Informática Forense al Servicio de una Justicia Moderna

Gastón Semprini y Alfredo Bozzetti,

Gastón Semprini es Licenciado en Sistemas de Información por la Univ. de Belgrano y Experto en Informática Forense por la Univ. Tecnológica Nacional. Es Jefe del Departamento de Informática Forense del Poder Judicial de Río Negro. gsemprini@jusrionegro.gov.ar

Alfredo Bozzetti es Ingeniero de Sistemas por la Univ. Nacional del Centro. Es Coordinador de Desarrollo Organizacional e Informático del Poder Judicial de Río Negro. Miembro del Comité de Informatización de la Gestión Judicial y representante del Poder Judicial en el Consejo Informático de la Provincia de Río Negro. abozzetti@jusrionegro.gov.ar

Abstract. En los últimos años el desarrollo de las Tecnologías de la Información y las Comunicaciones (TICs) han evolucionado y permiten que sean hoy cada vez más las personas que poseen acceso a las mismas. Si bien la utilización de las TICs trajo ventajas, también trajo aparejado la aparición de sucesos delictivos mediante el uso de las mismas. Una Justicia moderna comprometida con el Ciudadano tendrá, entre otras cualidades, los elementos para procesar causas o delitos de esta naturaleza. Un área de Informática Forense debidamente conformada puede ser la respuesta a ésta necesidad. Este trabajo aborda el camino recorrido por el Poder Judicial de Río Negro y pone a disposición de la comunidad la labor realizada para que otros también puedan ahorrar pasos y tiempos en la concreción de un área de investigación forense que aborde el ámbito descrito.

Abstract. In the past years the development of the Information Technology and Communications (ICT) have evolved and are now allowing more people who have access to them. Although the use of ICT brought many advantages, also brought criminal event occurrence using the same technology. A modern justice committed to the Citizen will, among other qualities, prosecuting cases or offenses of this nature. An area properly shaped Computer Forensics can be the answer to this need. This paper addresses the path taken by the judiciary of Rio Negro (Argentine) and makes available to the community for the work that others can save steps and time on the completion of a research area that addresses the field described.

Keywords: compromiso con el ciudadano, derechos del ciudadano, perito informático, protocolos de actuación, informática forense.

1 Introducción

El Poder Judicial de Río Negro trabaja en pos de fortalecer la relación con el ciudadano y mejorar así su nivel de acceso a justicia. En este camino y como fruto del trabajo del Foro Patagónico de Superiores Tribunales de Justicia adhirió, incorporando a la Ley Orgánica del Poder Judicial, la Carta de Derecho de los Ciudadanos de la Patagonia Argentina ante la Justicia [1]. Son pilares de este instrumento la transparencia, información y atención adecuada al ciudadano. Este último tiene el derecho a recibir información general y actualizada sobre el funcionamiento de los juzgados, tribunales y sobre las características y requisitos de los distintos procedimientos judiciales. A la par, ha trabajado en el desarrollo de la Carta Compromiso con el Ciudadano [2] asumiendo públicamente el compromiso de impulsar crecientes niveles de calidad y un servicio eficaz. Es decir construir un servicio de justicia moderno.

Estos derechos y compromisos se hicieron extensivos a Jueces, Procurador, Fiscales, Defensores, Asesores, Secretarios y todos los auxiliares del servicio de Justicia. Es de especial mención que en forma explícita se hace alusión a los Médicos Forenses. Cabe preguntarse entonces que pasa cuando el objeto de análisis se base en elementos tecnológicos. En los últimos años el desarrollo de las Tecnologías de la Información y las Comunicaciones (TICs) han evolucionado y permiten que sean hoy cada vez más las personas que poseen acceso a las mismas. Si bien la utilización de las TICs trajo ventajas, también trajo aparejado la aparición de sucesos delictivos por el mal uso de las mismas. Podemos enumerar los siguientes ejemplos: phishing, pedofilia, grooming, usurpación de identidad y amenazas por medio de correos electrónicos y redes sociales, entre otros. Estos ejemplos planteados son un claro análisis de la realidad en la que estamos viviendo y a lo que nos enfrentamos. En palabras de Susana Tomasi [3]:

> "… el crecimiento, desarrollo y expansión de los sistemas de la información ha comenzado a plantear nuevas temáticas y desafíos respecto a la seguridad informática, ya que empresas, organismos de gobiernos, e individuos adaptados a la era digital, se han encontrado con que personas inescrupulosas se aprovechan de dicha tecnología, para cometer delitos, fraudes o apropiarse de información almacenada y usufructuarla en su provecho, por lo cual se hacen necesarios nuevos tipos de investigaciones …".

A nivel legislativo muchas fueron tipificadas como Delitos Informáticos al amparo de la Ley 26.388.

De nada sirve declamar una Justicia moderna con una serie de instrumentos de apertura al ciudadano si cuando Este se presenta a denunciar la usurpación de su identidad en facebook o difamación a través del correo electrónico la respuesta es: " lo mejor que podes hacer es cerrar tu cuenta". Es por eso que de aquí surge la necesidad de capacitar a los operadores judiciales en este nuevo escenario y agiornar

las estructuras para abordar estas problemáticas. Como resultado de este proceso en el Poder Judicial de Río Negro se creó el Departamento de Informática Forense dependiente de los Cuerpos Técnicos Auxiliares brindado el mismo nivel de asesoramiento y prácticas periciales que los Médicos Forenses, Psicólogos Forenses, Peritos Calígrafos, etc. Es para mencionar que el trabajo iniciado basó sus primeras decisiones en la experiencia y el camino recorrido del área homónima del Poder Judicial de Neuquén, a cargo del Abogado y Licenciado en Ciencias de la Computación Sebastián Gómez[1]. Otras experiencias que se pueden consultar es las recorridas por el Ministerio Publico de Salta, Policía Judicial de Córdoba, Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires creado en Diciembre 2012.

2. Primeros Pasos

Durante un período de tiempo las UFAP (Unidades Fiscales de Atención Primaria) y los Juzgados recibían denuncias acerca de delitos que tenían como medio a la tecnología. En muchos casos se desestimaban por desconocimiento y en otras por no saber como obtener las pruebas necesarias para esclarecer el hecho. Con la incorporación de las tecnologías en los juzgados (Internet, mail, sistema de gestión de expedientes, etc.) y por cercanía o conocimiento de los técnicos informáticos se le solicitaba el asesoramiento y/o intervención en este tipo de causas. Esta práctica que no forma parte de las misiones y funciones de dicho técnico tuvieron un corto final dado que muchas veces no conocían de la temática de fondo, métodos y procedimientos adecuados y mucho menos contaban con las herramientas necesarias para una tarea profesional de investigación.
Un paso superador, pero no suficiente, fue crear dentro del Área de Informatización de la Gestión Judicial una División que se encargaría de éste tipo de tareas para que se comience a realizar los primeros asesoramientos a Jueces y Fiscales en la materia.
Finalmente, y luego de la renovación de los integrantes del Superior Tribunal de Justicia, y viendo, éstos nuevos Jueces, que la problemática descripta no estaba siendo abordada íntegramente decidieron la creación del Departamento de Informática Forense dentro de los Cuerpos Técnicos Auxiliares con el objetivo de brindar una solución profesional a la altura de las circunstancias, enmarcada en una de las Acordadas de dicho cuerpo[2]. El proceso finalizó con el concurso externo del Jefe del Departamento. Hoy ya en funciones. Solo a los efectos enunciativos se entiende hoy como Informática Forense en el Poder Judicial de Río Negro a:

> Un conjunto multidisciplinario de tareas, y métodos de análisis que brindan soporte a la investigación de la prueba indiciaria informática, entendiendo como prueba indiciaria a todo material de cualquier tipo y naturaleza que se encuentre en investigación, permitiendo con esas pruebas realizar una “reconstrucción de los hechos”. Si bien uno de los

1 Catálogo de Servicios para Pericias Informáticas (Poder Judicial Neuquén). http://www.jusneuquen.gov.ar/gab_tec_cont/datos/cat_serv_per_inf.pdf

2 Superior Tribunal de Justicia de Río Negro, Acordada Nro. 8, 2012. http://tsjrn.opac.com.ar/pgmedia/Acordadas/2012-008_AC.pdf

propósitos de Informática Forense consiste en determinar los responsables de los delitos informáticos, también lo es esclarecer la causa original de un ilícito o evento particular. De esa manera poder aportar en base a la reconstrucción de los hechos, información clave para que los Magistrados y Funcionarios tengan elementos para definir causas que estén bajo su investigación. [4], [5].

3. Construcción del Departamento

El desafío fue comenzar a trabajar en un ámbito muy dependiente de recursos tecnológicos desde cero. Es decir, sin contar con la infraestructura de base necesaria. Para ello se armaron una serie de procedimientos de actuación que dieron el marco normativo para el trabajo del área y cuya enunciación global se adjuntó como Anexo II de la acordada de creación del Departamento con el objetivo de evitar la contaminación y dispersión de la prueba durante el proceso judicial, formalizar el procedimiento de actuación pericial en materia informática y definir el alcance de los servicios de informática forense.

Las primeras causas que pudo atender el Departamento fueron específicamente injurias utilizando correos electrónicos, investigación de estafas bancarias, publicaciones en sitios web de elementos robados, identificación del origen de comentarios injuriosos en portales periodísticos online. El principal trabajo fue la identificación de los lugares y contactos en las distintas empresas proveedores de Internet, Servicios de Correos Electrónicos, Bancos, Redes Sociales, etc., para obtener la información correcta.

En el marco del Fuero Civil, se trabajó en la realización de pruebas anticipadas para la comprobación de licencias de software legales en diferentes empresas y organismos.

En cuanto a la infraestructura del Laboratorio de Informática Forense se armó un equipo avanzado PC, con ciertas características específicas, en donde poder utilizar el sistema operativo de base Linux. Para este trabajo se seleccionó la distribución Caine la cual posee herramientas para el análisis forense de dispositivos de almacenamiento. Esta distribución posee la particularidad de interactuar en forma gráfica y poder entre otras cosas, preparar el disco donde se almacenará la imagen forense, realizar la misma y analizarla. A nivel herramientas de esta distribución podemos mencionar Foremost y Scalpel para extraer documentos, imágenes, videos, etc. y el Autopsy para el análisis y la búsqueda de patrones.

Se adquirió una notebook para darle movilidad al área y una impresora color para la presentación adecuada de los informes periciales. Esto cobra mayor sentido a la hora de identificar archivos y fotografías en las computadoras secuestradas.

4. Herramientas Específicas

La multiplicidad de pedidos de pericias que comenzaron a llegar desde los Juzgados, y el tiempo de respuesta necesaria para mantener los parámetros de un servicio de justicia ágil y en pos de profesionalizar las herramientas del área generó la necesidad de adquirir elementos de trabajo más específicos y las adecuadas capacitaciones. Para esto se incluyó en el presupuesto anual del Poder Judicial una partida especial para la adquisición mencionada. Una vez aprobado el monto por la Legislatura Provincial (Ley 4814, Presupuesto 2012) se analizó suplir las necesidades más esenciales basadas en las estadísticas de los tipos de pericias solicitadas.

a. Bloqueador de Escritura: una herramienta de hardware que permite la conexión de diferentes dispositivos de almacenamiento (IDE/SATA) bloqueando el mismo ante escrituras. Esto permite de forma segura, evitando la escritura sobre los medios conectados, un análisis rápido de los archivos existentes. En particular se eligió el Tableau T35es-R2.
b. Evidencia de Comunicaciones en Internet: es un producto de software que obtiene los rastros de navegación, chats de diferentes proveedores de servicios (skype, facebook, etc), actividad de envío y recepción de emails, etc. Permite visualizar, recuperar y analizar comunicaciones basadas en el protocolo de Internet. En este caso se optó por el Internet Evidence Finder.
c. Búsquedas por Patrones: en muchas ocasiones es necesario buscar información en una imagen forense de un dispositivo de almacenamiento completo en los cuales EnCase Forensic y/o AccessData FTK pueden ser aliados en nuestras investigaciones. Aquí es necesario adquirir el equipamiento asociado dado que ya no se podrá usar una simple PC de escritorio sino que se necesitara una plataforma avanzada y potente que el mismo fabricante de software ayuda a configurar, convirtiéndose en una verdadera estación de trabajo forense.

Luego de “estas listas de deseos y compras” el Lab. contará con el equipamiento necesario no solo para abarcar un amplio espectro de pericias informáticas sino que además hasta nos permitirá tener herramientas específicas y en el caso de necesitarlo poder iniciar más de una investigación a la vez. Con los protocolos, procedimientos y con el apoyo de las herramientas correctas podremos transitar el ciclo de vida de la evidencia, mostrada en la Fig. 1, en consonancia con una de las propuestas más utilizadas presentada por el Departamento de Justicia de los Estados Unidos [6].

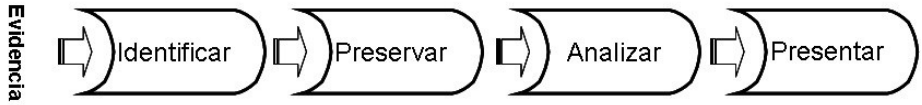

Fig. 1. Ciclo de vida de la Evidencia.

Se anexa al final del trabajo la planilla para uso en el paso de Identificación de la evidencia, la cual se fijará al elemento secuestrado. La misma puede ser usada o modificada libremente por quien desea incorporarla en sus procesos.

5. Estadísticas

Si bien el Departamento está pensado para atender requerimientos de todos los fueros, rápidamente el Fuero Penal se convirtió en el principal usuario de estas investigaciones digitales. Veamos a continuación que en este corto período de vida ya se ha intervenido en más de 80 causas, las cuales se distribuyen como se muestra en el siguiente gráfico[3] en donde se ha realizado uno o más tipos de análisis dependiendo del pedido del juzgado o fiscalía.

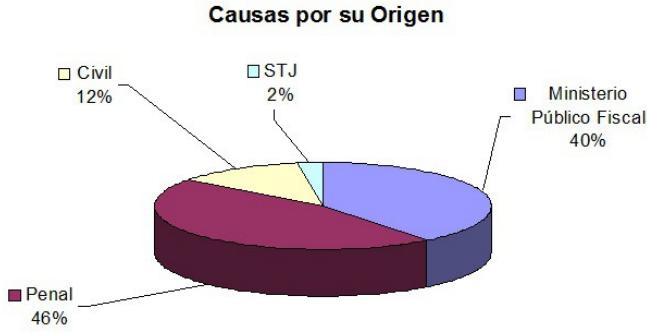

Fig. 2. Porcentajes de Causas según el origen de solicitud de la pericia.

Como puede observarse en la Fig. 2, Informática Forense, también ha intervenido en causas internas de expedientes disciplinarios del Superior Tribunal de Justicia.

Si bien este tipo de porcentajes es del estilo de las estadísticas de un Juzgado, un área específica como esta deberá llevar indicadores más precisos de su accionar. Cantidad de PCs investigadas, gigabytes analizados, análisis de información relacionadas a números IP, mails, cámaras de seguridad, etc. Es decir uno debe contar con información al estilo de un tablero de comando para conocer la salud operativa del Departamento y será unos de los objetivos para el próximo año. Adicionalmente es para destacar que el área se maneja con el mismo software de Gestión que los Juzgados permitiéndonos el pase digital de los expedientes.

3 Los datos que referencia este gráfico fueron extraídos del sistema de Gestión de Expediente del Departamento de Informática Forense, el cual reflejan el 100% de la actividad del área.

6. Casos

Caso A. Estafa Millonaria en la venta de terrenos de una Mutual

El caso se basa en una Mutual encargada de la venta de un plan de viviendas en un barrio determinado. Los mismos eran vendidos a diferentes familias con escasos recursos económicos. La mutual, vendió más viviendas de las que pretendía construir, llegando a vender hasta dos veces una misma unidad. En este caso se solicitó al Departamento de Informática Forense que de las computadoras secuestradas se extraiga todo material relacionado a la causa; como por ejemplo: facturas, remitos realizados a los involucrados, planos de mensura, nomenclatura catastral de cada una de las viviendas, etc.

Procedimientos y Herramientas utilizadas: Caine y Bloqueador de escritura Tableau.

1) En ese momento se coordinó con las partes involucradas la apertura de los CPUs para identificar y fotografiar, dejando constancia de las condiciones de cada uno de los CPU y las condiciones en las que se encontraban luego del secuestro de los mismos.

2) Se realizaron las Imágenes Forenses, y las funciones HASH[4] correspondientes de los discos rígidos, usando la herramienta bloqueadora y su software Tableau Imager, (resguardándose dichas imágenes en un disco con la capacidad suficiente). Los resultados de dichos HASH fueron entregados al juzgado y las partes.
3) En el Lab. se procedió a realizar la extracción de los datos con la herramienta FOREMOST Y SCALPEL, de todos los documentos y imágenes de las Imágenes Forenses.
4) Se realizó un análisis específico, con el Autopsy, para realizar búsquedas de palabras y caracteres especifica relacionadas a causa. Las cuales se concensuaron previamente con el Juzgado interviniente.
5) Por otro lado se realizó búsquedas con el comando grep, de palabras claves, dentro de los documentos extraídos con el FOREMOST.

Conclusión:

Del análisis anteriormente descrito se pudo obtener los modelos de remitos que se le entregaba a cada familia cada mes que iban a pagar la cuota a la mutual. Por otro lado se pudo encontrar planos de mensura de dichos terrenos mediante la nomenclatura catastral y un dato relevante para la causa, que fueron dos listas, una era el total de las personas que pagaron y se le adjudicaron las viviendas, y la otra lista las personas que

4 Función HASH: es la aplicación de un algoritmo a un conjunto de entrada (archivo, directorio, disco rígido, etc.) con el objetivo de determinar un valor determinado que referencia unívocamente a dicho conjunto de entrada. Un cambio, por mínimo que sea, a dicho conjunto provocará un valor de salida totalmente distinto.

pagaron por los terrenos, pero que finalmente no recibieron la vivienda pero si efectuaron los pagos correspondientes. Estos elementos, entre otros, permitieron que los presuntos estafadores se encuentren presos.

Caso B: Injurias por medio de Correos Electrónicos.

Una persona denunció en la UFAP (Unidad Fiscal de Atención Primaria) sobre la recepción de injurias realizadas desde un correo electrónico que tuvieron como destinatario su cuenta personal de Yahoo, la de su trabajo, y a las cuentas de otras personas familiares y de su entorno laboral.

Procedimientos y Herramientas utilizadas: MD5sum, CMD, impresión de pantalla de Windows.

1) Se coordinó con los destinatarios que recibieron los correos electrónicos, fecha y hora, para poder realizar la extracción de las propiedades y detalle de los mismos.
2) Se realizó la impresión y guardado de dichos mail, aplicándole a los mismos un algoritmo de HASH MD5sum para resguardar la prueba. (se dejó asentado con el CMD, nombre de la maquina, fecha y hora del procedimiento)
3) Para validar la veracidad de la información extraída se pidió a los proveedores de las cuentas de correo electrónicas involucradas, datos completos, IP o Log. de conexión en la fecha y hora del envío de los correos.
4) Una vez obtenidos los IP de conexión se constató si dichos IP eran iguales a los extraídos en las computadoras de las personas que recibieron dicho mail.
5) Con esta información se determinó a que proveedor de Internet correspondía dicho IP, solicitando que el mismo notifique datos completos del usuario al cual se le asigno dicho IP en fecha y hora.

Conclusión:

Como resultado de esta investigación se pudo comprobar el lugar físico desde donde se realizaron los envíos de dichos correos electrónicos. Por otros medios el Juzgado determinó quien podía llegar a ser, y uniendo ambos elementos se concluyó el lugar y la persona que realizó dicha injuria. Hoy se ha cerrado la causa mediante un acuerdo económico entre las partes.

Caso C: Robo Agravado por el Uso de Arma

Este caso en particular fue una denuncia realizada por el dueño de un Maxiquiosco el cual registró con sus cámaras de seguridad el hecho en el cual un individuo con un arma de fuego realizo el robo del total de la recaudación del día. En la causa intervino el Departamento de Informática Forense para realizar la verificación de existencia de videos de seguridad y en caso a afirmativo la extracción de los mismos.

Procedimientos y Herramientas utilizadas: Hash MD5sum, almacenamiento USB, Dvd.

1) Se coordinó con el dueño fecha y hora para la extracción de los videos de seguridad.
2) Una vez en el lugar del hecho se procedió a realizar la búsqueda del video en cuestión según su fecha y hora.
3) Se realizo la extracción mediante el programa propietario del DVR de los videos en formato AVI a un dispositivo de almacenamiento USB.
4) Se computó la función HASH MD5 a todos los videos extraídos.
6) Mediante el uso de un Software Libre (Video To JPG Converter), se extrajo imágenes fotográficas cada 1 segundo de los videos extraídos, acorde a lo solicitado por el Juzgado, durante el intervalo de tiempo en el que se visualiza el hecho.
7) Se realizó el grabado de los mismos a 3 copias de DVD una para el Maxiquiosco, otra para el Juzgado y otra para el Departamento de Informática Forense. Dentro de los mismos se encontraban, los resultados del HASH, acta de procedimientos, las imágenes fotográficas de los videos y los videos.

Conclusión:

El informe pericial concluyó la existencia de los videos, la clara visualización del momento del hecho y del rostro del autor. El juzgado determinó una condena de 6 años para dicho autor.

7. Conclusión Final y Pasos a Seguir

Desde su creación y una fuerte decisión institucional de un nuevo Superior Tribunal de Justicia que entiende la importancia de los delitos informáticos y su investigación, el Poder Judicial de Río Negro cuenta con un Departamento de Informática Forense. En la construcción del mismo se usaron otras experiencias vitales a la hora de su formación. Hoy con un primer camino recorrido es la intención de este trabajo contagiar a otros Poderes Judiciales y/o Policías de Investigación Judicial a que tengan esta iniciativa. Con mayor o menor presupuesto, con herramientas de software libre o las más caras del mercado se puede llevar adelante ésta tarea identificando a las PERSONAS que especializadas en el tema pueden instrumentar estas investigaciones. Nuestra construcción dejó una serie de trabajos escritos (protocolos, procedimientos, acordadas, llamados a concursos, pliegos de compras, etc.) que ponemos a disposición de quienes quieran usarlos para acompañarnos y crecer en este accionar de una Justicia que no solo declame su modernidad sino que la plasme en hechos como estos.

Nuestros próximos pasos son continuar profesionalizando el Lab., incorporando tecnología y en un futuro talvez personal. Desarrollar más procedimientos que aseguren procesos chequeados y estadísticas específicas como las ya planteadas anteriormente.

En el transcurso del año ya fueron programadas por la Escuela de Capacitación Judicial talleres en las ciudades cabeceras de Circunscripciones Judiciales de nuestra

provincia (Viedma, General Roca, Cipolletti, Bariloche) para capacitar y asesorar a Magistrados y Funcionarios sobre los posibles servicios a encontrar en ésta área de Informática Forense y en otras como la Oficina de Investigación de Telecomunicaciones (OITel).

Referencias

1. Ley Orgánica del Poder Judicial de Río Negro (K 2430) – Anexo A Carta de Derecho de los Ciudadanos de la Patagonia Argentina ante la Justicia. On-line: http://www.jusrionegro.gov.ar/inicio/oaci/carta_derechos.php

2. Segunda Carta Compromiso con el Ciudadano. (Poder Judicial de Río Negro, Octubre 2010). On-line: http://www.jusrionegro.gov.ar/inicio/oaci/cartacompromiso.php
3. Tomasi, Susana Noemí. Pericias Informáticas de Sistemas y Computación. Compilado en Tratado Jurisprudencial y Doctrinario. Derecho Informático. Tomo II. La Ley. 2011

4. Darahuge, María Elena y Arellano González, Luís. Manual de Informática Forense. Errepar. Buenos Aires. (2011)

5. Cano, Jeimy. Computación Forense. Descubriendo los Rastros Informáticos. Alfaomega. Méjico. (2009)

6. U.S. Deparment of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Nacional Institute of Justice.
On-line: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

ANEXO I – IDENTIFICACION DE LA EVIDENCIA

PODER JUDICIAL DE RIO NEGRO

DEPARTAMENTO DE INFORMATICA FORENSE

	FORMULARIO DE REGISTRO DE EVIDENCIA DE LA COMPUTADORA	

Nro. EXPEDIENTE	CARATULA	JUZGADO

Especificación de la Computadora	
Marca	
Modelo	
Nro de serie	
Placa madre	
Procesador	
Memoria Ram	
Fuente	
Otros	

Almacenamiento Secundario, Fijo y/o Removible				
Cantidad	Tipo: Disketera-CD-Disco Rígido-Pen Drive	Marca /Modelo	Velocidad /Capacidad	Nro. de Serie

Accesorios y Periféricos				
Cantidad	Tipo: Placa de red, modem, etc	Marca / Modelo	Velocidad / Capacidad	Nro. de Serie

Observaciones:		
Perito Informático Forense	Lugar	Fecha
Nombre:		

Apellido: DNI	Firma y Aclaración: