ANEXO

METOLOGIA DE INVESTIGACIÓN CRIMINALISTICA

PARA CASOS DE PERPETRACIÓN DE

DELITOS INFORMATICOS

TESIS

TITULACIÓN EN CARRERA DE

INGENIERIA EN INVESTIGACIÓN POLICIAL

12 – 06 – 2001

PRESENTADO POR:

CAPITAN SR. JOSE ALFONSO TOLEDO DUMENES

ANEXO

TESIS TITULACIÓN EN

CARRERA DE INGENIERIA EN INVESTIGACION POLICIAL

CRIMINALISTICA FORENSE INFORMATICA

CAPITULO I

INTRODUCCIÓN

Las nuevas estructuras en las comunicaciones, informaciones y negocios, han cambiado radicalmente nuestra perspectiva sobre la integración y globalización, estamos cada vez más cerca de los centros neurálgicos mundiales, del arte, de los negocios y de la entretención. Esta nueva forma de visualización de nuestro entorno social, cada día más se compenetra en las actividades políticas, culturas y comerciales de Chile, todo esto gracias al desarrollado y avances tecnológicos, llegando a todas las áreas del quehacer nacional y en los lugares más remotos, logrando acercarnos a altos niveles de desarrollo social. Que este impulso tecnológico y su entrada en los distintos ámbitos del desarrollo nacional, ha traido consigo la aparición de delitos emergentes, que utilizan estas nuevas herramientas para crearse nuevos e inmorales beneficios personales. A este nuevo elemento de transgresión de las normas sociales, ha despertado la sensación de inseguridad, especialmente en áreas del comercio electrónico y de gobierno, ante los cuales se ciernen graves pérdidas financieras y de imagen por la precariedad del control.

Esto abre nuevas áreas para desarrollar un adecuado control, seguridad e investigación del nuevo paradigma social, negocio que nos impulsa a ingresar aun mercado carente de formas de investigar y perseguir el crimen informático o “cibercrimen”.

1.- OBJETIVO GENERAL:

Realizar e implementar de una metodología técnica, en el ámbito de la informática, para el desarrollo de un **SERVICIO CRIMINALISTICO INFORMATICO FORENSE**, la investigación y resolución de hechos que revistan caracteres de delitos informáticos, acorde a la legislación y que alteren el orden social, causando graves perjuicios económicos al empresariado nacional; como también considerar hechos que sin encontrarse adscritos a una legislación nacional, causan problemáticas graves en las relaciones sociales, económicas y morales, técnicas que alcanzan los estandares de confiabilidad requeridos por los Tribunales de Justicia.

1.1.- OBJETIVOS ESPECÍFICOS:

1.- Creación de una metología de investigación de delitos informaticos, acorde a las técnicas aplicables a la Investigación Criminal

2.- El Personal del área Informática tiene las herramientas técnicas, de procedimiento y de vocabulario acorde para el trabajo criminalístico.

3.- El Personal del área Informática actua acorde a una pauta de investigación criminalístico para la implementación del Servicio de Informática Forense.

4.- Alta capacitación y destreza de Profesionales para el rubro de Informática Forense, para su nombramiento y aceptación como especialista ante los Tribunales de Justicia.

CAPITULO II

ANTECEDENTES TEMA DELITOS INFORMATICOS E INTERNET

1.- ANTECEDENTES LEGALES:

- Constitución Política de la República de Chile.
- Código de Procedimiento Penal y Código de Procesal Penal
- Ley Nro. 19.223 Tipifica Delitos Informáticos
- Técnicas de Investigación Policial.

2.- ANTECEDENTES PREVIOS

Carabineros de Chile, por medio de una Unidad especializada debe aportar a la prevención y control formal de los hechos inusuales y que revistan caracteres de delito en Chile, en el amplio espectro donde el cibercrimen ha podido utilizar maliciosamente la red para el su cometido. Es por ello capacitar a personal profesional y técnico en la metodología criminalística informática, acorde a los requerimientos actuales del nivel tecnológico que ha alcanzado nuestra sociedad y Chile, especialmente.

Para la investigación de estos hechos que son indicados en el artículo 1º y siguientes de la Ley Nro. 19.223 **"El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento", "El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él"** y **"El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información"**; no estamos preparados tanto a nivel público ni privado para el establecimiento de los delitos enunciados y que se ajusten a los requerimientos de fidelidad, prolijidad y comprobables que exige nuestro Código de Procedimiento Penal, existiendo un campo no explorado por las policías ni las empresas del rubro.

Es por ello, que ante esta nueva experiencia de crear una nueva metodología para una criminalística que llamaremos **"CRIMINALÍSTICA INFORMÁTICA"**, donde trataremos a la evidencia, que en este caso particular, se caracteriza por ser tanto física como logica, en que puede consistir en elementos del hardware o los datos exclusivamente. exploraremos, experimentaremos y probaremos los medios, caminos y capacidades para establecer los mecanismos que satisfagan los objetivos de toda investigación criminalística.

Para ello, deberemos considerar los siguientes conceptos generales para el trabajo criminalístico, conceptos que ampliaremos convenientemente y daremos sus características particulares, para esta área de investigación.

Determinaremos este proceso de trabajo informatico como "**Forense computacional"**, al trabajo de recoger y preservar las evidencias en el computador, como tambien al uso de esta evidencia en un procedimiento legal.

CAPITULO III

ANTECEDENTES METODOLOGICO / TECNICO SOBRE CRIMINA-LISTICA INFORMATICA

1.- SUCESO INFORMATICO:

Denominaremos **SUCESO INFORMATICO DE HACKEO**, a todo lugar fisico como virtual, donde ha ocurrido u ocurre un hecho de tratamiento no autorizado de datos informáticos, que precisa de un control, para establecer fehacientemente de que se trata, es decir, constatar : Que, cuando, donde, por que y quienes; o también causas, forma, motivos o manera, ubicación en el tiempo y en el espacio, identidades en general.

2.- TECNICAS GENERALES APLICABLES AL S.I.H.

Las técnicas hipotéticamente estarán subdivididas en:

- Protección.
- Inspección ocular
- Aislación
- Fijación
- Levantamiento

- **La protección:** Tiene por objetivo primordial conservar el S.I.H. en las mismas condiciones físicas de hardware, de software y del entorno físico en que fue encontrado.
- **Inspección Ocular**: Acto de comprobación personal en el mismo lugar de ocurrencia de los hechos, practicado para describir, recoger vestigios o elementos materiales de la perpetración del hecho y los objetos relacionados con la existencia y naturaleza del hecho. Esta labor debe ser realizada por el funcionario que tenga a cargo la investigación (excluyentemente) y cuente con la respectiva autorización para tal efecto, procurando mantener el lugar sin alteraciones de ningun tipo.
- **Aislamiento**: Consiste en delimitar el Sitio Informático de Hackeo, con el fin de impedir cualquier tipo de circulación de datos y personas, para evitar la más mínima alteración. Este cometido se debe realizar utilizando todos los medios de hardware o software adecuados con que se encuentre al alcance al momento de constituirse o tomar noticia del hecho, evitando usar elementos que formen parte del sitio del suceso.
- **Clausura**: consiste en cerrar los accesos tanto fisicos como en la red, que tenga un S.I.H., que se encuentre en un lugar, para evitar ingreso de personas tanto internas como externas a la red, que puedan modificarlo.

2.1.- INSPECCION de revisión de la red o sitio informatico hackeado

Acto de comprobación personal practicado para recoger vestigios o elementos materiales de la perpetración del hecho punible y describir el lugar y los objetos relacionados con la existencia y naturaleza del hecho. Esta labor debe ser realizada por el profesional que tenga a cargo el servicio de la empresa y cuente con la respectiva autorización para tal efecto, procurando mantener el lugar sin alteraciones.

Antes de proceder en la Fijación, Levantamiento, Custodia y Envío de Evidencias, es preciso que el Personal Profesional experto, consideren las siguientes recomendaciones, para su trabajo en el Sitio del Suceso:

- Establezca los tipos de evidencias que serán más probable que se encuentren.
- Concéntrese en las evidencias más transitorias o perecederas.
- Asegúrese que todo el personal considere la gran variedad de evidencias posibles que existe.
- Asegúrese de que tenga a mano suficiente material para empacar.
- Concéntrese en las áreas de fácil acceso que se encuentre a simple vista y luego en lugares menos accesible.
- Considere si la evidencia parece haber sido movida inadvertidamente.
- Determine si las evidencias han sido intencionalmente preparadas.
- Tome apuntes de todo lo que esta observando en el lugar.

2.2.- Fines de la inspección de revisión.

a) Comprobar la existencia real del hecho que revista las características de hackeo

b) Averiguación del móvil del hackeo.

c) Identificación del autor o autores.

d) Determinar y demostrar la participación y por lo tanto la culpabilidad del autor y las circunstancias concurrentes en el hecho de hackeo.

a) Comprobar la realidad del hackeo.

Ya que en determinadas situaciones, los hechos comunicados podrían corresponder a fallos del sistema de red, de hardware o software, ante lo cual el profesional deberá detectar con sus conocimientos si es un hecho de estos o verdaderamente estamos frente a un Sitio Informático de Hackeo; ante lo cual deberá con el máximo de cautela, a fin de evitar que con su acción modifique cualquier antecedente que posteriormente pueda destruir, alterar o borrar algún medio de prueba.

b) Averiguación del móvil del delito

Denominaremos móvil del delito de hackeo, al interés que tiene un individuo que lo lleva a perpetrar un acto delictivo.

El llegar a descubrir que motivo al autor a cometer el delito nos facilita su descubrimiento y a demostrar su culpabilidad.

c) Identificación del autor o autores

La investigación de los delitos informáticos, tiene como primera finalidad el descubrimiento del o de los autores del hecho, labor que se ve facilitada con una buena Inspección Ocular.

En lo que se refiere a delitos informáticos, Olivier HANCE en su libro "Leyes y Negocios en Internet", considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos, que son las siguientes:

- Acceso no autorizado: Es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.

- Actos dañinos o circulación de material dañino: Una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre se es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

- Interceptación no autorizada: En este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él."[i]

2.3.- Fijación:

Antes de levantar cualquier evidencia, tales como instrumentos que sirvieron para su perpetración, rastros, huellas y señales que haya dejado el hecho, etc. Éstas deben ser fijadas previamente, siguiendo la siguientes metodología:

Metodología a utilizar:

Pasos Previos a la llegada del Personal

- Recibido el aviso de parte de la empresa afectada, se le comunicará inmediatamente al Personal Policial Técnico para que se traslade hasta las instalaciones del recurrente.
- El administrador de la red o persona responsable de la empresa afectada, deberá seguir los siguientes pasos, para cooperar y mantener la información:

Ø Conocer y mantener a mano los números telefónicos importantes para comunicar al servicio especializado de Carabineros de Chile, sobre el problema que esta enfrentando.

Ø Mantener la Calma personal y de sus ejecutivos.

Ø Desconectará la red, servidor o estaciones afectadas, preferentemente en forma física.

Ø No permitirá que se ejecute ningun programa en el servidor, terminal o sistema de seguridad.

Ø No permtirá que el equipo sea apagado o desconectado del servicio eléctrico.

Ø Deberá tomar las precauciones para que todo el equipamiento se mantenga en las mismas condiciones, es decir, se mantendrán encendidas o apagadas, no debiendo intervenirlas de ninguna forma.

Ø Tomará nota de TODAS las personas que de alguna forma han tomado contacto con el hardware y no permitira que nadie lo utilice.

Ø No permitira que se retire desde el edificio, habitación o sector, elementos de Registro o Respaldo de Información (Cd., Disquet, cintas magnéticas, etc.)

Ø Se mantedrá en el lugar a la espera del personal técnico para que sirva de orientación en el primer momento, como también ser el nexo con el área gerencial de la empresa afectada.

Ø Se orientará por el medio de comunicación adecuado lo que debe o no debe hacer.

Una vez en el lugar físico:

- En caso de no contar con la persona responsable o capacitada, el Personal Profesional (preferentemente) o Técnico debera dejar fuera de Servicio el computador, sector, servidor o red; para la realización de los pasos necesarios para fijar la información y evitar su adulteración o modificación, tanto en forma premeditada como de rutina, esto por el tiempo que se sea necesario y conveniente.
- Con la guía del administrador de red o persona responsable, el Personal técnico realizará los siguientes pasos:

- **Inspección Personal:**

Ø Revisará el hardware de toda la red, modelos y marcas, instalaciones, conecciones, suministro eléctrico, ambiente; en a fin de comprobar personalmente que el hecho no esta basado en una falla física o de la instalación.

Ø Tomará conocimiento de los software, Sistemas Operativos y Diagrama y forma de operación de la red.

Ø Ubicará donde se encuentran los elementos de seguridad de la red, tales como hardware del Firewall, Router y Sistema de Detección de Intruso (I.D.S.), modelos, características técnicas y su configuración.

Ø Se asesorará para tomar conocimiento de las claves de usuarios y de administrador necesarias para el acceso a todos los puntos de la red.

Ø Se informará sobre las Políticas de Seguridad, Políticas de Password y de Usuarios en la red interna de la empresa.

- El Personal de Carabineros, portará consigo dentro de los elementos de laboratorio, un Notebook, equipado con Tarjeta de Red, modem y grabador externo o interno de cds, que será un **"labotario fuera del laboratorio"**, lo que se utilizará para el analisis o el almacenamiento de datos o para acceder en un caso al sistema de administración de la red, equipamiento que utilizará de la siguiente manera:

- **Fijación y respaldo de archivos**

Ø Procederá a conectar, con la debida autorización, en red al equipo Notebook, accediendo a las características de configuración, archivos LOG, bases de datos y otros convenientes para la investigación y establecimiento del delito de hackeo, desde los puntos preestablecidos de la red, ante lo cual grabará en la forma que hubiese sido encontrado, directa e integramente el archivo al grabador de Cd, usando un disco sin uso y que se caracterice por ser editado por una sola vez. Finalizada la grabación, se retirará el cd desde el reproductor/grabador y a vista de los presentes, se guardará en un contenedor de cds, sin usar.

Ø Esta operación de Grabación de cd y en las sucesivas se realizará en tres versiones, la primera utilizada como respaldo para su remisión a los Tribunales, la segunda para el trabajo del Personal de Carabineros de Chile y la tercera como respaldo para la empresa afectada.

Ø El primer cd llevará un protocolo de autentificación, consistente en un contenedor que se sellará adecuadamente con cintas de papel, consignando de puño y letra del responsable de la pericia: Nombre y Céd. De Id. del responsable que manipulo el disco, Fecha, Hora, Nro. de serie, Empresa y Persona responsable de la empresa que observa el procedimiento y sello o timbre de autentificación de la empresa. Las restantes copias no llevarán esta autentificación, pero si la individualización conveniente

Ø Uno de los funcionarios especializados de Carabineros, tomará nota y registrará en una hoja de notas (formato anexo 1), dará número de serie comenzando con el Nro. 1 hasta n, a los cd, y indicando de que hardware y los archivos grabados en general.

Ø El Cd formalizado y destinado a Tribunales, será almacenado en una caja de cartón adecuada, evitando su deterioro y destrucción de sellos, donde se mantendrá hasta su remisión a Tribunales si es necesario.

- El Personal de Carabineros de Chile, comenzará la fijación y respaldo en cd, del hardware existente y que reuna las condiciones técnicas y de configuración, que permita la existencia de LOG, Archivos de Sistema, etc., en el siguiente orden :

Ø Accediendo directamente y previa autorización, al equipo I.D.S., desde donde obtendrá los archivos integros de LOG, editará si es necesario los archivos de sistema, observará y tomará nota de las I.P. registradas y sospechosas, de los procedimientos adscritos a estas I.P., de los puertos en uso, del procedimiento utilizado para invadir e ingresar sin autorización desde el exterior y los terminales de la red que se logran identificar con algun procedimiento sospechosos realizado.

Ø Mismo procedimiento se realizará, siempre y cuando técnica y de configuración permita que el Firewall haya almacenado los intentos de ingresos externos o internos, respaldando los archivos necesarios y convenientes para la investigación.

- Revisado y respaldado los hardware de seguridad de la red, se dedicará a la revisión y respaldo del Servidor.

Ø Obtendrá, editará y respaldará los archivos “sensibles para la empresa, importantes u oportunos” que sea necesario fijar, no siendo determinante su mayor o menor tamaño.

Ø Verificará la existencia de archivos tipo Troyanos en algun archivo del servidor, que permitiese el ingreso posterior del hacker.

Ø Verificará la existencia de archivos modificados, reemplazados o eliminados, por medio de los registros del LOG del Servidor de la red o del I.D.S.

Ø Se obtendrá del Administrador de Red o persona responsable una copia del último respaldo realizado al Servidor, de utilidad para verificar la existencia de destrucción o adulteración de archivos.

- Revisado el Servidor, se procederá a la revisión y respaldo de todos los terminales en uso o fuera de servicio que los registros puedan determinar como parte del procedimiento sospechoso, desde donde se procederá a lo siguiente:

Ø Verificará las políticas de seguridad aplicados en la empresa afectada, de password y niveles de administración de los usuarios.

Ø Revisará archivos, registros, elementos de programas ajenos o sospechosos al servicio de la red, archivos temporales, etc.

- Una vez revisado y respaldado la totalidad de los elementos de seguridad y terminales de la red:

Ø Procederá con la información obtenida, especialmente de los archivos LOG del IDS, a repetir integramente el procedimiento de ingreso no autorizado a la red, con la finalidad de constatar inmediatamente la validez de ese recurso, por lo cual ubicará el Notebook en la parte externa de la red, repetirá los comandos preestablecidos, ingresará a la red y registrará su paso en uno de los terminales, ya antes seleccionado.

Ø Luego, procederá a la revisión y respaldo en un solo cd de la información obtenida en el IDS., Firewall y terminal seleccionado donde quedó el registro.

- Como segundo elemento de seguridad para el respaldo, especialmente archivos LOG, es necesario y advertir la configuración conveniente para que los hardware de seguridad, especialmente IDS y Firewall, mantengan habilitados el registro de LOG, advertencia oportuna de intentos de ingreso no autorizado, remisión via correo electrónico de los archivos LOG, más sensibles e importantes, sacándolos del área de manejo de un hacker especializado, tomando en consideración que estos documentos por disposiciones legales internacionales, son autentificadas de hecho, puede probarse por cualquier medio: “testimonios referentes a las circunstancias que rodean al mensaje, las funciones internas del mensaje o bien por una demostración del procedimiento utilizado para producirlo”[ii]

Finalizado el proceso de fijación y respaldo de la información contenida en la red de informática, se podrá autorizar a proceder a conectar la red al área externa (internet, host, ISP).

Detectado la presencia de adulteración, borrado o copiado de archivos tanto del Servidor o uno de sus terminales de trabajo, podrá proceder a apagar, levantar y retirar este equipo, conforme a los siguientes pasos.

2.4.- Búsqueda, revelado y recogida de pruebas.

Debemos considerar que estamos frente a una situación, en que nuestras pruebas de la acción de hackeo, la encontramos tanto en el hardware o en el software, o en ambos simultaneamente. Del hardware es conveniente que la evidencia sea procesada y almacenada en un lugar o laboratorio idoneo para ello, en este lugar ayudará al investigador a desarrollar una variedad de preguntas, como tambien experimentar e interactuar dentro de un campo del desarrollo computacional. Se recomienda que este laboratorio medianamente incluya:

-Ethernet

-Estaciones Linux

-Estaciones Unix

-Pcs.

-Sistema de grabación, lector /grabador de cd

-Capacidad de movimiento de partes y piezas de hardware y suficiente espacio en blanco para software y drivers.

-Instalaciones físicas debidamente controladas en su acceso y de ambiente (temperatura, húmedad, luz).

Tambien es necesario, recoger las herramientas de software, necesarias para la investigación de un crimen o fraude computacional, software que deberan ser usados convenientemente para preservar las evidencias en laboratorio. Esto incluiría sistemas operativos, base de datos de sistemas (para ir guardando y analizando datos), programas de archivos de datos para el manejo seguro de respaldo de cintas y sistema de lectura/grabación de cd y en su caso sistema de administración de control. En el caso del sistema de administración, es una pieza clave en el proceso de investigación, ya que proporciona al investigador como un medio de almacenar sus apuntes y sobre la información, sobre todo de las actuaciones y puntos en una investigación dada, como tambien la de mantenerse en el caso de la repetición en el tiempo de sucesos similares.

Las preguntas sobre “quien”, “que”, “donde”, y “como”, son una dirección para cada caso en los archivos de datos para el sistema de administración. Idealmente estos datos deberan ser almacenados e interactuaran en una manera segura. Cuando en el caso de datos sean transmitidos o archivados, estos deberan ser debidamente encriptados, y en el caso de acceder a ellos será a traves de los medios convenientes de autentificación. En el curso de la investigación, el sistema de administración suministrará todo de las caracteristicas de cualquier base de datos. Tambien este sistema de administración deberá ser accesible desde fuera del laboratorio de preservación de evidencias, a fin que el investigador al encontrarse en el area de trabajo externa pueda acceder a notas del caso de la investigación.

2.5.- Levantamiento: El levantamiento de las pruebas encontradas en el Sitio Informático de Hackeo, es de una gran complejidad y consiste en recoger las pruebas encontradas, maniobra que siempre debe realizarse posteriormente a la fijación y por el personal experto y claramente identificado para dicha labor.

Recoger evidencias en el sitio del suceso y conservar su valor potencial de prueba en la comprobación del hecho, significa manipular los objetos respetando ciertas técnicas que haremos conocidas y que están en relación con el objeto y con el sentido común. Todas las precauciones son válidas para evitar que las huellas y rastros sean destruidos, ya que de omitirse esta diligencia todo el trabajo aplicado en la protección del sitio del suceso quedaría nulo.

Para ello, se ceñiran a las siguientes reglas generales:

Seguimiento de las Evidencias Computacionales

Ø Para mejor examen, someter solo la unidad de procesador central y los medios de almacenamiento externos e internos.

Ø Use un contenedor de carton duro para cuando envie los componentes del computador. Si es posible, use la caja original con el relleno adecuado. Use sin limitaciones goma plastica de envoltura o espuma de goma de caucho como contenedor. No use poliestireno suelto, debido que al interior roza el computador y / o sus componentes y crean cargas estaticas que pueden causar perdida de datos o daños a la placa de circuitos. Selle el contenedor con una cinta fuerte de embalaje.

Ø El paquete y la unidad del procesador central en la posición correcta. En el exterior del contenedor dira **ESTE LADO ARRIBA.**

Ø Discos, cartridges, cintas, discos duros, deben ser empacados para evitar los movimientos durante el envio.

Ø Parte exterior del contenedor dira **FRAGIL, EQUIPO ELECTRONICO SENSIBLE** y **MANTENER RETIRADO DESDE MAGNETOS O CAMPOS MAGNETICOS.**

Requerimientos de Examen de evidencias.

Todos los requerimientos para examen de evidencias deben indicar claramente escrito la dirección del destinatario y la información del contenido enviado:

Ø Nombre de la persona enviada, empresa, dirección y número de teléfono.

Ø Numero de identificación del caso, evidencia enviada y antecedentes relativos al mismo.

Ø Descripción de la naturaleza y los datos básicos concernientes al caso, dando lo pertinente al laboratorio examinador.

Ø El nombre o nombres y la descripción de los datos sobre la persona o Personas involucradas (sujetos, sospechosos, victima, o una combinación de todas estas categorias) y la persona responsable del caso y;

Ø Una lista de las evidencias contenidas y enviadas (cerradas) y bajo las cubiertas separadas.

· La evidencia adjuntada, debe estar limitada al tamaño del contenedor, para que no resulten peligrosas para su transporte. Escriba en la sobrecubierta la evidencia que se encuentra al interior, para evitar daños o alterar las evidencias. El documento escrito nos mostrara e indicara la evidencia que se esta adjuntando, como separadamente, por el tipo de evidencia.

· La separación al interior del embalaje es usada para enviar numerosas o distintos items de evidencia o ambas clases de evidencias. Se incluirá una copia del documento petitorio de evidencia. La comunicación escrita enviada mostrara una lista detallada del contenido de la caja, separados por la división interior del empaque, para el seguimiento en los distintos puntos de las evidencias.

Ø El estado y tipos de examenes requeridos.

Ø El estado, cuando la evidencia ha sido devuelta y cuando el laboratorio nos envia su reporte, sea parcial o final.

Ø Adjuntar una información si la evidencia fue examinada por otros expertos en algun otro campo de especialidad, si ellos estan alguna controversia, o si otra sección tiene interes en el caso.

Ø Estudiar la necesidad, razon o razones para el examen de los expedientes por otras personas, no se requerirá un expediente para examenes rutinarios.

Ø Enviar separadamente las conclusiones para casos multiples.

Para ello, el trabajo con estos medios de fijación electrónica, se encuentran avalados mediante la Ley Nro. 18.857, introduce modificaciones al Código de Procedimiento Penal, que a la letra dice: “Art. 113 bis. Podrán admitirse como pruebas películas cinematográficas, fotografías, fonografías, y otros sistemas de reproducción de la imagen y del sonido, versiones taquigráficas y, en general, cualquier medio apto para producir fe. Estos medios podrán servir de base a presunciones o indicios”, y lo expresado en el Art. 203, del Código Procesal Penal, que a la letra dice “**Medios de prueba no regulados expresamente**. Además de los medios de prueba expresamente regulados en la ley, podrán admitirse como pruebas las películas cinematográficas, fotografías, fonografías, videograbaciones y otros sistemas de reproducción de la imagen y del sonido, versiones taquigráficas y, en general, cualquier medio apto para producir fe. El tribunal determinará la forma de su incorporación al procedimiento, adecuándola en lo posible al medio de prueba más análogo.”[iii]

Para lo anterior, el encargado de la sección especializada o más antiguo del equipo de trabajo, que tiene como responsabilidad la de registrar en las hojas de datos, deberá registrar en un acta el equipo, acorde a los antecedentes considerados en el formato. (anexo 2), acta que considera la firma de la o las personas responsables.

Para el cumplimiento de las formalidades establecidas en la Ley; es de conveniencia que este proceso sea desarrollado por dos personas hábiles (mayores de 18 años), capaces de comparecer en juicio, con conocimientos en el área de investigación y que se encuentren plenamente de acuerdo en sus dichos.

3.- Tratamiento de las evidencias:

3.1.- Custodia: consiste en cuidar de que las evidencias, pruebas o cualquier elemento encontrado no se pierdan ni deterioren hasta que lleguen a su final destino. Esta custodia debe realizarse desde el mismo sitio del hackeo y se debe contar con una dependencia apropiada que permita la custodia de las evidencia impidiendo cualquier tipo de sustracción y una adecuada conservación. Para ello se aplicara un documento en el que constará toda persona, sea cual sea su relación con el S.I.H., y que haya tomado contacto con el equipo objeto de investigación, desde el momento mismo de la información del hackeo.

3.2.- Envío: posterior a la custodia las evidencias deben ser remitidas a los laboratorios y tribunales pertinentes, debiendo tener la precaución de adjuntar la totalidad de las evidencias obtenidas, elementos encontrados y cualquier antecedente recopilado, como también todos los documentos probatorios.

4.- Trabajo de Laboratorio Forense Informático:

4.1.- RECEPCION DE LOS MEDIOS DE PRUEBA Y RESPALDOS DE ARCHIVOS.

Recibido los medios de prueba, respaldos, hardware y cualquier elemento recogido en el Sitio del Suceso de Hackeo, el personal responsable de esa área, procederá a lo siguiente:

Ø Recibir cada una de las especies enviadas, con su correspondiente detalle escrito sobre sus características particulares, identificación y estado de uso general.

Ø En el caso de las pruebas de Respaldo de Archivo, las recibirá, comprobará su existencia, registrará su nombre y céd. de identidad en la Hoja de Cadena de Custodia, (anexo 3), como tambien de sus sellos y estado general.

Ø Los respaldos de archivos, serán almacenados en un lugar seguro, cerrado y de acceso restringido a cualquier persona.

Ø Se verificará la existencia de los otros elementos recogidos, su estado general, de su embalaje, conservación y registrará su nombre y céd. de identidad en la Hoja de Cadena de Custodia.

Ø Todos los elementos recibidos, serán almacenados en un ambiente adecuado, evitando la exposición a compuestos corrosivos, humedad, zonas de campos electromagnéticos o de alta o baja tensión,

Ø Los elementos en cuestión, serán desembalados exclusivamente para su pericia y revisión, finalizado este procedimiento volverán a ser embalados adecuadamente y en las mismas condiciones de su recepción.

Ø Se tomarán precauciones para que el Personal Técnico, use las vestimentas adecuadas (antiestáticas) y brazaletes o soportes a tierra, etc.

CAPITULO IV

¿A QUIEN BUSCAMOS?

1.- ANTECEDENTES CRIMINOLOGICOS DEL PERFIL HACKER

Nuestra labor como investigadores y entrega de Servicio Forense Informático, nos obliga a encontrar y determinar al o los responsables, para ello es conveniente conocer su perfil y modus operandi, de esta manera, el autor mexicano Julio TELLEZ VALDEZ, en su trabajo de investigación, señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)". Por su parte, el tratadista penal italiano Carlos SARZANA, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

Según el investigador, este tipo de acciones presentan las siguientes características principales:

a. Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

b. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se haya trabajando.

c. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" a aquellos que las realizan.

e. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

f. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

g. Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i. En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j. Ofrecen facilidades para su comisión a los menores de edad.

k. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

2.-Clasificación de estos delitos, de acuerdo a los criterios:

2.1.- Como instrumento o medio.

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
b. Variación de los activos y pasivos en la situación contable de las empresas.
c. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
d. Lectura, sustracción o copiado de información confidencial.
e. Modificación de datos tanto en la entrada como en la salida.
f. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
g. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
h. Uso no autorizado de programas de computo.
i. Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
j. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
k. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
l. Acceso a áreas informatizadas en forma no autorizada.
m. Intervención en las líneas de comunicación de datos o teleproceso.

2.2.- Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a. Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.
c. Daño a la memoria.
d. Atentado físico contra la máquina o sus accesorios.
e. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f. Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje o comerciales.

CAPITULO V

FINALIZACIÓN.

5.- CONFECCION DE LOS INFORMES:

La persona encargada de la confección de los informes, deberá considerar los siguientes aspectos:

- Relación cronológica de los hechos que investiga.
- Metología utilizada para la realización de sus pericias.
- Los métodos tecnicos, de software y hardware utilizados.
- Usar un lenguaje convenientemente de uso común, para su fácil comprensión por personas ajenas a las labores de informática.
- Detallar en la medida de lo posible, la relación de hechos, acciones y consecuencias del hecho investigado.
- La descripción de la persona o cosa que fuere objeto de él, del estado y modo en que se hallare
- La relación circunstanciada de todas las operaciones practicadas y su resultado
- Las conclusiones, que en vista de su labor, formulen los profesionales, conforme a los principios de su ciencia, arte u oficio.[iv]
- Confeccionar en informes distintos, conclusiones de areas distintas de investigación.
- El desarrollo y confección de los informes, deberán ser cuidadosamente respaldados en un sistema de administración, debidamente asegurados y encriptados.

JOSE ALFONSO TOLEDO DUMENES

Capitan de Carabineros

7.- INDICE

CAPITULO I

¿A QUIEN BUSCAMOS?

CAPITULO V

FINALIZACIÓN.

_____

(anexo Nro. 1)

ACTA LEVANTAMIENTO DE FIJACIÒN Y RESPALDO ARCHIVOS

En Santiago, a _____ días del mes de _____ del año _____, quien abajo firma, procede a levantar acta por la custodia y traslado de la Fijación en Sistema de Respaldo Disco Compacto, correspondiente al proceso de Trabajo Informático Forense en _____, bajo la responsabilidad de _____,Céd. de Id. Nro. _____, conforme al siguiente detalle:

Nro. Cd. Lugar de Respaldo Archivo OBSERVACION

1.- _____

2.- _____

3.- _____

4.- _____

5.- _____

6.- _____

7.- _____

8.- _____

TESTIGOS:

Ø _____ _____

Ø _____ _____

FIRMA RESPONSABLE

_____

Nota: Tarjar espacios en blanco/firmas completas/

(anexo Nro. 2)

ACTA LEVANTAMIENTO DE ESPECIES

En Santiago, a _____ días del mes de _____ del año _____, quien abajo firma, procede a levantar acta por la custodia y traslado de las especies, correspondiente al proceso de Trabajo Informático Forense en _____, bajo la responsabilidad de _____,Céd. de Id. Nro. _____, conforme al siguiente detalle:

Nro.Orden ESPECIE OBSERVACION

1.- _____

2.- _____

3.- _____

4.- _____

5.- _____

6.- _____

7.- _____

8.- _____

TESTIGOS:

Ø _____ _____

Ø _____ _____

FIRMA RESPONSABLE

_____

Nota: Tarjar espacios en blanco/firmas completas/las especies deberán ser debidamente guardadas y selladas.

---

[i] Leyes y Negocios en Internet, Oliver Hance.

[ii] C.Durham"Las structures émergentes du droit criminel de l´information: tracer les contours d´un nouveau paradigme"

[iii] Art. 203, del Código Procesal Penal.

[iv] Art.237º del Código de Procedimiento Penal, Art. 244º del Código Procesal Penal.