ESTADO LIBRE Y SOBERANO DE CHIHUAHUA
Secretaría de Educación, Cultura y Deporte

FISCALÍA GENERAL DEL ESTADO

T E S I N A

PRÓTOCOLO DE OPERACIÓN PARA LA CONFISCACIÓN DE LA EVIDENCIA DIGITAL EN EL ESTADO DE CHIHUAHUA

Para obtener el Grado de:

MAESTRO EN GESTIÓN DE SISTEMAS DE SEGURIDAD PÚBLICA

Catedrático Tutor: Dr. José Caín Lara Dávila

Postulante: Angela María Vega Assmar

Chihuahua, Chih. 18 de diciembre de 2015

Chihuahua
Gobierno del Estado
Fiscalía General

ESTADO LIBRE Y SOBERANO DE CHIHUAHUA

Secretaría de Educación, Cultura y Deporte

FISCALÍA GENERAL
CHIHUAHUA
ESCUELA ESTATAL DE POLICÍA

FISCALÍA GENERAL DEL ESTADO

ESCUELA ESTATAL DE POLICÍA

T E S I N A

PRÓTOCOLO DE OPERACIÓN PARA LA CONFISCACIÓN DE LA EVIDENCIA DIGITAL EN EL ESTADO DE CHIHUAHUA

Para obtener el Grado de:

MAESTRO EN GESTIÓN DE SISTEMAS DE SEGURIDAD PÚBLICA

ESTADOS UNIDOS MEXICANOS
ESTADO LIBRE Y SOBERANO DE CHIHUAHUA
FISCALÍA GENERAL DEL ESTADO
ESCUELA ESTATAL DE POLICÍA
08OSU0001E
CHIHUAHUA, CHIH.

Catedrático Tutor: Dr. José Caín Lara Dávila

Postulante: Angela María Vega Assmar

Chihuahua, Chih. 18 de diciembre de 2015

AGRADECIMIENTOS

A Dios

A mi familia

GLOSARIO

PGR	Procuraduría General de la República.
Carding	Uso ilegitimo de las tarjetas de crédito.
TELMEX	Teléfonos de México.
PIN/ NIP	Personal identification number/número de identificación personal.
MICROSOFT	Empresa multinacional de origen estadounidense,fundada el 4 de abril del 1975, por Bill Gates y Paul Allen.
FARC	Fuerzas armadas revolucionarias de Colombia.
PGP	Privacidad bastante buena.
ICE	U.S Immigration and Customs Enforcement.
LFPDPPP	Ley Federal de Protección de datos personales en posesión de particulares.
OCDE	Organización para la cooperación y desarrollo económicos.
RAM	Random Access Memory/ Memoria Volátil.
CD	Compac Disc.
DVD	Disco Versatil Digital.
IPODS	Intelligence Portable Device/Aparato Portable Inteligente.
GPS	Sistema de navegación y localización mediante satélites.
Skimmers	Herramienta utilizada por los delincuentes para clonar tarjetas.
IDE	Integreted Device Electronic.
USB	Univesal Serial Bus.
e-mail	Correo electrónico.
Logs	Registro/bitácora.
Torrents	Es un pequeño archivo con extensión ".torrent". Este archivo contiene la dirección de un "servidor de búsqueda" encargado de localizar posibles fuentes con el archivo o parte de él. Los archivos se descargan por partes, en secuencias aleatorias, directamente desde las computadoras que tienen dichas partes.
Crackeo	Es un parche cuya finalidad es la de modificar el comportamiento del software original y creado sin autorización del desarrollador del programa.
Software	Programas que permiten realizar rutinas a una computadora.
Malware	Malicious Software.
Troyanos	Software malicioso que se presenta al usuario como legítimo.

INDICE

CAPITULO CUARTO

4. PROTOCOLO PARA LA CONFISCACIÓN DE PRUEBAS DIGITALES

CAPITULO QUINTO
5. CRÍMENES Y EVIDENCIA POTENCIAL

ANTECEDENTES

La delincuencia ha migrado sus operaciones a la red, bajo perfiles falsos circulan en el "anonimato" que brinda internet: defraudadores, estafadores, tratantes de personas, distribuidores de pornografía infantil y hasta células del crimen organizado, operando libremente con una simple conexión a la web.

Las redes sociales, los teléfonos inteligentes, blogs, sitios web entre otros, han propiciado que estos medios faciliten el flujo de la información donde ciberdelincuentes se aprovechan de cualquier omisión para burlar las leyes y de esta manera perpetrar distintos tipos de delitos y continuar operando impunemente.

La Fiscalía del estado de Chihuahua creó la Unidad Estatal de Delitos Electrónicos e Informáticos en el año 2010, con la finalidad de dar seguimiento a los nuevos medios que están utilizando los criminales para cometer delitos, sin embargo la inexistencia de protocolos de operación para la confiscación y la falta de un laboratorio para el análisis forense de la evidencia digital, provoca que distintas evidencias sean desechadas en los juicios. En el 2013 la Unidad Estatal de Delitos Electrónicos e Informáticos colaboró en coordinación con la Procuraduría General de la República (PGR), en una investigación a cinco personas dedicadas a la clonación de tarjetas de crédito (carding), los distintos domicilios de los miembros de la banda fueron incautados, fueron encontradas una gran cantidad de tarjetas de crédito y equipo para realizar carding, sin embargo el procedimiento de confiscación y de análisis forense no fue el apropiado, ya que la evidencia recolectada se contaminó por parte del equipo de requisa (Los policiacas ministeriales son quienes hacen el levantamiento de evidencia electrónica, sin un procedimiento formal, en contadas ocasiones los peritos informáticos que se encuentran en el área de servicios periciales acuden a las escenas del crimen); esto por no contar con un protocolo formal, ni con material, ni equipo o herramientas especializadas., al presentar el análisis durante el juicio las pruebas fueron desechadas y los clonadores quedaron en libertad, el líder de la banda que fuera trabajador de Telmex, recibió salarios caídos al quedar "libre de cargos".

Es por ello que como objetivo general de este proyecto se establece lo siguiente: Analizar la eficacia de los protocolos de operación actual para la confiscación y análisis de la evidencia

digital en el estado de Chihuahua y como objetivo particular: Establecer un protocolo de operación para la confiscación y análisis de la evidencia digital en el estado de Chihuahua.

Es por ello que para eficientar las labores operativas en materia electrónica e informática de la Fiscalía General del estado de Chihuahua se harán un análisis del protocolo actual de confiscación de la evidencia electrónica y digital con el que se cuente.

En esta tesina se abordaran los siguientes temas: en el capítulo primero hablaremos de manera general de los delitos y conductas en materia electrónica e informática específicamente de lo que se observa como recurrente en el estado de Chihuahua, en el capítulo dos se describen los casos relevantes en distintas partes del mundo en relación a esta materia. El capítulo tercero abordará el tema de la regulación (legislación) donde se brinda un panorama de las distintas leyes en materia internacional, nacional y estatal que regulan lo relacionado a los delitos electrónicos e informáticos. El capítulo cuarto proporciona información sobre buenas prácticas para la confiscación de pruebas digitales, el capítulo quinto sobre los crímenes más comunes que se presentan y la evidencia potencial que se deberá confiscar en una requisa, finalmente el capítulo sexto es la propuesta de los formularios a utilizar para la confiscación, terminando con la conclusión y recomendaciones correspondientes.

CAPITULO PRIMERO

1. DELITOS Y CONDUCTAS EN MATERIA ELECTRÓNICA E INFORMÁTICA

El maestro (Valdés J. T., 2005) conceptualiza, a los delitos informáticos clasificándolo de dos maneras, la primera como aquel delito informático típico, que son aquellas conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y la segunda a delito informático atípico, que son las actitudes ilícitas en el que se tiene a la computadoras como instrumento o fin.

(Lima, 1984) define que el *delito electrónico* en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin.

1.1 Tipos de delitos en materia electrónica e informática

El análisis de la tipología de los delitos y conductas que se mencionan a continuación son solo algunos de los tantos que existen actualmente, el extracto recopila el nombre de los casos con mayor incidencia registrados por la Unidad de Delitos Electrónicos e Informáticos en el Estado de Chihuahua desde su creación.

1.1.1 Phishing: (Guerrero, 2010) El método más común consiste en la recepción de mensajes de correos falsos, de diversas entidades bancarias, de las que, se puede o no ser cliente, donde se le solicita por distintos motivos que facilite sus datos así como que se introduzca el código PIN. Esta modalidad tiene como objetivo conseguir la mayor cantidad posible de datos personales y bancarios, con el fin de ser utilizados posteriormente de forma fraudulenta. Por ello suplantan de manera impecable la identidad de las entidades bancarias reales.

1.1.2 Sabotaje informático: (Ledeira, Cortizo, Sánchéz 2006) definen esto como una especialidad dentro de los delitos informáticos constituyendo uno de los atentados contra los sistemas de procesamiento de datos de mayor gravedad. El sabotaje informático tiene dos formas claramente diferenciadas: puede producirse por medio de la modificación y/o destrucción de los datos o programas del afectado, o puede producirse por medio de la paralización o bloqueo del sistema sin que necesariamente se produzca alteración ni destrucción de los datos o programas.

1.1.3 **Uso y acceso ilícito a los sistemas de información:** Quien accede a un sistema informático de manera no consentida, independientemente de si lleva a cabo algún tipo de daño en el sistema o algún perjuicio al propietario del equipo; (a quien se mantiene dentro de un sistema informático en contra de la voluntad de quien lo tiene).

1.1.4 **El robo o usurpación de identidad:** De acuerdo al centro de seguridad y protección de Microsoft el robo de identidad no es nuevo. Los ladrones siempre han encontrado modos de apropiarse ilegalmente de información personal mediante engaños (también conocido como ingeniería social), robando el correo de los buzones e incluso revisando hasta los botes de basura. Ahora que el robo de identidad se ha trasladado a internet, los delincuentes pueden engañar a una mayor cantidad de personas, lo que lo hace un delito más rentable y de gran crecimiento

1.1.5 **Ciberacoso:** (También llamado cyberbullying por su traducción al inglés). Los intimidadores suelen atormentar a sus víctimas cara a cara, ya sea en el colegio, en el parque o al practicar un deporte. Sin embargo, en la actualidad, el ciberacoso o la intimidación en línea puede ocurrir en cualquier momento del día a través de equipos informáticos, teléfonos móviles, consolas de videojuegos u otros medios conectados a Internet.

1.1.6 **Grooming:** El sitio en internet Delitos Informáticos define al grooming como uno de los delitos que más se suscitan y que tienen como fin el acoso y abuso sexual. De entre ellos destaca por su gravedad ya que dirigido a menores, en estos casos, el delincuente, mediante un perfil falso en las redes sociales, se gana la confianza del menor, generalmente haciéndose pasar por otro niño.

1.1.7 El sitio pantallas amigas1 define el sexting como él envió de contenidos de tipo sexual (principalmente fotografías y/o vídeos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles.

---

[1] Pantallas Amigas: es una iniciativa que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia: http://www.pantallasamigas.net/ Año: 2004

1.1.8 Amenazas: Son un delito o una falta, consistente en el anuncio de un mal futuro ilícito que es posible, impuesto y determinado con la finalidad de causar inquietud o miedo en el amenazado.

Actualmente el estado de Chihuahua cuenta con una legislación vigente derogada el 19 de Noviembre del 2011 título vigésimo segundo en delitos contra la seguridad y el normal funcionamiento de las vías de comunicación y de los medios de transporte. Capítulo IV del uso y acceso ilícito a los sistemas y equipos informáticos y de comunicación de delitos contra la seguridad y el normal funcionamiento de las vías de comunicación y de los medios de transporte, acceso ilícito a los sistemas y equipos informáticos y de comunicación contenida en el artículo 327 la cuál apoya a la prevención e investigación de los delitos que se cometen por medios informáticos, la cual no está tipificada.

La Fiscalía por medio de la Unidad Estatal de Delitos Electrónicos e Informáticos que opera desde las mismas fechas de la promulgación de dicha ley, sin embargo la Unidad se ha enfrentado a la problemática de que la víctimas no conocen que leyes les protegen en esta materia y ni los Ministerios Públicos que en ocasiones no saben orientar a los afectados sobre estos temas, quedando sin registro las distintas denuncias que se interponen en las Unidades Especializadas o bien proporcionando información que no es correcta a la víctima la que termina desistiendo a la hora de interponer una denuncia de manera formal.

CAPITULO SEGUNDO

2. CASOS RELEVANTES EN MATERIA DE DELITOS ELECTRÓNICOS E INFORMÁTICOS

Antiterrorista, D. d. (30 de 9 de 2010). Las computadoras e internet son un aspecto típico de la vida cotidiana. A diario, gente de todo el mundo se pasa horas frente a las computadoras o utilizando dispositivos móviles para enviar y recibir mensajes, navegar por internet, actualizar bases de datos y participar en un sinfín de otras actividades.

Lamentablemente quienes cometen delitos no se han quedado fuera de la revolución informática. Los delincuentes y los terroristas utilizan la tecnología moderna, como teléfonos celulares, computadoras portátiles, servidores de red e internet como herramientas para cometer delitos.

En algunos casos, las computadoras constituyen el medio para cometer un delito. Por ejemplo puede utilizarse el internet para enviar una amenaza de muerte por correo electrónico, app o alguna red social, lanzar ataques a una red informática vulnerable, diseminar virus informáticos o transmitir imágenes de pornografía infantil.

Las computadoras y otros medios digitales constituyen posibles fuentes de pruebas de delitos que superan el ámbito cibernético. En algunos casos, la tecnología no es el medio para cometer el delito sino un depósito de fácil acceso.

2.1 Lista de cosas para hacer de Santana Basu

Santanu Basu, agente de seguros, fue condenado en los Estados Unidos por homicidio. El mismo día en que le vendió a su novia una póliza de seguros por US$100,000 en la cual figuraba él como único beneficiario.

La policía incautó la computadora que utilizaba en la agencia de seguros donde trabajaba. Una simple búsqueda por palabra reveló que Basu había planeado el homicidio de antemano compilando una "lista de cosas por hacer". Más adelante se descubrió que Basu había escrito esta lista primero en papel, luego la había transferido a su teléfono inteligente y finalmente a la computadora. En la lista figuraban actos como "comprar municiones", "alquilar vehículo" y "verificar póliza de seguros".

2.2 Confiscación de computadora portátil de las FARC

El ejército del pueblo también conocido como las FARC[2] es un grupo insurgente conocido por atacar blancos militares, políticos y económicos de Colombia. Las FARC también están involucrada en narcotráfico, secuestros, extorsión, homicidio y otras actividades delictivas.

Luis Edgar Devia-Silva, integrante de la secretaría y asesor del Bloque Sur de las FARC, murió a mano de las fuerzas de seguridad colombianas en un operativo militar el 1° de marzo de 2008. Devia-Silva abogó por la ampliación de las actividades de tráfico de cocaína al mundo, la imposición de impuestos al comercio de drogas en Colombia para recaudar fondos.

Durante el operativo militar que desencadenó la muerte de Devia-Silva se incautaron tres computadoras portátiles. Según las autoridades colombianas, en todas las computadoras abundaba información sobre las FARC, incluidos sus operativos y conexiones. Se contrató a un grupo de expertos de la INTERPOL[3] a fin de que examinaran las computadoras y sus periféricos. El alcance del análisis realizado por la INTERPOL fue limitado: certificar si el gobierno colombiano de alguna manera había alterado la información. No se les pidió que examinaran el contenido de los documentos. En el informe realizado por la INTERPOL, se indicó que los documentos clave no se habían dañado ni modificado pero se observó que tras la incautación, se había manejado y accedido a los dispositivos sin protección contra escritura.

Más de 3,500 archivos contenían una fecha y hora que indicaban que se habían creado o modificado después de la fecha de incautación. En el informe se indicó que "estos archivos habían sido creados originalmente antes del 1° de marzo de 2008, en uno o más dispositivos que tenían mal configurada la fecha y la hora". La lista de información compilada por la INTERPOL y recuperada de los dispositivos incluye más de 30,000 documentos escritos y más de 7,000 direcciones de correo electrónico.

2.3 Metadatos del asesino BTK

Entre 1977 y 1979, el asesino BTK[4], iniciales impuestas por sí mismo que describen su modus operandi cobró la vida de más siete víctimas. Si bien dejaba rastros de ADN[5] en las escenas del crimen, realizaba llamadas telefónicas para denunciar los asesinatos cometidos y

---

[2] Las Fuerzas Armadas Revolucionarias de Colombia http://www.definicionabc.com/historia/farc.php Año: 2015
[3] International Criminal Police Organization http://es.thefreedictionary.com/Interpol Año: 2015
[4] Bind, torture, kill/ Atar, torturar, matar. Traducción del autor
[5] Acido desoxirribonucleico, ácido nucleico que contiene la información genética de un ser vivo. http://es.thefreedictionary.com/ADN Año:2015

enviaba cartas a periódicos locales en los que confesaba haber sido el autor de dichos homicidios, el asesino BTK evitó ser identificado durante casi 30 años.

Habiendo pasado por un aparente anonimato en las décadas de los años ochenta y noventa, el asesino comenzó a volver a enviar cartas en el 2004 en las que se adjudicaba otros tres homicidios, dos de los cuales se habían cometido en la década de los ochentas y el otro en 1991. En una de las cartas, se apartó del proceso anterior de enviar cartas fotocopiadas y en su lugar, le envío a la policía un archivo con un documento tipo texto vía electrónica.

Tras realizarse un análisis forense, se supo que allí estaba otro documento que había sido borrado. La policía recupero el archivo y examinó sus propiedades, en las que figuraba que el autor era un tal "Dennis" y el lugar donde había sido creado pertenecía a "Christ Lutheran Church[6]". Una búsqueda rápida en el sitio web de la iglesia reveló que Dennis Rader, sospechoso previamente no identificado era integrante de la junta directiva de la iglesia. La policía descubrió que Rader había creado el documento borrado en la computadora de la iglesia.

Con un sospechoso identificado, los investigadores pudieron recopilar pruebas contundentes que llevaron al arresto de Dennis Rader, quien se encuentra en la cárcel de Arizona cumpliendo 10 sentencias consecutivas de cadena perpetua.

2.4 Portátil de Sebastien Boucher

El 17 de diciembre de 2006, cuando Sebastien Boucher cruzaba la frontera de Canadá a los Estados Unidos por Derby Line, Vermont, le inspeccionaron la computadora portátil (modelo Alienware D9T). La computadora estaba cargada, lo cual permitió que se viera el contenido. Los agentes del ICE[7] presuntamente vieron imágenes de pornografía infantil, por lo cual incautaron la computadora, interrogaron a Boucher y luego lo arrestaron con acusación formal de haber transportado pornografía infantil.

Cuando se encendió la computadora y arrancó el 29 de diciembre de 2006, no se podía acceder a toda la información almacenada. Esto se debía a que la computadora portátil estaba protegida con un cifrado en un disco PGP[8], por ende los investigadores que trabajaban con el gobierno estadounidense no pudieron ver el contenido del disco Z, en el que presuntamente se

---

[6] Christ Lutheran Church/ Iglesia Luterana Cristo. Traducción del autor

[7] ICE: U.S. Immigration and Customs Enforcement https://www.ice.gov/ Año:2015

[8] Privacidad bastante buena o muy buena protección. http://www.abbreviationfinder.org/es/acronyms/pgp.html Año:2015

encontraba el contenido ilícito. Luego, el jurado le emitió una cita judicial al acusado en la que exigía que entregara la contraseña para la clave de cifrado que protegía los datos. Con el tiempo, Boucher entregó la clave, gracias a lo cual la policía pudo ubicar las imágenes de pornografía infantil, lo condenaron, le impusieron una pena de tres años de cárcel y lo deportaron.

Es por ello la importancia de la confiscación y el análisis de la evidencia digital para poder sustentar un caso, de esta manera al presentarse adecuadamente ante un juez puede tomar la decisión acertada en cuanto a un caso de esta índole y no dejar libre a un criminal peligroso.

CAPITULO TERCERO
3. REGULACIÓN LEGAL DE LOS DELITOS ELECTRONICOS

3.1 Convenio de sobre cibercriminalidad del Consejo de Europa

El Convenio sobre ciberdelincuencia, también conocido como el Convenio de Budapest sobre ciberdelincuencia o simplemente como Convenio Budapest, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China.

El Convenio y su informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001. El 23 de noviembre de 2001 se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004. A partir del 28 de octubre de 2010, 30 Estados firmaron, ratificaron y se adhirieron a la convención, mientras que otros 16 estados firmaron la convención, pero no la ratificaron.

El 1 de marzo de 2006, el protocolo adicional a la convención sobre cibercrimen entró en vigor. Los Estados que han ratificado el protocolo adicional son necesarios para penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como de las amenazas racistas y xenófobas e insultos.

3.1.1 Objetivos

El convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Los principales objetivos de este tratado son los siguientes:

- La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.
- La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.
- Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

Los siguientes delitos están definidos por el Convenio: acceso ilícito, interceptación ilegal, la interferencia de datos y del sistema, mal uso de los dispositivos, la falsificación informática, el fraude relacionado con la informática, los delitos relacionados con la pornografía infantil y los delitos relacionados con los derechos de autor y derechos conexos.

Asimismo, se exponen cuestiones de derecho procesal como la preservación expeditiva de los datos almacenados, la preservación expeditiva y divulgación parcial del tráfico de datos, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido. Además, el convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua (con consentimiento o disponibles al público) y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las partes colaboradoras.

El convenio es el resultado de años de trabajo de expertos europeos e internacionales. Se complementa con un protocolo adicional que realiza cualquier publicación de la propaganda racista y xenófoba a través de redes informáticas como una ofensa criminal. En la actualidad, el terrorismo cibernético también se estudia en el marco del convenio.

3.1.1.1 Países adscritos

Canadá, Japón, Estados Unidos y Sudáfrica.

3.1.1.2 Países por adherirse

El Salvador, Argentina, Uruguay, Chile y México.

3.2 Código penal federal

CAPÍTULO II
ACCESO ILICITO A LOS SISTEMAS Y EQUIPOS DE INFORMÁTICA

A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. **(Artículo 211 Bis).**

Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. **(Artículo 211 bis 1).**

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. **(Artículo 211 bis 1).**

Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. **(Artículo 211 bis 2).**

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. **(Artículo 211 bis 2).**

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. **(Artículo 211 bis 3).**

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. **(Artículo 211 bis 3).**

Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. **(Artículo 211 bis 4).**

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. **(Artículo 211 bis 5).**

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. **(Artículo 211 bis 5).**

Las penas previstas en este artículo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. **(Artículo 211 bis 5).**

Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este código. **(Artículo 211 bis 6)**.

Las penas previstas en este capítulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno. **(Artículo 211 bis 7).**

3.3 Código penal del estado de Chihuahua

TÍTULO VIGÉSIMO SEGUNDO
DELITOS CONTRA LA SEGURIDAD Y EL NORMAL FUNCIONAMIENTO DE LAS VÍAS DE COMUNICACIÓN Y DE LOS MEDIOS DE TRANSPORTE
CAPÍTULO IV
DEL USO Y ACCESO ILÍCITO A LOS SISTEMAS Y EQUIPOS INFORMÁTICOS Y DE COMUNICACIÓN
19 de Noviembre del 2011

A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrán de seis meses a dos años de prisión y de cien a mil días multa. (**Artículo 327).**
A quien revele, divulgue, utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le impondrán de tres a doce años de prisión y de doscientos a mil días multa. (**Artículo 327).**
A quien sin la debida autorización o excediendo la que tenga y con ánimo de lucro, en beneficio propio o de un tercero, acceda, copie, modifique, destruya, deteriore, intercepte, interfiera, o use, información contenida en equipos informáticos o de comunicación, se le impondrán de seis meses a tres años de prisión y de cien a cuatrocientos días multa. (**Artículo 327 Bis).**
Al que diseñe, programe, fabrique, introduzca, importe, comercialice o distribuya programas de cómputo, aparatos, sistemas, códigos de acceso, o cualquier dispositivo físico, que tengan por objeto violar uno o más mecanismos de seguridad de equipos informáticos, de comunicación, de programas de cómputo, en beneficio propio o de un tercero, se le impondrán de seis meses a cuatro años de prisión y de doscientos a quinientos días multa. (**Artículo 327 Ter).**
Al que valiéndose de equipos informáticos o de comunicación, utilice indebidamente, datos o información personal de otro para ostentarse como tal sin consentimiento de éste, ya sea en beneficio propio o de un tercero, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. **(Artículo 327 Quater).**
Las penas previstas en este Capítulo se incrementarán en una mitad cuando las conductas sean cometidas en contra de una entidad pública estatal o municipal. (**Artículo 327 Quinquies).**

3.4 Ley de protección de datos personales

La protección de datos personales se ubica dentro del campo de estudio del Derecho Informático. Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso. En algunos países la protección de datos encuentra reconocimiento constitucional, como derecho humano y en otro simplemente legal.

En México la LFPDPPP[9] define como dato personal a: cualquier información concerniente a una persona identificada o identificable. El pleno del instituto federal de acceso a la información pública, (con fundamento en lo dispuesto por los artículos 15, 16 y 37 fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 28 y 64 de su Reglamento) emitió los lineamientos generales para la clasificación y desclasificación de la información de las dependencias y entidades de la administración pública federal.
Cuando se trata de datos personales la información es clasificada confidencial tal como lo estipula en su artículo trigésimo segundo: Será confidencial la información que contenga datos personales de una persona física identificada o identificable relativos a:

Origen étnico o racial
Características físicas
Características morales
Características emocionales
Vida afectiva
Vida familiar
Domicilio particular
Número telefónico particular
Patrimonio
Ideología

[9] Ley Federal de protección de datos personales en posesión de particulares. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf 05/07/2010

Opinión política

Creencia o convicción religiosa

Creencia o convicción filosófica

Estado de salud física

Estado de salud mental

Preferencia sexual

Otras análogas que afecten su intimidad, como la información genética. Los datos personales serán confidenciales aun cuando no hayan sido obtenidos de su titular. También se consideran confidenciales los datos de una persona fallecida, los únicos que podrán tener acceso y derecho a corregirlos son el cónyuge y los familiares en línea recta ascendente o descendente sin limitación de grado, y en línea transversal hasta el segundo grado. Sólo en caso de que no existiera ningún familiar de los mencionados, los parientes en línea transversal hasta cuarto grado tendrán derecho a solicitar la corrección de datos.

En la actualidad muchas de las actividades humanas requieren información y diariamente las personas transmiten o intercambian algunos de sus datos personales, por lo que se hace necesario trabajar sobre la importancia que tiene para las personas el uso adecuado, obtención y transmisión de su información personal.

La protección de datos personales busca garantizar la privacidad de las personas, el resguardo o protección de su intimidad, lo cual supone la posibilidad real de controlar el uso y la finalidad para la cual se destina la información relativa a cada individuo y la facultad de oponerse a su utilización, impidiendo que esa información sirva a propósitos no aceptados por su titular.

3.5 Ley de comercio electrónico

El comercio electrónico es definido OCDE[10] como el proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación. Representa una gran variedad de posibilidades para adquirir bienes o servicios ofrecidos por proveedores en diversas partes del mundo.

[10] Organización para la cooperación y el desarrollo económico http://www.oecd.org/centrodemexico/laocde/ Año:2015

3.6 Directrices de la OCDE

PARTE PRIMERA

OBJETO:

Estas directrices se aplican solamente al comercio electrónico entre proveedores y consumidores y no a las transacciones entre proveedores.

PARTE SEGUNDA

Principios generales, protección efectiva y transparente:

Los consumidores que participen en el comercio electrónico deberán tener asegurada una protección efectiva y transparente de sus derechos, que no sea menor al nivel de protección que se les asegura en otras formas de comercio.

Los gobiernos, proveedores, consumidores y sus representantes trabajarán en forma conjunta para conseguir esa protección y determinar qué cambios serían necesarios para abarcar las especiales circunstancias del comercio electrónico.

3.7 Comercio, publicidad y prácticas de mercadeo honestas

- Los proveedores que utilicen el comercio electrónico deberán prestar especial atención a los intereses de los consumidores y actuar de acuerdo a un comercio, una publicidad y prácticas de marketing honestas.
- Los proveedores no realizarán ninguna manifestación, u omisión, o realizarán ninguna práctica que pueda ser falsa, engañosa, fraudulenta o abusiva.
- Los proveedores que vendan, promuevan o realicen marketing de bienes o servicios a los consumidores no realizarán prácticas que puedan causar un riesgo o daño irrazonable a los consumidores.
- Cuando los proveedores entreguen información sobre ellos mismos, o los bienes o servicios que proveen, deben presentar esa información de manera que sea clara, conspicua[11], certera y fácilmente accesible.
- Los proveedores deberán observar en cada manifestación que hagan las políticas o prácticas relacionadas con sus transacciones con los consumidores.

[11] Ilustre, famoso o sobresaliente http://www.wordreference.com/definicion/conspicuo Año:2015

- Los proveedores deben tener en cuenta la naturaleza global del comercio electrónico y, siempre que sea posible, deberán considerar las variadas características regulatorias de los mercados a que ellos apuntan.
- Los proveedores no explotarán las características especiales del comercio electrónico para ocultar su identidad o ubicación real, o para evitar cumplir con los estándares de protección del consumidor y/o los mecanismos de aplicación.
- Los proveedores no usarán términos contractuales abusivos.
- La publicidad y el marketing deberán ser claramente identificados como tales.
- La publicidad y el marketing identificarán al proveedor para el cual tales actividades e realizan, y la falta de tal identificación se considerará como engañosa.
- Los proveedores deberán ser capaces de probar cualquier manifestación expresa o tácita durante el tiempo que las mismas sean mantenidas, y por un período de tiempo razonable luego de ello.
- Los proveedores desarrollarán e implementarán procedimientos efectivos y fáciles de utilizar que permitan a los consumidores elegir si desean o no recibir mensajes comerciales a través del correo electrónico.
- Cuando los consumidores indiquen que o desean recibir mensajes comerciales a través del correo electrónico, esa elección debe ser respetada.
- En algunos países, el correo electrónico comercial no solicitado está sujeto a requerimientos legales o autorregulatorios.
- Los proveedores deberán tener especial cuidado en la publicidad y el marketing que está destinado a los menores, la tercera edad, los enfermos graves, y otros que no tengan la capacidad de entender plenamente la información que les es presentada.

3.8 Informaciones en línea, información sobre el proveedor

Los proveedores que trabajen con comercio electrónico deberán proveer a los consumidores de información clara, correcta y de fácil acceso sobre sí mismos, suficiente para permitir, como mínimo:

- La identificación del proveedor incluyendo el nombre legal del proveedor y el nombre bajo el cual desarrolla sus actividades comerciales; el domicilio principal del

proveedor; la dirección de correo electrónico u otra forma electrónica de contacto, o un número telefónico; y, cuando corresponda, un domicilio para fines de inscripción y cualquier número de inscripción o licencia otorgado por las autoridades;

- Una comunicación del consumidor con el proveedor que sea rápida, sencilla y efectiva;
- Un sistema de solución de conflictos que sea apropiado y efectivo;
- El procedimiento legal; y
- La ubicación del proveedor y sus funcionarios para conocimiento de los funcionarios reguladores y los encargados de control.
- Cuando el proveedor haga pública su pertenencia a algún esquema de autorregulación, una asociación de proveedores, una organización de resolución de conflictos u otro órgano de certificación, el proveedor deberá informar a los consumidores los detalles apropiados y un método sencillo para verificar tal pertenencia, y contar con un fácil acceso a las reglas y las prácticas de esos organismos.

CAPITULO CUARTO
4. PROTOCÓLO PARA LA CONFISCACIÓN DE PRUEBAS DIGITALES

4.1 Prepararse para confiscar pruebas digitales

Como investigador, deberá responder al lugar de los hechos e identificar, proteger y analizar correctamente las pruebas electrónicas una vez ocurrido el hecho. ¿Cómo se prepara para confiscar las pruebas? deberá hacer lo siguiente:

- Recolectar información
- Documentar todo
- Preparar una bolsa para confiscación

4.2 Recolectar información

Cuanta más información recolecte antes de la incautación, más preparado estará. Los testigos, las víctimas, los informantes, son excelentes fuentes de información.

Al entrevistar a las fuentes, formule preguntas tales como:

¿Quién es el dueño o encargado de los artículos que se decomisarán?
¿Qué grado de experiencia tiene con la informática?
¿Es usuario autorizado?
¿Qué tipos de artículos se decomisaran probablemente?
¿Una computadora o cinco?
¿Computadoras autónomas o en red?
¿Windows, Macintosh o Linux?
¿Dónde se encuentran los artículos que se decomisaran?
¿En una casa? ¿En una empresa?
¿Cuándo se realizará el operativo de decomiso?
¿Por qué se decomisaran los artículos en cuestión?
¿Cuáles son los hechos generales del caso?
¿Cómo se decomisaran los artículos?
¿Quién los decomisara?
¿Dónde se guardarán?

4.3 Documentar todo

Una regla de oro es "si no lo puso por escrito, no ocurrió". Documentar todo es crucial. Deberá documentar todos los pasos, desde el momento en que se entere del incidente. Use

formularios cuando corresponda. Si documenta todo con precisión y de manera oportuna, puede respaldar su testimonio. También le puede ayudar a recordar pequeños detalles.

4.4 Preparar una bolsa para decomisos

Deberá preparar la bolsa para decomisos, que utilizará para decomisar las pruebas. Las herramientas que necesite para recopilar las pruebas dependerán del tipo de pruebas que deba decomisar.

4.5 Tipos de pruebas digitales

Las pruebas digitales pueden clasificarse como volátiles o no volátiles. En general, las pruebas volátiles permanecen en la computadora de forma transitoria mientras que las no volátiles son más permanentes. Los datos almacenados en los discos duros, por ejemplo, son menos volátiles que los que son almacenados en la memoria física (RAM[12]).

Como primer respondiente, será el responsable de identificar y recolectar las pruebas informáticas volátiles y no volátiles, lo cual puede ser sencillo, como incautar una computadora, o difícil, como reconocer y recopilar datos cifrados con una computadora en funcionamiento.

Los esfuerzos por recopilar pruebas afectaran posiblemente, las pruebas almacenadas en el disco duro. Es probable que pierda hasta un 30% de las pruebas en la memoria en el simple.

4.6 Herramientas de respuesta a incidentes

Como primer respondiente, tal vez deba recopilar pruebas de un sistema de computadoras encendido. Esto puede incluir, entre otros, la memoria RAM, los datos volátiles del sistema e imágenes de archivos, carpetas o discos enteros.

4.7 Herramientas para recopilar pruebas

4.7.1 Win32dd de Mantthieu Suische

El programa Win32dd es una herramienta sumamente capaz y compatible para hacer imágenes de la memoria física. Almacena todo el contenido de la memoria RAM en un archivo de

---

[12] Random Access Memory http://definicion.de/ram/ Año: 2015

imagen binario que se puede analizar utilizando herramientas como EnCase,Volatily o FTK. Win32dd es parte de MoonSols Windows Memory Forensic Toolkit.

Existen dos versiones: La versión comunitaria, que es gratuita y la versión comercial. Win32dd puede hacer un volcado de la memoria RAM de todas las versiones de Windows, incluso las ediciones de 32 y 64 bits (utilizando Win6 de4dd).

4.8 Herramientas de respuestas a incidentes

Las herramientas de respuesta a incidentes son una serie de herramientas de línea de comandos de dominios públicos fabricadas por Microsoft y Sysinternals. Pueden utilizarse para recopilar información de una red y otros datos volátiles del sistema. Pueden ejecutarse de manera individual o colectiva como archivo de batch[13] de Windows.

4.9 CryptHunter de la Universidad Carnegie Mellon

CryptHunter es una herramienta para las fuerzas del orden que detecta el uso activo de cifrado. Detecta volúmenes cifrados montados pero no los que no están montados.

4.10 FTK imager Lite de Access Data

FTK Imager Lite crea imágenes forenses de archivos enteros, volúmenes, archivos, carpetas y física.

Todas estas herramientas pueden ejecutarse desde un disco duro con conexión USB[14]. Es preferible utilizar discos duros con conexión USB para almacenar las pruebas. Por ende, antes de usarlo el disco debe estar limpio. Un disco limpio desde el punto de vista forense debe borrarse antes de utilizarse para almacenar información, a fin de evitar contaminar las pruebas. Esto se logrará utilizando el programa de dominio público Eraser.

---

[13] Se conoce como sistema por lotes (en inglés batch processing), o modo batch, a la ejecución de un programa sin el control o supervisión directa del usuario (que se denomina procesamiento interactivo). http://diccionario.reverso.net/ingles-espanol/batch Año: 2015

[14] El Bus Universal en Serie (BUS) (en inglés: Universal Serial Bus), más conocido por la sigla USB, es un bus estándar industrial que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras, periféricos y dispositivos electrónicos .http://definicion.de/usb/ Año:2015

4.11 Documentar la integridad de las herramientas

Documentar las herramientas es un componente crucial para presentar evidencias ante un juez. Calculando en valor HASH [15]de cada herramienta tres veces:

Antes de copiarlo al disco USB,
después de copiarlos al disco USB y
después de usarlo en el campo.

El proceso HASH produce una representación alfanumérica estadísticamente singular (es decir, el valor HASH) del contenido del archivo. Una vez que el archivo cuente con un valor HASH es fácil identificar si ha sido modificado. Incluso los cambios más pequeños, por ejemplo una palabra nueva o un espacio adicional, cambian todo el valor HASH.

Por lo tanto, se puede utilizar este valor para verificar que no se hayan cambiado los archivos, es importante destacar que el nombre del archivo no es un factor para el cálculo del valor el mismo siempre que no se haya modificados su contenido.

4.12 Armar otras herramientas para recopilar pruebas

Además de recopilar pruebas de un sistema de computadoras encendido, también deberá recopilar datos no volátiles y otras pruebas tradicionales como discos, memorias portátiles, manuales, papel escrito, armas, etc.

Este proceso suele denominarse embalaje y rotulación de pruebas. Para completar la bolsa de decomisos, se necesita: cámara, pila de repuesto, vídeo, libretas para notas y bosquejos, medios de almacenamiento masivos, cintas para pruebas, etiquetas, plumas y marcadores, recipiente para almacenamiento, bolsas antiestáticas, juego de herramientas, guantes de goma, pulseras antiestáticas, formularios de la cadena de custodia y cualquier otro que corresponda.

4.13 Responsabilidades del investigador principal

El investigador principal, o jefe de equipo, tiene numerosas responsabilidades en el lugar de los hechos. Primero, debe recolectar la mayor cantidad posible de información sobre el lugar o la persona que requisara esto con la finalidad de formular un plan adecuado. Luego, debe conformar un equipo calificado para identificar y recolectar las pruebas electrónicas.

---

[15] A las funciones HASH (adopción más o menos directa del término inglés hash function) también se les llama funciones picadillo, funciones resumen o funciones de digest.
https://es.wikipedia.org/wiki/Funci%C3%B3n_hash Año:2015

Los protocolos para preservar la integridad de las pruebas comienzan a entrar en vigencia antes de que los investigadores lleguen al lugar de los hechos.

4.14 Logística de la requisa

Recolectar información sobre el lugar de los hechos, cerciorándose de contemplar lo siguiente: distribución del lugar. ¿Cuál es la distribución del lugar que se requisara?, ¿Cuál es la mejor forma de acercarse al lugar sin ser detectados?, ¿Cuáles son las posibles vías de escape?, ¿Hay alguna estructura cercana que podría representar riesgos para la seguridad o contener pruebas?

4.15 Potencial de que los ocupantes ofrezcan resistencia

No suponga que las personas que las personas que se encuentran en lugar no representan una posible amenaza física para los que ejecuten la orden judicial por el solo hecho de que las computadoras son el motivo de la requisa. Cerciórese de identificar todas las amenazas potenciales antes de proceder a la requisa.

4.16 Diseño de la red informática

¿Prevé encontrar una computadora o varias?
¿Estarán conectadas a la red?
¿Alguna es un servidor para usuarios externos?

4.17 Potencial de requisas adicionales

¿Es probable que las computadoras estén conectadas a una red remota?

4.18 Manejo del equipo de requisa

El investigador principal es el responsable de informarle a todo el equipo el tipo de requisa que tendrá lugar, identificar y asignar funciones y cerciorase de que todo el equipo comprenda sus funciones y responsabilidad. El investigador principal debe marcar pautas claras en cuanto a lo que el equipo puede y no puede hacer.

El equipo debe comprender el alcance de la requisa, que puede incautar y que no, así como donde requisar y donde no. Los integrantes del equipo que van más allá de alcance de la requisa o su capacidad de realizarla suelen pasar por alto pruebas o recolectarlas de manera incorrecta.

4.19 Funciones del equipo de requisa:

- **4.19.1 Control de ocupantes:** Mantener el control de todos los ocupantes.
- **4.19.2 Seguridad del lugar:** Impedir acceso no autorizado al lugar.
- **4.19.3 Equipo de requisa:** Realizar requisas.
- **4.19.4 Custodia de las pruebas:** Custodiar y documentar todos los artículos confiscados.
- **4.19.5 Equipo de entrevistas:** Entrevistar a todos los ocupantes pertinentes.
- **4.19.6 Documentación del lugar:** Documentar el lugar antes y después de la requisa.

Proteger el lugar de los hechos, la seguridad de los cuerpos de seguridad es la inquietud principal de todos los que participan de la requisa. El jefe del equipo debe asignar oficiales puntuales a las funciones de: ingresar y proteger el lugar de los hechos; un equipo de oficiales o equipo de respuesta especial suele desempeñar esta función, el trabajo del equipo consiste en ser los primeros en ingresar y protege el lugar de los hechos. La estructura del equipo y los métodos empleados para ingresar al lugar variarán de una investigación a otra. Por ejemplo, el equipo seleccionado para proteger una casa de seguridad será distinto al equipo elegido para proteger un banco cuyas computadoras están comprometidas.

4.20 Proteger a los ocupantes

El equipo de ingreso realiza esta tarea inicial. El equipo de ingreso puede o no estar conformado por los mismos oficiales encargados de mantener la custodia de los ocupantes mientras se realiza la requisa.

4.21 Mantener la seguridad perimetral

Las personas asignadas a esta función deben estar correctamente informados y comprender las limitaciones de esta función. Su función consiste en cerciorarse de que ninguna persona no autorizada ingrese al lugar de los hechos. Su trabajo no es buscar pruebas.

4.22 Cerciorarse de que no se alteren las pruebas

Una persona será la responsable máxima de asumir la custodia de las pruebas. Sin embargo, es responsabilidad del jefe de equipo cerciorarse de que esta persona cuente con la ayuda que necesite y que se apliquen y mantengan todos los elementos de seguridad a fin de garantizar la integridad del proceso de recolección de pruebas

4.23 Fotografiar el lugar de los hechos

Una vez que el equipo de ingreso y el jefe de equipo declaran que el lugar de los hechos está protegido, el o los responsables de documentarlo, deben comenzar de inmediato a fotografiar, filmar o trazar bosquejos del lugar de los hechos. El motivo principal por el que se documenta el lugar antes de la requisa es para captar la ubicación exacta de los artículos en caso de que se muevan o documenten erróneamente en el proceso de requisa.

4.24 Hacer un bosquejo del lugar de los hechos

Al hacer un bosquejo del lugar de los hechos, rotule sistemáticamente todos los ambientes para poder hacer referencia a ellos en toda la documentación correspondiente. Por ejemplo, si desea describir el lugar donde encontró el primer artículo de prueba, puede decir: "El articulo #1 fue hallado en la habitación X. Al hacer el bosquejo, cerciórese de indicar donde se encontraban los ocupantes cuando el equipo de ingreso los halló. Esto es útil para mostrar la custodia y el control de los artículos incautados posteriormente.

4.25 Documentación escrita

Es útil usar formularios para documentar el lugar donde se encontró un artículo, quien lo encontró, y documentar la cadena de custodia. Los informes posteriores son útiles para describir cómo se realizaron los ingresos y la requisa, así como la función que desempeño cada uno de los integrantes del equipo.

4.26 Entrevistas in situ

En algún momento durante la requisa, se recomienda entrevistar a los ocupantes (si se permite). Según las circunstancias, el objeto principal, es obtener una declaración de si el ocupante tenía la custodia y el control de los equipos decomisados. No formule preguntas donde la respuesta sea un sí o un no.

4.27 Incautar una computadora (encendida)

Si la computadora está encendida, recuerde el orden de volatilidad. Proceda a la incautación en el siguiente orden: tome una foto de la pantalla, recolecte los datos de la memoria RAM, recopile los datos volátiles, desactive la conexión a la red para impedir el acceso remoto, si hay cifrado, recolectar las copias lógicas, desconéctela, incaute y embale todas las pruebas.

4.28 Incautar una computadora (apagada)

No la encienda, fotografíela de todos los ángulos, desconecte y rotule todas las conexiones, inspeccionar los medios removibles.

Antes de embalar la computadora, verifique si tiene un CD[16] o DVD[17] insertando. Además de poder llegar a perder parte de una prueba, transportar la computadora con el disco adentro puede dañarlo.

4.29 Confirmar que tenga disco duro

Finalmente, quite la caja y verifique si está el disco duro. Generalmente remueven el disco duro y lo esconden en otro lado.

Si encuentra el disco duro, tome nota de marca, modelo y número de serie. Si es un disco duro IDE[18], tome nota de la configuración del puente de conexión. Un disco esclavo sin el maestro es indicio de que el maestro está escondido en otro lugar.

4.30 Dispositivos electrónicos

Es probable que los primeros respondientes se topen con una amplia gama de dispositivos de almacenamiento de datos de toda forma y tamaño. Los reproductores de medios portátiles, como iPods[19] y otros tales como teléfonos, GPS[20] y vídeo juegos pueden contener pruebas electrónicas.

Es probable que las máquinas de fax, las impresoras, los teléfonos y otros dispositivos de comunicación contengan registros, datos de las llamadas en incluso archivos.

En el lugar de los hechos también puede haber dispositivos atípicos, tales como lectores de tarjetas de crédito (skimmers).[21]

---

16 Compac Disc http://www.significado-s.com/e/cd/ Año:2015

17 Disco Versátil Digital http://www.significados.com/dvd/ Año:2015

18 Integrated Device Electronic http://www.informaticamoderna.com/Disco_duro_IDE.htm#defin Año:2015

19 Intelligence Portable Device http://www.cusiglas.com/significadode/ipod.php Año:2015

20 Global Positioning System http://www.euroresidentes.com/gps/que-es-el-gps.htm Año:2015

21 Herramienta utilizada por los delincuentes para clonar tarjetas http://www.welivesecurity.com/la-es/2015/04/06/que-es-skimmer-como-proteger-tarjeta/ 6/04/2015

4.31 Requisa de la escena del delito

Al buscar las pruebas tómese su tiempo. Si bien las computadoras y los dispositivos de comunicación son relativamente fáciles de reconocer, los dispositivos con conexión USB [22]pueden tener prácticamente cualquier aspecto.

No suponga que las pruebas electrónicas estarán en las inmediaciones de la computadora. Con frecuencia, los discos duros y otros dispositivos de almacenamiento se encuentran escondidos alejados de la computadora.

No olvide buscar disquetes, CD's y DVD's. Los examinadores forenses pueden necesitar los discos para instalar el software informático a fin de examinar la computadora. Sin embargo, no suponga que los rótulos son los correctos. Lo que puede aparentar ser una película puede resultar ser un disco de datos. De la misma manera, un disco que aparente ser el de la instalación puede resultar contener pruebas.

4.32 Incautación de pruebas no electrónicas

Además de incautar los dispositivos de almacenamiento electrónico, deberán incautar otros artículos que puedan contener pruebas. Artículos como apuntes manuscritos, libros revistas, casetes de audio y de vídeo, fotos y diagramas pueden contener pruebas relativas al delito.
Se recomienda incautar los accesorios de la computadora, como: el monitor, teclado y mouse. Si bien en estos no se almacenan datos, pueden contener las huellas digitales del sospechoso.

4.33 Embajale de pruebas electrónicas

Cerciórese de que todas las pruebas estén adecuadamente documentadas, embaladas y rotuladas antes de retirarlas del lugar de los hechos. Al embalar los dispositivos de almacenamiento electrónico, utilice bolsas antiestáticas para impedir que se dañe por descargas de electricidad estática.
A fin de ayudar a prevenir encender accidentalmente la computadora, inserte un disco virgen en la unidad del disquete y coloque cinta para pruebas sobre las ranuras de los discos de conexión de electricidad.

---

[22] Universal Serial Bus/ Bus Universal en Serie http://definicion.de/usb/ Año:2015

4.34 Transporte de pruebas electrónicas

Al transportar pruebas electrónicas, tenga cuidado de aislar las pruebas del calor y la humedad extremos, ya que, ambos pueden dañar el dispositivo. No use polietileno extraído para proteger las pruebas electrónicas. Genera electricidad estática. Use envoltura de plástico de burbujas si las hay.

Si bien algunas fuentes de calor y humedad pueden ser evidentes, también se deben tener presentes las fuentes magnéticas. Por lo tanto, es importante recopilar las pruebas de manera tal que minimice el impacto en la mayoría de los datos volátiles.

CAPITULO QUINTO
5. CRÍMENES Y EVIDENCIA POTENCIAL

Los siguientes crímenes pueden involucrar el uso de una computadora o de otro medio electrónico, la lista de a continuación pueden ser evidencia potencial que deberá ser recuperada.

5.1 Fraude

Datos de la cuenta de donde se hizo la transacción (defraudador)

Lista de direcciones

Conversaciones vía chat

Información del cliente

Datos de la tarjeta de crédito

Registros

5.2 Pornografía infantil y abuso infantil

Conversaciones

Software de la cámara digital

e-mails

Juegos

Software de edición

Clasificación de imágenes

Imágenes

Logs [23]de la actividad en Internet

Archivos de video

Nombres de archivos y directorios

5.3 Investigaciones para la intrusión a redes

Direcciones

Archivos de configuración

e-mail, notas, cartas

---

[23] Registro/bitácora en español Traducción de autor

Ejecutables

Actividad en internet, logs, nombres de usuarios y password[24]

Malware

Caché información

Internet Protocol Address (IP)

Historial de conexión

Conversaciones vía chat

Random Access Memory (RAM)

Conexiones a red

5.4 Investigaciones por homicidios

Lista de direcciones

Registros médicos

Historial de Internet

Registros telefónicos

Diarios

Mapas

Fotos víctimas y sospechoso

e-mail, notas, cartas

Registros Financieros

5.5 Investigaciones sobre violencia domestica

Lista de direcciones

Historial de Internet

Registros telefónicos

Diarios

e-mail, notas y cartas

Registros financieros

5.6 Fraudes financieros y falsificación

---

[24] Clave, contraseña. Traducción del autor.

Direcciones

Calendarios

Imágenes

Imágenes de transacciones

Información de los clientes

Bases de datos

e-mails, notas y cartas

Identificaciones falsas

Registros y financieros

Imágenes de firmas

Registros de logs con bancos

Números de tarjetas de crédito

5.7 Amenazas y acoso

Direcciones

Diarios

Imágenes

e-mails, notas y cartas

Estados financieros

Documentos legales

Mapas de la localización de la víctima

Identificaciones falsas

5.8 Investigaciones sobre narcotráfico

Direcciones

Calendarios

Bases de datos

Recibos de drogas

e-mails, notas y cartas

Identificaciones falsas

Registros financieros

Logs de actividad en Internet

Imágenes de drogas

5.9 Investigaciones sobre piratería

Logs de chats

Torrents[25]

Chats de audio y video

e-mails, notas y letras

Fotos y certificados de software

Software con copyright

Seriales de software

Archivos compartidos y sitios web

Software para crackeo[26]

Directorios de usuarios y nombres de archivos

5.10 Investigaciones de suplantación de identidad

Herramientas de software[27]

Transacciones con tarjetas de crédito

Software para escaneo

Documentos borrados

Ordenes on-line

Logs o historial en Internet

Certificados de regalos

Certificados de regalos

Malware[28] o troyanos[29] instalados

---

[25] Es un pequeño archivo con extensión ".torrent". Este archivo contiene la dirección de un "servidor de búsqueda" encargado de localizar posibles fuentes con el archivo o parte de él. Los archivos se descargan por partes, en secuencias aleatorias, directamente desde las computadoras que tienen dichas partes. De esa forma se reduce la carga en el servidor, ya que los usuarios intercambian los archivos entre ellos, no con el servidor. https://es.wikipedia.org/wiki/Archivo_Torrent Año:2015

[26] Es un parche cuya finalidad es la de modificar el comportamiento del software original y creado sin autorización del desarrollador del programa. https://es.wikipedia.org/wiki/Crack_inform%C3%A1tico Año:2015

[27] Rutinas que le permiten a la computadora realizar ciertas tareas http://definicion.de/software/ Año: 2015

[28] Software malicioso http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=193#queEs Año_2015

CAPITULO SEXTO

6. FORMULARIOS PROPUESTOS PARA LA RECOLECCIÓN DE DATOS INFORMÁTICOS EN RESPUESTA A UN INCIDENTE

6.1 Formulario para la tomar apuntes de investigación en respuesta a un incidente:

Este formato documentar en relación al incidente. Permite llevar un orden por tiempo y su descripción correspondiente.

Formulario para tomar apuntes de la investigación en respuesta a un incidente

FECHA:	ORGANISMO:	AGENTE:	LUGAR:
Hora	Descripción de actividades y resultados		

Página ________ de ________

[29] Software malicioso que se presenta al usuario como legítimo http://www.seguridadpc.net/troyanos.htm Año:2015

6.2 Formulario de recolección de datos informáticos en respuesta a un incidente

Este formulario permitirá llevar un registro de las características de los equipos confiscados durante un cateo.

Formulario de recolección de datos informáticos en respuesta a un incidente

FECHA:	HORA:	ORGANISMO:
Nombre del examinador o examinadores:		
Contacto:	Lugar:	
Modalidad de recepción de las pruebas (por ej., entregadas, decomisadas, recibidas en el intercambio de pruebas)		
Información sobre el sistema		
Fabricante del sistema:		
Número de serie del sistema:		
Nombre del sistema:		
Nro. de modelo del sistema:		
Número de pieza del sistema:		
Fecha y hora del sistema:		
Otros datos de identificación (por ej., daños, etiqueta, etc.):		
Procesadores:		
Memoria:		
Tarjeta de video:		
Tarjeta de sonido:		
Tarjeta de red:		
Tarjeta SCSI:		
Modem:		
Teclado:		
Monitor:		
Mouse:		
Unidad/es de disquete:		
Unidad/es de CD ROM:		
Unidad/es de DVD:		
Impresora/s:		
Otras tarjetas:		
Otras unidades:		
Información sobre el disco duro		
Fabricante:		
Número de serie:		
Número de la pieza:		
Tamaño del disco duro:		

Formulario de recolección de datos informáticos en respuesta a un incidente

FECHA:	HORA:	ORGANISMO:
Nombre del examinador o examinadores:		
Contacto:	Lugar:	

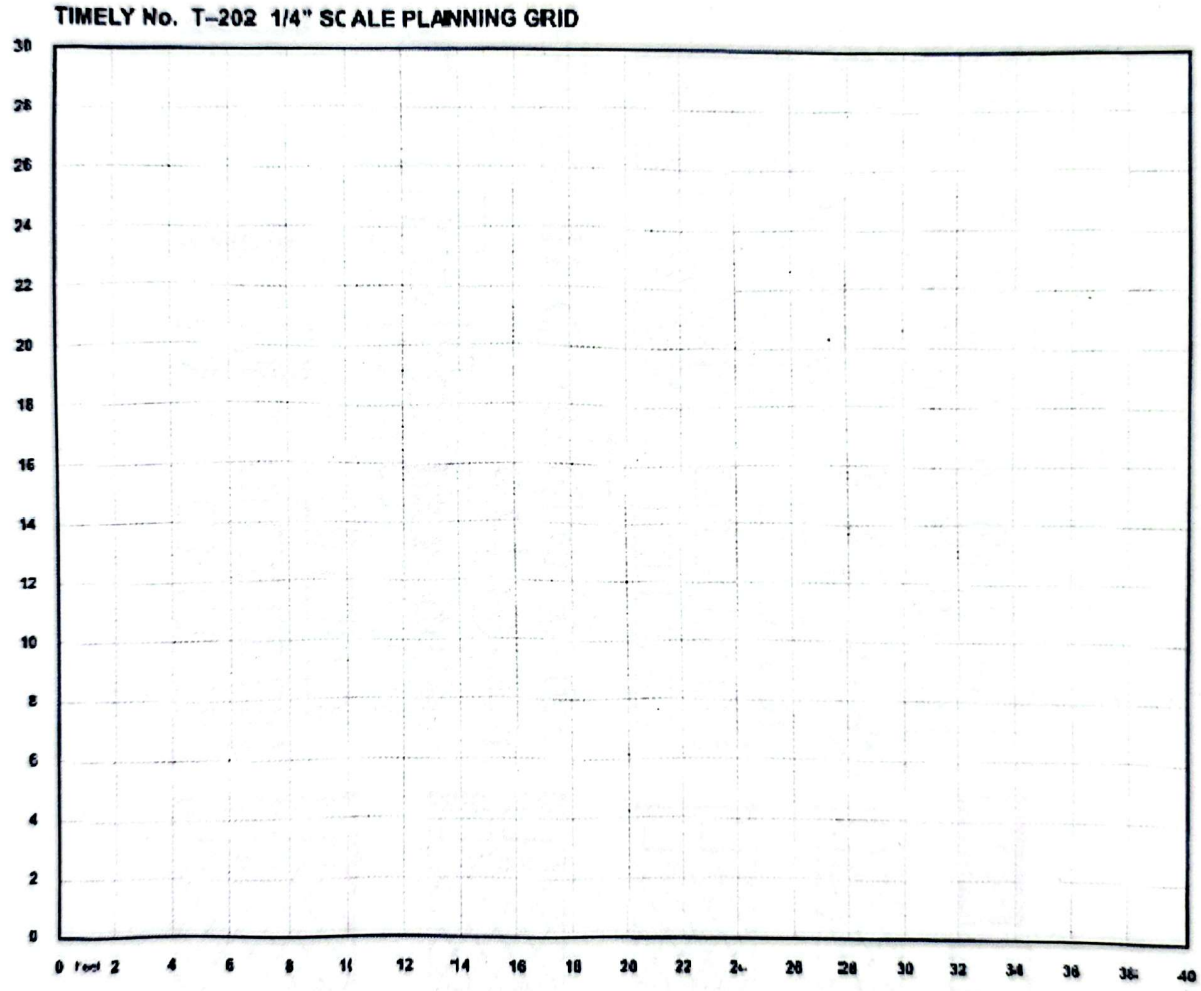
Modalidad de recepción de las pruebas (por ej., entregadas, decomisadas, recibidas en el intercambio de pruebas)

Información sobre el sistema	
Fabricante del sistema:	
Número de serie del sistema:	
Nombre del sistema:	
Nro. de modelo del sistema:	
Número de pieza del sistema:	
Fecha y hora del sistema:	
Otros datos de identificación (por ej., daños, etiqueta, etc.):	
Procesadores:	
Memoria:	
Tarjeta de video:	
Tarjeta de sonido:	
Tarjeta de red:	
Tarjeta SCSI:	
Modem:	
Teclado:	
Monitor:	
Mouse:	
Unidad/es de disquete:	
Unidad/es de CD-ROM:	
Unidad/es de DVD:	
Impresora/s:	
Otras tarjetas:	
Otras unidades:	

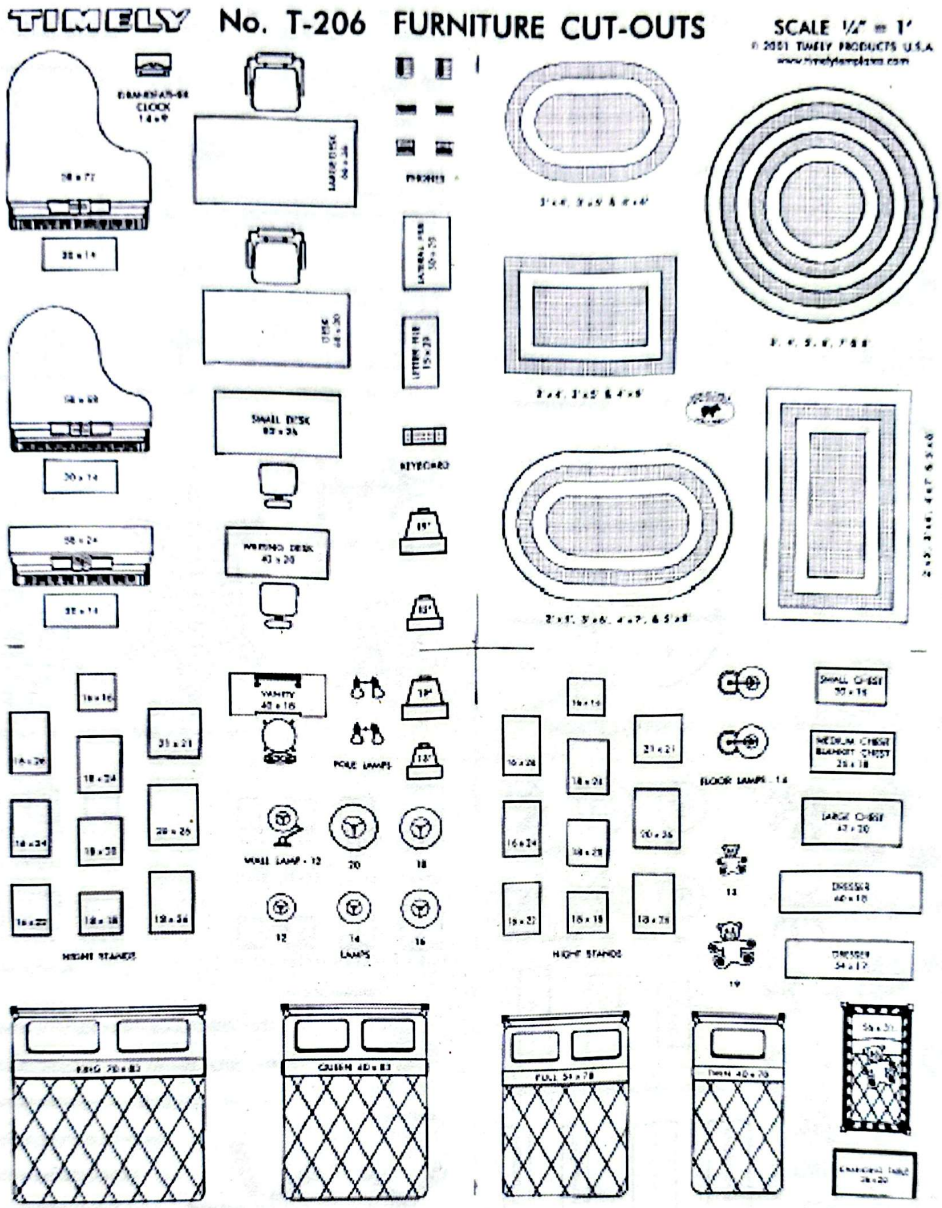
Información sobre el disco duro	
Fabricante:	
Número de serie:	
Número de la pieza:	
Tamaño del disco duro:	

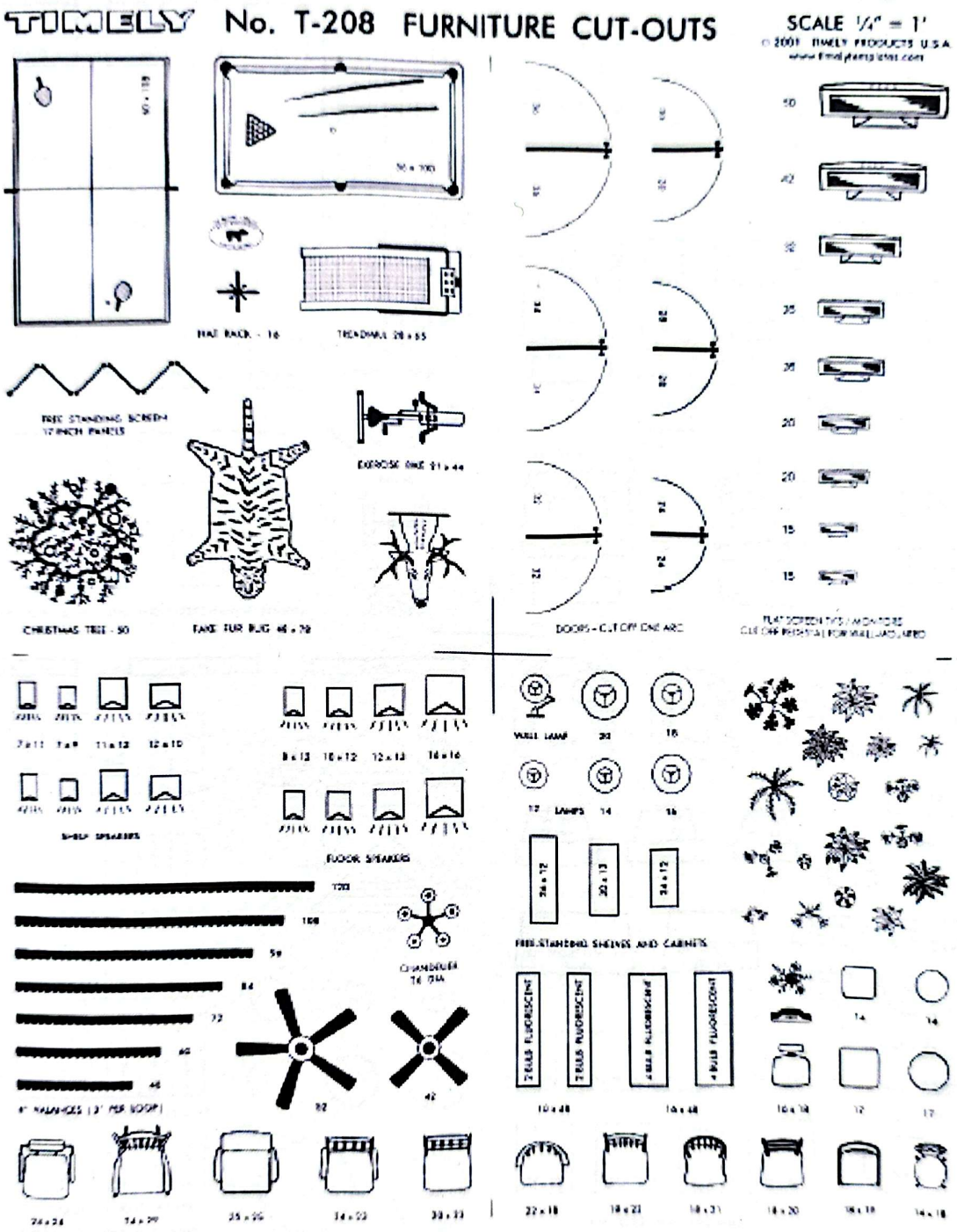
6.3 Uso de mapas para la distribución del lugar

Este formato crea un bosquejo a escala del lugar en el cual se llevar a cabo la requisa, apoya en la salvaguarda del equipo esto en cuanto a la ubicación de puertas, ventanas, sótanos etc. Mantiene un control de los posibles ocupantes.



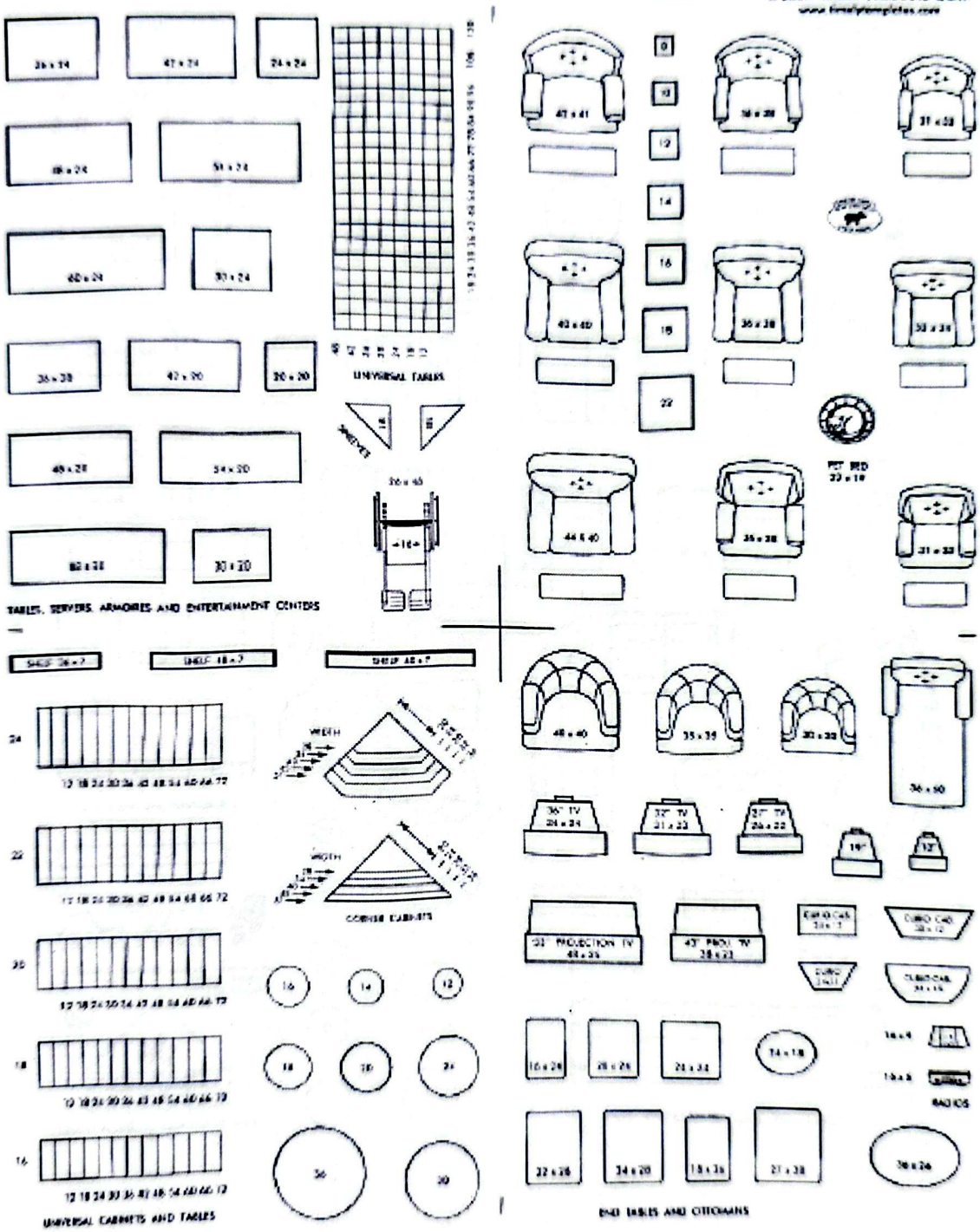
6.3.1 Tipos de muebles que se pueden integrar al mapa a la distribución del lugar





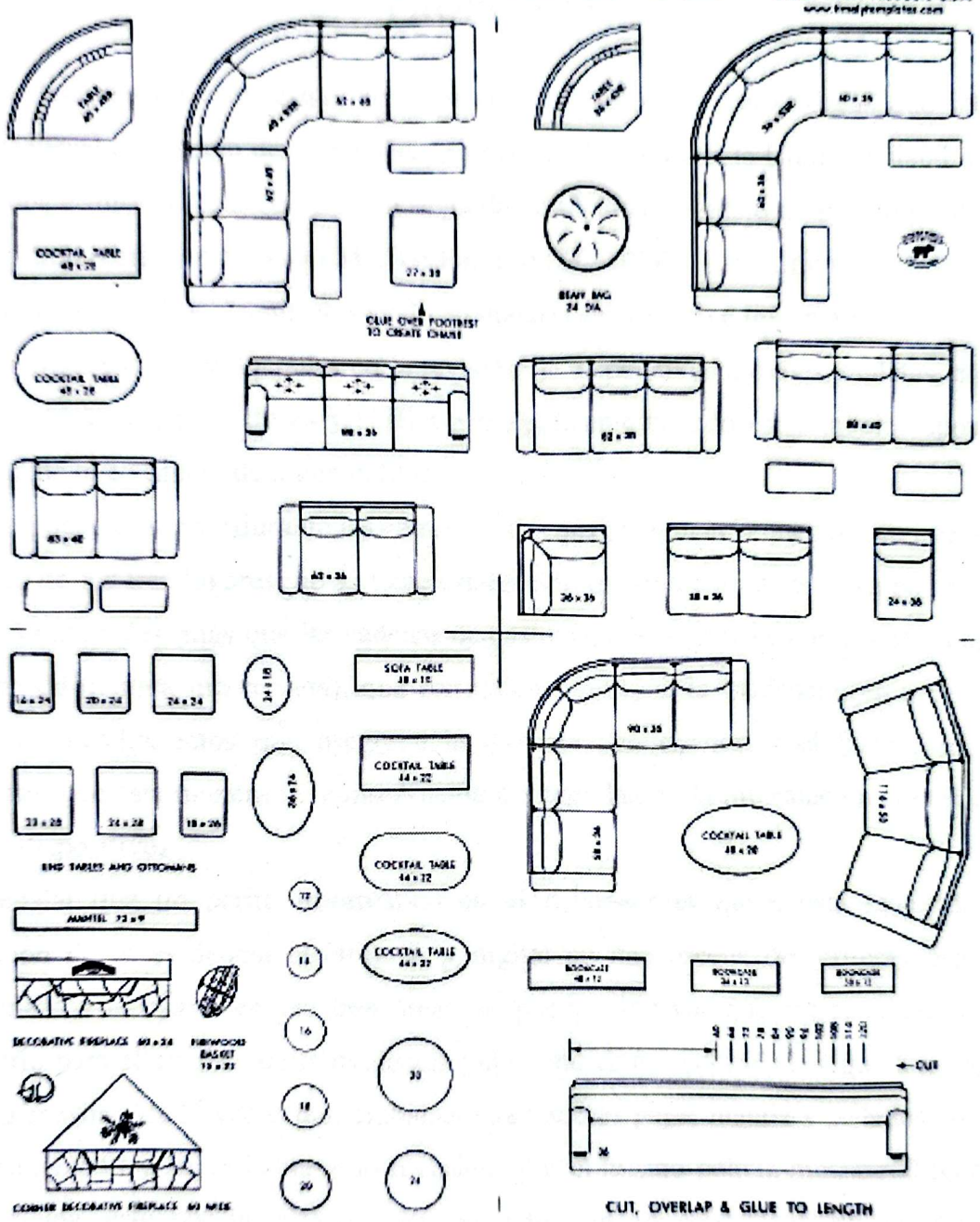
TIMELY No. T-205 FURNITURE CUT-OUTS

SCALE ¼" = 1'



TIMELY No. T-204 FURNITURE CUT-OUTS

SCALE ¼" = 1'



PROPUESTA

Para la realización de esta tesina, se tuvieron entrevistas con varias áreas que integran la Fiscalía General del estado de Chihuahua, en primer término con la Unidad Estatal de Delitos Electrónicos e Informáticos (UDEI), en segunda con Unidad Modelo de Investigación Policial (UMIP) y en tercero con Servicio Médico Forense (SEMEFO). Esta última con los dos peritos informáticos con los que cuenta el Estado en materia electrónica e informática.

Estas tres áreas están involucradas en la revisión de dispositivos móviles, tabletas, equipos de cómputo, cámaras, discos duros y USB´s principalmente cuando estos medios apoyan en la resolución de la comisión de algún delito.

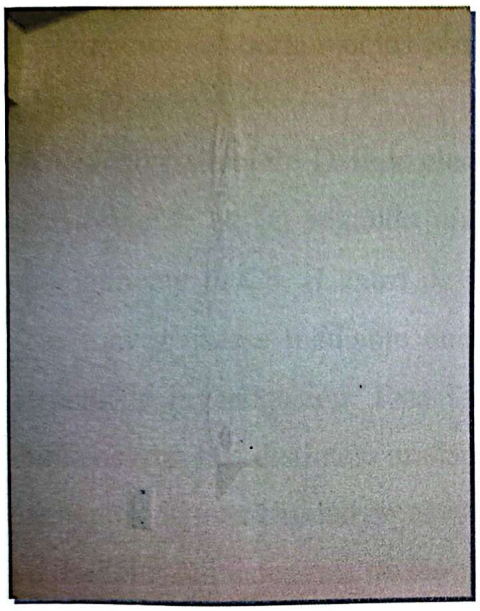
Lo que se puedo observar durante las entrevistas es que la evidencia que reciben puede llegar a cualquiera de los tres lugares, no se tiene establecido un protocolo de entrega por parte de los Policia Ministeriales (más que las cadenas de custodia, que en muchos de los casos el registro está lleno de manera incompleta), que son quienes recogen la evidencia, en muchos de los casos sin procedimientos que aseguren la correcta confiscación y el buen manejo de la demostrando de esta manera la conservación e integridad de la información contenida en los distintos dispositivos.

Cabe señalar que un perito informático en el deber-ser es quien está facultado para la recolección de la evidencia electrónica y digital en una escena del crimen, esto por sus conocimientos técnicos, en las tres áreas se puedo observar que ninguna cuenta con un laboratorio para el análisis de la evidencia bajo condiciones controladas, que los dispositivos llegan la mayoría de la veces mal embalados (en sobres papel manila y sellados con tape) y que posiblemente pueden haber sido revisados por el mismo policía ministerial (conectados) en su oficina, esto por la falta de conocimiento. Sin ser conscientes de que este tipo de disposición puede invalidar una prueba ante un juez en un tribunal por un mal manejo de la misma.

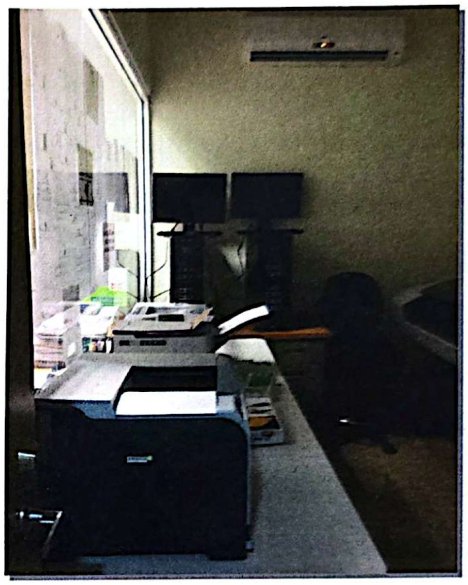
El 24 de noviembre del 2015 se hizo una visita a Unidad Modelo de Investigación Policial (UMIP), ubicada en el complejo estatal de seguridad en un primer piso, al entrevistar al encargado nos comenta que desde que él está en funciones del puesto la evidencia analizada ha sido regresada después de analizada a las Unidades correspondientes (víctimas, si aplica)

Está área se ha visto afectada por filtraciones de agua en la oficinas ya que las fugas de agua constantes de los baños ubicados en el segundo piso, oficinas utilizadas por personal del área de plataforma México y la Unidad Estatal de Delitos Electrónicos e Informáticos.

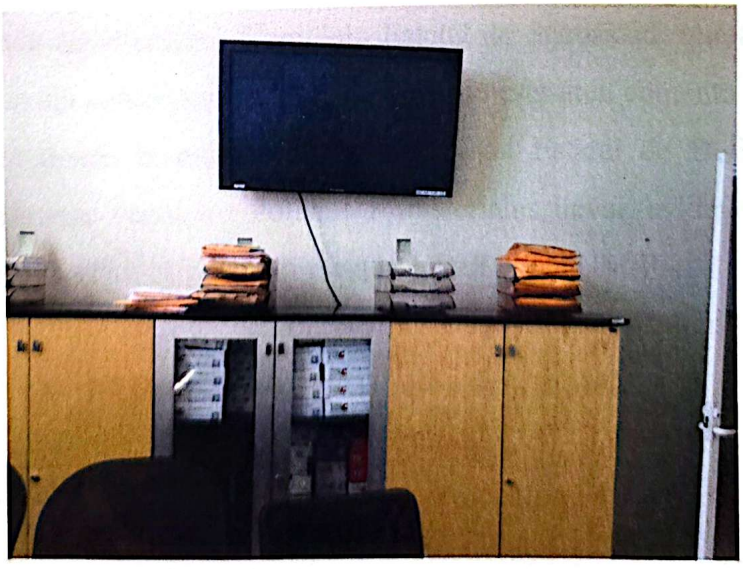
Los analistas comentan que esta área ha sido la más afectada ya que durante el primer incidente varias equipos tanto de la UMIP así como evidencia sufrieron daños.



Captura de la filtración en uno de los lugares de los analistas por parte de la UMIP



Lugar donde se tienen ubicados los equipos para realizar extracciones forenses en la UMIP



Evidencia por entregar de los distintos casos atendidos

Cabe señalar que la UMIP ha hecho un gran trabajo en cuanto al orden que manejan en el área evidencia de casos anteriores que se ha quedado en el olvido ha sido devuelta después de muchos años a las Unidades correspondientes.

Esta área recibe la evidencia sin asegurar que su confiscación haya sido la adecuada, esto cuando la misma es incautada por alguien que no pertenece a esta misma área. No cuenta con un laboratorio de análisis forense, los analistas trabajan en sus lugares compartiendo tanto el equipo como las herramientas con las que disponen.

La Unidad Estatal de Delitos electrónicos e Informáticos, está ubicada como ya se mencionó anteriormente en un segundo piso, en el mismo Complejo Estatal de Seguridad donde era antiguamente el C3, (Centro de Control de Confianza) de igual manera recibe equipos que necesitan revisarse mediante una cadena de custodia, teléfonos y que pertenecen a alguna carpeta de investigación. Esta Unidad al igual que la UMIP colabora con los Ministerios Públicos de las distintas unidades en la investigación de distintos tipos de casos. Los elementos de esta Unidad no acuden a las escenas del crimen, la confiscación queda a cargo de los Policías Ministeriales de las distintas Unidades, cabe señalar que no en todos los casos la confiscación se hace de manera correcta, por lo que la evidencia puede llegar comprometida. La falta de conocimiento de los Ministerios Públicos, Defensores, Jueces y víctimas, permite a la fecha que dichas pruebas no sean invalidadas ante un tribunal.

La SEMEFO, ubicada en el mismo Complejo Estatal de Seguridad, quienes cuentan con un documento que los avala como peritos, el encargado de esta área comenta que su actividad se ha visto disminuida desde la existencia de la Unidad Estatal de Delitos Electrónicos e Informáticos, que algunas veces los Policías Ministeriales llevan evidencia a revisión, pero como puede llegar a sus oficinas puede llegar a la UDEI o a la UMIP.

Antes ellos analizaban los mensajes de voz, pero esta actividad se vio absorbida por el área de antisecuestros. Solo una vez han acudido a una escena del crimen.

Bajo estos antecedentes es necesario que exista un protocolo general para quienes asistan a las escenas del crimen y confisquen la evidencia electrónica y digital (se deben revisar las funciones de las tres áreas y coordinar tanto los esfuerzos como los conocimientos y que la

evidencia resulte fehaciente y concluyente cuando se presente por tener un buen tratamiento y análisis).

Se ve como una necesidad inmediata establecer procedimientos y formularios de confiscación, así como la completitud del llenado de las cadenas de custodia. Así mismo contar con material y equipo adecuado para la confiscación así como un laboratorio donde dicha evidencia se trabaje bajo condiciones controladas para que su aceptabilidad no sea rechazada en ningún momento ante el tribunal correspondiente.

El próximo año la Unidad Estatal de Delitos Electrónicos e Informáticos tiene como proyecto visitar la fiscalía de todas las zonas con la finalidad de proporcionarles un protocolo de actuación en relación a este tipo de delitos, donde los Ministerios Públicos y Policías Ministeriales tengan un protocolo formal de actuación y la evidencia sea manejada con el debido tratamiento.

Es necesario la implementación de un Laboratorio para el análisis de la evidencia digital en el mismo complejo estatal de seguridad y que la evidencia sea resguardada (por contar con el lugar disponible) en el SEMEFO. Las instalaciones deben garantizar la integridad y la seguridad de la evidencia, es por esto que contará con medidas de seguridad que permitan el acceso solo a personal autorizado, para definir.

Es conveniente un acceso por huella dactilar y que cuente con un sistema de video por circuito cerrado, que grabe todos los acontecimientos en el laboratorio, de la misma manera un sistema de alarma de sensor por movimientos, todo el personal deberá de portal credencial visible y no se aceptaran visitas al mismo, si en un caso especial se requiere el ingreso de un tercero, esto deberá ser autorizado por el supervisor del laboratorio.

El Laboratorio deberá contar con las condiciones ambientales ideales, eléctricas, de temperatura, iluminación, ventilación y humedad. Un Laboratorio de ciencias forenses debe estar preparado para el peor de los casos, puesto que se manejan dispositivos, eléctricos y electrónicos.

- Esterilidad Biológica: Limpiar la superficie de trabajo con cloro
- Interferencia electromagnética: Utilizar una caja Faraday
- Suministro Eléctrico: Instalación de un suministro eléctrico y UPS
- Ruido y vibración: Instalación de materiales aislantes para evitar la propagación del ruido y la vibración.

El sistema de climatización, e instalación de filtros evita el paso de polvo, la humedad y el sobrecalentamiento y deterioro de los equipos de cómputo que se usará en las distintas etapas del análisis de la evidencia., de la misma manera deberán estar ubicados en lugares estratégicos extintores.

Al interior del Laboratorio es necesario, contar con cableado de red, internet, cableado telefónico, generado eléctrico y UPS, que el laboratorio de ser posible no tenga ventanas.

El Laboratorio estará dividió en tres secciones, área de control de acceso y entrada, almacenamiento, mecánica y análisis.

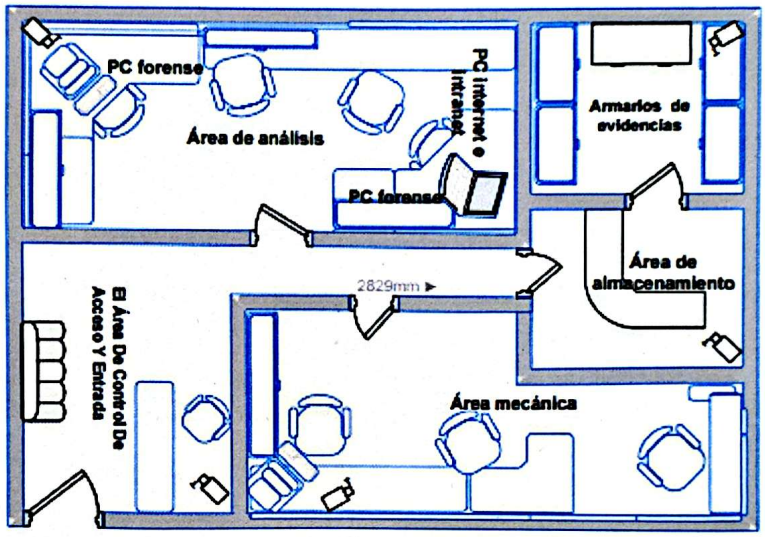


Imagen 1: Propuesta de la distribución del Laboratorio para el análisis de evidencia digital

El área de control y acceso es donde se recibirá la evidencia por parte de las distintas Unidades que integren una cadena de custodia, se mantendrá un control del equipo que llegue el armario de evidencia con la asignación al analista correspondiente. El área mecánica, está orientada a la manipulación del hardware, si es necesario desarmar algún equipo para su revisión.

El área de almacenamiento, es donde se obtendrán los respaldos correspondientes y las imágenes forenses para su análisis posterior. En cuanto al software utilizado, se considera el Encase en estos momentos como el más adecuado, cabe señalar que varios elementos de la UMIP ya cuentan con certificaciones en este tipo de herramientas, que facilita principalmente la clonación de discos, la comprobación de la integridad criptográfica, recuperación de

archivos, de contraseñas, recuperación de archivos borrados, recuperación de e-amils borrados, análisis forense en redes, análisis forense en navegadores, análisis de dispositivos móviles, análisis de firmas de archivos, búsqueda de archivos, reportes automáticos, adquisición de evidencia RAM y herramientas de automatización.

La implementación de un Laboratorio fluctúa dentro de un rango económico de 50,000 a 100,000 dlls.

CONCLUSIONES

Internet se ha convertido en la opción favorita de una nueva generación de criminales, son menos de siete Unidades en materia de delitos electrónicos e informáticos que se encuentran operando activamente en nuestro país, los delitos en estos medios van en aumento, es imperante que las autoridades enfrenten estas nuevas formas delictivas estableciendo protocolos estandarizados para la confiscación de evidencia así como para su tratamiento. Se cuenta con personal especializado en la Fiscalia General del Estado de Chihuahua, sin embargo se observa orgánicamente una separación de tres áreas que si se fusionaran obtendrían resultados mucho más eficaces.

Los Ministerios Públicos y Policías Ministeriales, deben estar atentos a los cambios tecnológicos y a las nuevas maneras de operar por parte de la delincuencia., se observa un marcado desconocimiento en cómo atender a las víctimas de este tipo de delitos, quienes terminan desistiendo por la falta de orientación a continuar con sus casos.
De poco servirán las herramientas y los métodos utilizados si no se puede acreditar su validez ante un tribunal. Para ello es necesario que cumplan determinados requisitos. No hay que olvidar que los resultados de la labor investigadora serán puestos a disposición de autoridades judiciales y otras instancias decisorias.

Una herramienta forense debe demostrar en su funcionamiento niveles altos de eficacia e integridad para ganarse el respeto tanto de la comunidad profesional de investigadores como del personal que trabaja en la administración de justicia. Lo mismo cabe decir de los métodos de trabajo y la forma de exponer resultados.

Fuentes de Investigación

Bibliográficas

Código Penal del Estado de Chihuahua.2011.Capitulo IV. Articulo 327Bis.

Guerrero, D. (2010). *Fraude en la Red.* España: Editorial Ra-Ma. ISBN 978-84-9964-013-6

Lima, M. d. (1984). Delitos Electrónicos. *Criminalía #1-6.* Ediciones Porrua. México

Renato Alberto Ledeira Prado, V. R. (2006). *Diccionario Jurídico de los Medios de Comunicación.* España: Ed. Reus.

Valdez, J. T. (2005). Derecho Informáticos. México: 3ra Edición. Mc. Graw Hill.

Electrónicas

Amigas, P. (s.f.). *http://www.pantallasamigas.net/.* Obtenido de http://www.pantallasamigas.net/: http://www.sexting.es/

Antiterrorista, D. d. (2014). Identificción y confiscación de pruebas.

Best Practices For Seizing Electronic Evidence v 4.2 a Pocket Guide for First Responders U.S. Departament of Homeland Security, United States Secret Service (Security)

CSIRT Canadá. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

CSIRT Estados Unidos. https://www.us-cert.gov/

CSIRT España. https://www.ccn-cert.cni.es/

CSIRT México. http://www.cns.gob.mx/portalWebApp/wlp.c?__c=7d1

Centro de Respuesta a Incidentes de Seguridad Computacionales de la Universidad Autónoma de México. http://www.cert.org.mx/

Convenio sobre la ciberdelincuencia. (Noviembre de 2001). Obtenido de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

Delitos Informáticos. (9 de Noviembre de 2011). Obtenido de Delitos Informáticos: http://www.delitosinformaticos.com/11/2011/noticias/grooming-el-acoso-a-menores#.UnL9JXDTvl4

Derat, M. V. (17 de Enero de 2012). *www.ahoramismo.com.mx.* Obtenido de www.ahoramismo.com.mx: http://www.ahoramismo.com.mx/noticia.aspx?id=32279

Diplomatic Security Service, O. o. (s.f.). Principios de las investigaciones en Internet.

Diseño de Laboratorio para el análisis forense. http://mattica.com/

Equipo de respuesta a incidentes y delitos informáticos. http://csirtchihuahua.uach.mx/

Garza, L. C. (29 de Mayo de 2013). *www.proceso.com.* Obtenido de www.proceso.com: http://www.proceso.com.mx/?p=343455

Ley de comercio electrónico. (16 de Enero de 2015). Obtenido de www.profeco.gob.mx: http://www.profeco.gob.mx/internacionales/com_elec.asp

Ley Federal de Datos personales en posesión de particulares. (05 de Julio de 2010). Obtenido de www.diputados.gob.mx: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

México, U. p. (5 de Septiembre de 2013). *www.pan.senado.gob.mx*. Obtenido de www.pan.senado.gob.mx: http://www.pan.senado.gob.mx/gppan/intervencion-del-senador-victor-hermosillo-y-celada-combatir-la-pornografia-infantil/

Noticias, U. (9 de Septiembre de 2013). *http://www.uniradioinforma.com/*. Obtenido de http://www.uniradioinforma.com/: http://www.uniradioinforma.com/noticias/policiaca/articulo219117.html

Policia Científica México. http://www.cns.gob.mx/portalWebApp/wlp.c?__c=7d1

Protección, M. C. (s.f.). *Microsoft Centro de Seguridad y Protección*. Obtenido de www.microsoft.com: http://www.microsoft.com/es-es/security/resources/identitytheft-whatis.aspx

Security, U. D. (s.f.). Best Practices For Seizing Electronic Evidence v. 4.2. Estados Unidos.