abreviada. dia, mes,año y numero de muestra con eodigo alfanumerico co**

**rrelativo (A,B,C;) E¡., 1 A, 2A ete.Si hay mas de ana causasenel mismo dia usar B, C. para la oirá EÍ.RG04042014-1 A. 2A, 3Á . . según corresponda a cada indicio**

**Organismo intervWente: Juzgado -**

**Descripción eteitténto dé pn^ba/lnrfido: :D breve de! mismo y pertenencia**

**Levantado por: Persona que realiza el ievarttamiéñto, cargo y lima y aclaración**

**Entrega de Material La misma persona que realiza el levantamiento con sus datos y firma**

**Motivo: marcar lo qué corresponda**

Recepción : Persona que recibe el elemente de prueba o indicia

**Organismo: lugar donde se desempeña Ej LR1F**

Recordar: Por cada indicio corresponde una planilla de cadena de custodia