Instituto Politécnico Nacional

Escuela Superior de Ingeniería Mecánica y Eléctrica

Unidad Culhuacán

"Delitos Electrónicos y su Prevención"

T E S I S

QUE PARA OBTENER E TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A

Joan Victorio Citalán

Ciudad de México, Marzo de 2016.

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESIS INDIVIDUAL

Que como prueba escrita de su Examen Profesional para obtener el Título de **INGENIERO EN COMPUTACIÓN** deberá desarrollar el C.:

JOAN VICTORIO CITALAN

"DELITOS ELECTRÓNICOS Y SU PREVENCIÓN"

Justificación del Trabajo:

Debido a la falta de atención de las autoridades al momento de sancionar estas actividades ilícitas de esta índole o del desconocimiento de ellas; o mejor dicho por la gran falta de legislación en los delitos informáticos, así como la falta de educación hacía a la población sobre estas nuevas formas de delitos. Es necesario ver otras formas de combatirlos, así como informar a la parte más afectada que es la sociedad. Actualmente la policía federal enfrenta los delitos informáticos con mucha deficiencia con las actuales leyes que rigen a México, el desconocimiento y mal manejo del nuevo tipo de evidencia que se desarrolla en el mundo virtual, así como el manejo de los dispositivos que contienen dicha evidencia a provocado las malas sanciones a las personas que incurren en dichos delitos.

Por eso en la mejor manera para evitar estos delitos son la prevención y conocimiento de estos, por parte de la población en general, así como la manera de tratar a estos por parte de los funcionarios encargados de hacer cumplir la ley

CAPITULADO:

CAPÍTULO I.- ESTADO DEL ARTE
CAPÍTULO II.- CONCEPTOS TEÓRICOS
CAPÍTULO III.- LEGISLACIÓN
CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

México D. F., a 11 de diciembre del 2015

M. EN C. HÉCTOR BECERRIL MENDOZA
PRIMER ASESOR

M. EN C. VÍCTOR GUILLERMO LÓPEZ GARCÍA
SEGUNDO ASESOR

DR. JOSÉ VELÁZQUEZ LÓPEZ
JEFE DE LA CARRERA DE I.C.

M. EN C. HÉCTOR BECERRIL MENDOZA
SUBDIRECTOR ACADEMICO

Instituto Politécnico Nacional

Escuela Superior de Ingeniería Mecánica y Eléctrica

Unidad Culhuacán

"Delitos Electrónicos y su Prevención"

T E S I S

QUE PARA OBTENER E TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A

Joan Victorio Citalán

Ciudad de México, Marzo de 2016.

Agradecimientos

Agradezco a toda mi familia por el apoyo otorgado a mi persona, en especial a mi Señora Madre por todo lo que ha hecho por mí. A todas las personas que de alguna u otra manera ha afectado mi vida, no menciono nombres porque no quiero omitir a nadie. Así mismo expreso mi enorme gratitud con el Instituto Politécnico Nacional, noble institución donde obtuve grandes enseñanzas. A la Policía Federal, institución en donde sigo reafirmando mi compromiso hacia México.

A continuación algunas frases que me han inspirado, a lo largo de mi vida.

"Solo sé que no se nada y, al saber que no sé nada, algo sé; porque sé que no sé nada".

Sócrates, Filósofo Griego.

"*Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores****".***

Kevin Mitnick, El hacker más famoso de todos los tiempos.

"el crimen perfecto no existe, lo que existen son las investigaciones imperfectas"

Licenciado Eloy Emiliano Torales, Experto en Ciencias Penales y en Criminología.

Índice General

Índice de Figuras

Anexos

INTRODUCCIÓN

El propósito de la informática forense se debe principalmente a la amplia variedad de delitos informáticos que tienen lugar. En los avances tecnológicos actuales, es común para todas las organizaciones utilizar los servicios de los expertos en informática forense. Hay diversos delitos informáticos que se producen a pequeña escala, así como a gran escala. La pérdida resultante depende de la sensibilidad de los datos de la computadora o la información del delito cometido.

Se ha vuelto vital en el mundo corporativo, un robo de los datos en una organización puede generar grandes pérdidas. Para ello la informática forense se utiliza, ya que ayudan en el seguimiento de los criminales.

La necesidad de ella en esta época se puede considerar como de vital importancia debido a los avances de Internet y la dependencia de la misma.

Esta es también eficiente en donde se almacenan los datos en un sistema único para la copia de seguridad. El robo de datos y el daño intencional de los datos en un único sistema también se puede minimizar con ella. Hay hardware y software que emplean en las medidas de seguridad con el fin de rastrear los cambios y la actualización de los datos o la información. La información del usuario se proporciona en los archivos de registro que pueden ser utilizados eficazmente para producir la prueba en caso de algún delito.

Su objetivo principal es la producción de pruebas en el tribunal que puede dar lugar a la sanción, la ciencia forense es en realidad el proceso de utilizar el conocimiento científico con el propósito de recolectar, analizar, y lo más importante presentar la evidencia en el tribunal de justicia.

La necesidad o la importancia es asegurar la integridad del sistema informático. Un sistema con algunas pequeñas medidas pueden evitar el costo de operación y mantenimiento de la seguridad. El tema ofrece un profundo conocimiento para la

comprensión del marco jurídico, así como los aspectos técnicos de la delincuencia informática. Es muy útil desde el punto de vista técnico.

Su importancia es evidente en el seguimiento de los casos de la pornografía infantil y el spam de correo electrónico. Así mismo se ha utilizado eficientemente para localizar a los terroristas de las diversas partes del mundo. Los terroristas utilizan Internet como medio de comunicación pero en la mayoría de los casos pueden ser localizados y sus planes pueden ser conocidos.

Hay muchas herramientas que pueden utilizarse en combinación con la informática forense para averiguar la información geográfica y las salidas de los criminales. La dirección IP tiene un papel importante para determinar la posición geográfica de los terroristas.

Capítulo 1

“Estado del Arte”

1.1 Historia de la Informática Forense

Si bien los delitos informáticos aparecieron prácticamente desde la invención de las computadoras, en los últimos años se ha visto un aumento del cibercrimen orientado a infectar computadoras como objetivo final, enmarcados en ataques ciberterroristas, hacktivistas o del crimen organizado.

Según el reporte de cibercrimen 2012 de Norton, se estima que en ese año tan sólo en México más de 14.8 millones de personas fueron víctimas de delitos informáticos que ocasionaron pérdidas financieras directas por un monto de 2.2 miles de millones de dólares.

Estas cifras son evidencia de una gran fragilidad y falta de prevención frente a los delitos informáticos de parte de los usuarios, especialmente, en el ámbito corporativo. De acuerdo con un estudio realizado por Kapersky Lab, el 48% de las compañías tiene una protección insuficiente contra el robo de propiedad intelectual y otros ilícitos realizados en línea. Esta situación se agrava a causa de la falta de despliegue de políticas de seguridad y la falta de concientización de los empleados, lo que facilita a los ciberdelincuentes encontrar nuevas formas de beneficiarse de las corporaciones y, al mismo tiempo, lograr la profesionalización del ejercicio delictivo en la red.

Entre los delitos más frecuentes, especialmente en nivel empresarial, tenemos el robo de información. El 80% de los delitos de este tipo provienen del interior de la misma corporación, es decir, los empleados, incluso los que generan mucha confianza pueden ser la mente maestra detrás del robo de información valiosa para la empresa.

Tal es el caso, por ejemplo, de la industria automotriz: al desarrollar sus operaciones en ambientes abiertos, este tipo de corporaciones son proclives a padecer algún tipo de delito cibernético de manera deliberada o por descuido de sus colaboradores. En ese sentido es importante que cualquier agencia, por pequeña que ésta sea, tome las medidas mínimas en seguridad como el de

impulsar una cultura de las Cartas de Asignación de equipos de cómputo en la empresa, lo que ayudará a individualizar responsabilidades.

Otro de los delitos de mayor frecuencia son los ciberataques en redes sociales y teléfonos móviles. En lo que respecta a los ataques en redes sociales, el robo de identidad es uno de los métodos más usados para obtener información de una persona con el fin de perjudicarla u obtener algún beneficio. De acuerdo al último Reporte de Cibercrimen de Norton, tan solo en Facebook durante el 2012 hubo casi seis millones de fraudes manuales y cerca de 600 mil falsas ofertas y encuestas.

1.2 Investigación Forense Digital

En la actualidad cualquier dispositivo digital que forma parte de la vida de una persona es capaz de generar información que puede convertirse en evidencia valiosa en caso de presentarse un incidente de seguridad; ya sea en forma de una fotografía, documento, registro de geo localización GPS, mensaje de texto, correo electrónico o incluso un número telefónico registrado como parte de una llamada. Esta evidencia es útil para investigar casos relacionados con actividades cibercriminales o de ataques informáticos, el problema es que muchas veces la recolección y el manejo de esta información no se realizan de manera adecuada.

La mayoría de las empresas aún no cuentan con políticas o normas que refieran como debe realizarse la respuesta a un incidente de estas características. La falta de preparación y conocimiento de los procedimientos para manejar estos incidentes lleva muchas veces a privilegiar la continuidad de las operaciones del negocio, sin averiguar de dónde provino el ataque o cual fue el grado de impacto y afectación.

Con el creciente número de ataques dirigidos o de APTs vale la pena revisar la importancia que tiene elevar el nivel de consciencia de las organizaciones en este sentido. Un malware hecho a la medida con el fin de realizar labores de

ciberespionaje o sabotaje y que no es detectado a tiempo o que no se llega a conocer cuál fue su origen puede provocar daños importantes para las organizaciones. Peor aún, si se logra detectar y rastrear el origen pero no se llevaron a cabo los procedimientos adecuados, el resultado será que cualquier evidencia obtenida durante el proceso de investigación no podrá ser utilizada en una corte en caso de pretender llevar a juicio a los delincuentes.

¿Cuáles son entonces los procedimientos adecuados? ¿Existe alguna norma o regulación internacional? ¿Cualquier persona puede realizar estos procedimientos?

1.2.1 Procedimientos para realizar una investigación forense digital

1.2.1.1 Adquisición

Esta fase es sumamente importante y contempla la obtención de información por medio de copias desde los dispositivos donde se sospeche que pudiera existir evidencia que ayude a la investigación del caso. Estas copias deben realizarse con herramientas especiales que permitan la transferencia bit a bit de la información y la generación de una firma digital basada en un algoritmo hash para garantizar la integridad de la evidencia obtenida.

Para la realización de los procedimientos de esta fase es muy importante que se cuente con la preparación adecuada y las herramientas correctas ya que cualquier error puede provocar la contaminación o pérdida de la evidencia y que esta pueda ser inadmisible en la corte en un eventual juicio.

Adicionalmente existen procedimientos que se deben seguir de forma cuidadosa, como son el aseguramiento de la escena y seguir la regla de, si el equipo se

encuentra encendido, realizar el procedimiento sin apagar el equipo y si el equipo se encuentra apagado, no encenderlo para evitar compromiso de la evidencia.

Algunos de los procedimientos más importantes para realizar en la etapa de la recolección es:

- Fotografiar la escena.
- Realizar entrevistas con las personas que conocen del caso.
- Documentar los procedimientos.
- Realizar un inventario de cada elemento a ser analizado, esto pudiera incluir: cables de red, dispositivos USB, CD o DVD.
- Almacenar todo en empaques o bolsas especiales con etiquetas para guardar evidencia, estas bolsas están hechas de material especial para evitar que el contenido se dañe.

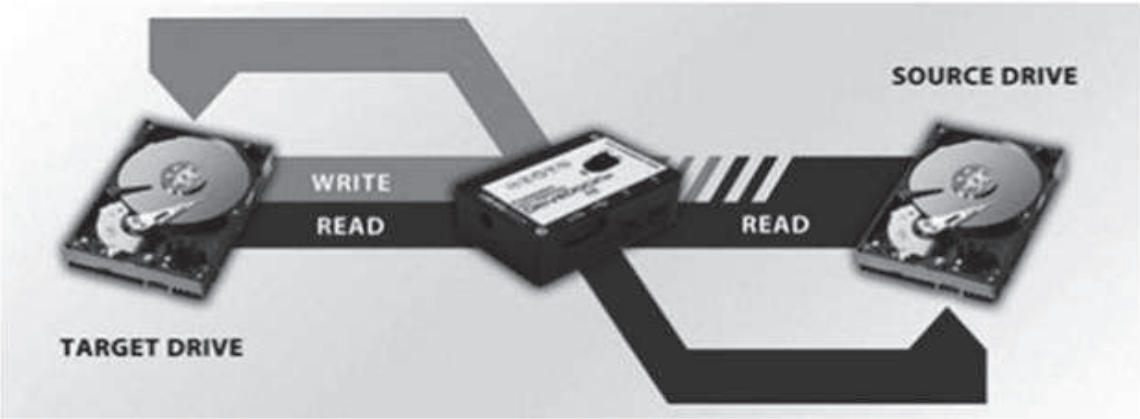


Figura 1.1.- Adquisición de la Información de un dispositivo de almacenamiento masivo

1.2.1.2 Preservación

Una vez que se ha obtenido la información de los dispositivos es muy importante mantener y preservar dicha información. Para ello debe realizarse un procedimiento denominado “Cadena de Custodia” que consiste en generar un documento que contenga la información de los dispositivos de los cuales se

realizaron copias digitales como números de serie, marcas, modelos, firmas digitales, persona que realizo el procedimiento, además de incluir el nombre y firma con fecha de la persona que entrega el dispositivo original, así como de la persona que lo recibe.

El objetivo de la Cadena de Custodia es documentar el traslado y posesión de los dispositivos digitales o medios de donde se obtuvo la información para la realización de la investigación, desde que inicia el proceso, durante la investigación y hasta que finalice el juicio o la investigación para garantizar que no exista contaminación, daño, alteración o manipulación de la evidencia y de esta forma mantener la confiabilidad en el proceso.

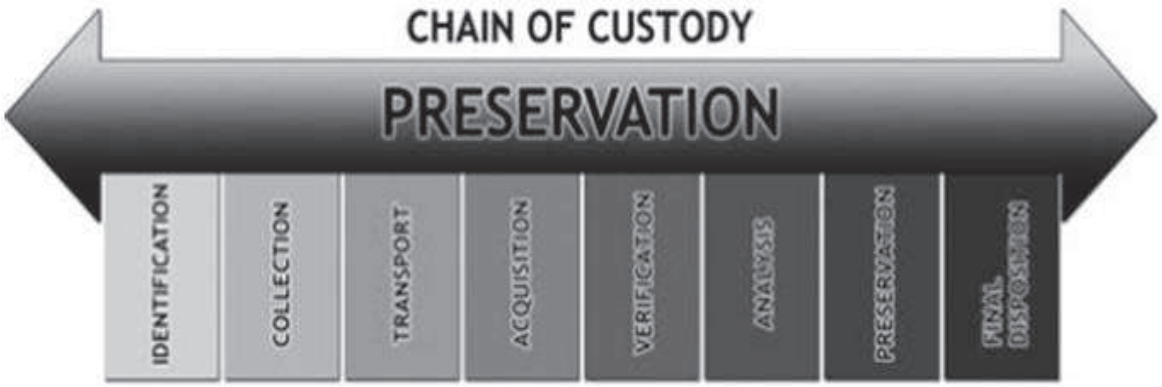


Figura 1.2.- Uso de la Cadena de Custodia en la fase de Preservación

1.2.1.3 Análisis

Ya en el laboratorio forense, comienza la fase de análisis de evidencia en el laboratorio. Éste es un proceso que puede ser laborioso y la duración de esta fase depende de la complejidad del caso y el alcance de lo que se está buscando.

Adicionalmente se presentan varios inconvenientes para poder realizar la investigación, por ejemplo, el equipo o alguna información pudieran estar protegidos con contraseña, cifrados o manipulados para ocultar sus contenidos

mediante técnicas como estenografía o incluso algo tan simple como cambiar las extensiones de los archivos para hacer creer que estos están dañados.

En esta etapa es fundamental contar con las herramientas adecuadas así como el conocimiento, experiencia e intuición del investigador.

1.2.1.4 Presentación

Una vez concluida la investigación se preparan los informes correspondientes con los hallazgos encontrados respaldados con evidencia robusta y confiable.

Existen diferentes tipos de informes y mucho dependerá del tipo de investigación realizada, por ejemplo, el informe puede ser dirigido hacia los directivos de la empresa que solicitó la investigación pero que no están considerando darle un cauce legal, o puede ser un informe detallado que incluya términos legales para ser presentado en una corte para un juicio.

Existen informes que incluyen contenido altamente técnico o aquellos que sólo resaltan los aspectos más importantes de la investigación sin contener información muy técnica y en un lenguaje más cotidiano.

1.2.2 Importancia de la Evidencia Digital y Retos

Como se puede observar, en todo este procedimiento la evidencia juega un papel fundamental ya que para poder demostrar un supuesto se debe contar con todos los elementos de prueba que respalden la forma como se dio el incidente y permitan responder 6 preguntas clave: Qué, Quién, Cómo, Cuándo, Dónde y Por qué.

Por esa razón es muy importante que se lleven a cabo los procedimientos adecuados en la obtención y manejo de la evidencia ya que su confiabilidad representa nuestro único elemento de prueba para demostrar algo.

Los ciberdelincuentes utilizan, cada vez con mayor frecuencia, herramientas y técnicas antiforenses con la idea de confundir, complicar y entorpecer la labor de los investigadores.

Por otro lado, la mayoría de los países no tienen una legislación clara en relación a los delitos informáticos y en el peor de los casos ni siquiera existen leyes para poder perseguir estos delitos.

De nada sirve que se realicen todos los procesos de investigación si al final las pruebas obtenidas no tendrán una validez o peso legal debido a las carencias de las leyes. En algunos otros casos existe una brecha generacional y tecnológica en los jueces y muchos de ellos mantienen una verdadera resistencia al cambio, lo que conlleva al rechazo de evidencia obtenida digitalmente.

La falta de información en la materia por parte de las empresas e incluso los abogados es otro factor importante ya que muchos de los delitos o incidentes informáticos no se denuncian debido a que se asume que será costoso el proceso y al final no se tendrán resultados.

1.2.3 Dispositivos de Comunicación Móvil

Los teléfonos celulares, así como todos los dispositivos móviles, son aparatos que en la actualidad utiliza la mayoría de la gente. Al igual que las computadoras, estos artefactos han dejado de ser un lujo, pues se han convertido en una necesidad. Además de cumplir con la función básica de un celular (realizar y recibir llamadas telefónicas), la mayoría de ellos cuentan con funciones especiales: el envío de Mensajes de Texto Cortos (SMS), Mensajes de Texto Multimedia (MMS), Mensajes Instantáneos (IM), correos electrónicos, navegar en

Internet y Administrador de Información Personal (PIM) con ayuda de ciertas aplicaciones, entre otras.

Casi todos los celulares permiten a los usuarios la instalación de ciertas aplicaciones, así como el almacenamiento de información personal y confidencial, sin importar el sistema operativo, la forma en la que se sincroniza la información o cómo se conectan con los equipos de cómputo. Los celulares son parte de la tecnología que nos rodea hoy en día. Su mejora y actualización es constante.

Cuando un celular es involucrado en un crimen o en un incidente, los analistas forenses requieren de herramientas que permitan obtener una apropiada y rápida recuperación de la información almacenada en el dispositivo. Después de ser analizada, servirá para redactar un reporte detallado de las actividades realizadas, incluyendo fechas, con la finalidad de buscar evidencias que revelen la causa y forma en la que se llevó acabo un delito o se violó una política, en algunos casos esta información puede obtenerse, aun cuando ésta haya sido borrada.

1.2.3.1 Análisis Forense en Celulares

En este trabajo normalmente se involucran la identificación, preservación (no modificación de la evidencia), obtención, documentación y análisis de información. En el análisis forense clásico se siguen ciertas metodologías y procedimientos bien definidos. Muchas de estas metodologías pueden ser adaptadas al análisis forense en celulares. Tales consisten generalmente en los siguientes pasos:

- Preparar una copia de la evidencia digital (sin tener que arriesgar la integridad de la evidencia).
- Examinar la copia obtenida con la finalidad de recuperar la información.
- Analizar la información recuperada.
- Crear un reporte describiendo los datos recuperados en todo el procedimiento de análisis.

Las herramientas de análisis forense intentan facilitar el trabajo en cada uno de estos pasos, enfocados a crear un reporte final de calidad y veraz.

Este tipo de trabajo en celulares es un tema relativamente nuevo, surge a raíz del análisis forense en equipos de cómputo, enfocado a servidores de trabajo y red. Un dispositivo móvil es capaz de almacenar información digital en una memoria interna o externa, en una pequeña tarjeta que traen todos los celulares (SIM Módulo de Identificación de Abonado) o enviarla a otro dispositivo haciendo uso de Internet. Toda información digital puede convertirse en evidencia que revele detalles de actividades realizadas en el dispositivo móvil; dichas actividades deben investigarse contestando las mismas preguntas en las que se basa el análisis forense clásico: ¿qué se hizo?, ¿cómo se hizo? y ¿en qué orden se hizo? Las discrepancias entre el análisis forense a celulares y el análisis forense clásico existen debido a varios factores, entre los que se incluyen:

- El diseño orientado a la facilidad de transporte (por ejemplo el tamaño y las pilas que requieren de una interfaz y hardware especial).
- El sistema de archivos almacenado en una memoria volátil contra memorias no volátiles.
- El comportamiento de hibernación, la suspensión de procesos cuando se apaga y se vuelve a activar.
- La diversidad de sistemas operativos embebidos.
- Ciclos cortos de producción para introducir nuevos dispositivos.

La mayoría de los dispositivos móviles ofrecen excelentes sistemas operativos básicos con capacidades competentes entre ellos. Sin embargo, la diversidad de familias existentes en el mercado difiere en áreas como tecnología del hardware, características avanzadas, incluso en el aspecto físico.

En un caso práctico de un dispositivo móvil con tecnología GSM (Sistema Global para las Comunicaciones Móviles), puede trabajarse en dos escenarios: el primero inicia con la tarjeta SIM instalada en el celular y el segundo parte simplemente de una tarjeta SIM, sin necesidad de conocer el modelo y fabricante del dispositivo móvil donde fue instalada la tarjeta SIM.

1.2.3.2 Un Dispositivo Móvil como parte de un Delito

El tema de la extorsión telefónica se ha incrementado por la facilidad con la que se puede adquirir un celular, sin necesidad de que el usuario proporcione datos de identificación personal. Cada vez que una persona mal intencionada tenga acceso a un celular que no necesariamente le pertenezca, puede utilizar la información encontrada para hacer una extorsión telefónica.

La forma más común de operar de los extorsionadores telefónicos se basa en hacer llamadas al azar, y en las subsecuentes que el extorsionador realice, sólo necesitará cambiar los dos últimos dígitos. Si la llamada es contestada, el exige grandes cantidades de dinero a cambio de la libertad de un familiar presuntamente secuestrado. En este tipo de casos un analista forense, utilizando las herramientas correctas, podría obtener las últimas llamadas realizadas y contestadas, los últimos mensajes de texto enviados y recibidos, los últimos mensajes de texto multimedia, los mensajes instantáneos, correos electrónicos e incluso información personal, sin olvidar los archivos de imágenes que podrían ayudar a describir acciones delictivas. El analista, al encontrar todos los eventos registrados en el dispositivo móvil, tendrá elementos suficientes para asegurar que se ha realizado un acto delictivo y culpar o exonerar al dueño del dispositivo.

Por diversos que sean los dispositivos móviles, tecnológicamente puede ser fácil encontrar evidencias digitales, esta misma diversidad acarrea consigo una desventaja al momento de crear leyes internacionales que puedan aplicarse en cualquier país en el que se esté haciendo mal uso del dispositivo móvil. La velocidad con la que cambia la tecnología en los dispositivos móviles es mayor comparada con la velocidad en que cambian las leyes de un país, lo que puede significar un problema si se considera que un intruso puede diseñar una estrategia de ataque, usando un dispositivo móvil desde un país donde no existan leyes que consideren la evidencia digital como parte de un delito.

1.2.3.3 Futuras Amenazas

De acuerdo con la actual evolución tecnológica de los dispositivos móviles existen nuevas bondades que los asemejan cada vez más a una computadora, del tamaño de un celular o un Asistente Personal Digital (PDA), por lo que estos dispositivos presentan la capacidad de funcionar como una cámara digital que obtiene imágenes y video de alta calidad, un reproductor de música con capacidad de almacenar hasta 250 canciones (en el peor de los casos), una agenda personal con capacidad de conectarse a Internet, de forma inalámbrica, para consultar correo electrónico o cualquier sitio Web, un sistema de posicionamiento global que ayude a localizar la ubicación física de quien porta el dispositivo, así como la ruta más corta para llegar a un destino, finalmente, un teléfono que pueda llevarse a casi cualquier parte del mundo, con la confianza de que el dispositivo hará lo necesario para negociar la renta de señal y realizar una llamada o videollamada, esto en un mismo dispositivo de tamaño atractivo.

Para que los nuevos dispositivos móviles puedan ser aprovechados al máximo, la mayoría de los proveedores de servicios de Internet y telefonía están instalando y ajustando su infraestructura para que el intercambio de información sea más rápido y accesible en casi cualquier parte del mundo. Con estos avances en la tecnología, los analistas forenses predicen que a corto plazo, los vectores de ataques estarán enfocados a apoderarse de los dispositivos móviles conectados a Internet. Los intrusos aprovecharán el ancho de banda para infectar a los dispositivos móviles con algún virus o gusano. Una vez infectados, los intrusos programarán instrucciones que reporten las actividades de las víctimas, para lo cual recibirán imágenes o videos en tiempo real que detallen el lugar donde se encuentre las víctimas, las personas que lo acompañan, la forma como viste la víctima e incluso quienes la rodean. El intruso estará recibiendo de forma automatizada una serie de imágenes y videos en un servidor central, desde el cual podrá enviar órdenes para aumentar o disminuir la frecuencia a la que el dispositivo móvil mandará archivos multimedia. En el ataque también pueden

incluirse conversaciones privadas obtenidas gracias al dispositivo móvil que la víctima porte en la bolsa del pantalón, en la camisa o atado a la cintura.

Esta nueva forma de espionaje puede ser nombrada como “Botphones”, haciendo alusión al término “**bot**”, utilizado para nombrar un equipo de cómputo comprometido que puede ser controlado remotamente tanto de forma centralizada como descentralizada. Siguiendo la misma línea de los “Botphones”, otro vector de ataque puede estar basado en las conexiones de salida que realiza un dispositivo móvil. Con esto podemos pensar en una negación de servicio provocado por miles de dispositivos móviles comprometidos, que intenten hacer conexiones a un servidor al mismo tiempo, hasta lograr impactar la disponibilidad de un servicio.

Este y otros ataques forman parte de los problemas que está sufriendo como sociedad. Mientras no existan leyes que respalden a las víctimas, se tendrá que procurar formas para evitar que la tecnología se convierta en un instrumento que los intrusos usen para beneficiarse.

1.3 Delito Informático

Un delito informático o ciberdelincuencia es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática.

La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por crackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

Existen leyes que tienen por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos en las variedades existentes contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

1.3.1 Generalidades de los Delitos Informáticos

La criminalidad informática incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

1. Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, Spam, ataques masivos a servidores de Internet y generación de virus.
2. Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc.

Un ejemplo común es cuando una persona comienza a robar información de websites o causa daños a redes o servidores. Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra en forma digital y el daño aunque real no tiene consecuencias físicas distintas a los daños causados sobre los ordenadores o servidores. En algunos sistemas judiciales la propiedad intangible no puede ser robada y el daño debe ser visible. Un ordenador puede ser fuente de pruebas y, aunque el ordenador no haya sido directamente

utimarinalizado para cometer el crimen, es un excelente artefacto que guarda los registros, especialmente en su posibilidad de codificar los datos. Esto ha hecho que los datos codificados de un ordenador o servidor tengan el valor absoluto de prueba ante cualquier corte del mundo.

1.3.2 Sujetos Activos y Pasivos

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Esta categoría requiere que:

- El sujeto activo del delito sea una persona de cierto estatus socioeconómico.
- Su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional.

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

Para la labor de prevención de estos delitos es importante el aporte de los damnificados que puede ayudar en la determinación del modus operandi, esto es de las maniobras usadas por los delincuentes informáticos.

1.3.3 Crímenes Específicos

1.3.3.1 Spam

Correo electrónico no solicitado, usado con propósito comercial, es ilegal en diferentes grados. La regulación de la ley en cuanto esté en el mundo es relativamente nueva, por lo general impone normas que permiten la legalidad de el en diferentes niveles. El spam legal debe cumplir estrictamente con ciertos requisitos como permitir que el usuario pueda escoger el no recibir dicho mensaje publicitario o ser retirado de listas de correo electrónico.

Dentro de los delitos informáticos que relacionan a este existen distintos tipos:

- El que se envía a través del correo electrónico.
- El que usa en aplicaciones de mensajería instantánea (Messenger, etc).
- El que se envía a dispositivos móviles mediante mensajes de texto o imágenes.

1.3.3.2 Fraude Informático

Es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente:

1. Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.
2. Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar.
3. Alterar o borrar archivos.

4. Alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento.

Otras formas de este delito incluye la utilización de sistemas de computadoras para robar bancos, realizar extorsiones o robar información clasificada.

1.3.3.3 Contenido Obsceno u Ofensivo

El contenido de un website o de otro medio de comunicación puede ser obsceno u ofensivo por una gran gama de razones. En ciertos casos dicho contenido puede ser ilegal. Igualmente, no existe una normativa legal universal y la regulación judicial puede variar de país a país, aunque existen ciertos elementos comunes. Sin embargo, en muchas ocasiones, los tribunales terminan siendo árbitros cuando algunos grupos se enfrentan a causa de contenidos que en un país no tienen problemas judiciales, pero sí en otros. Un contenido puede ser ofensivo u obsceno, pero no necesariamente por ello es ilegal.

Algunas jurisdicciones limitan ciertos discursos y prohíben explícitamente el racismo, la subversión política, la promoción de la violencia, los sediciosos y el material que incite al odio y al crimen.

1.3.3.4 Hostigamiento/Acoso en Redes Sociales

El hostigamiento o acoso es un contenido que se dirige de manera específica a un individuo o grupo con comentarios vejatorios o insultantes a causa de su sexo, raza, religión, nacionalidad, orientación sexual, identidad etnocultural, etc. Esto ocurre por lo general en canales de conversación, grupos o con el envío de correos electrónicos destinados en exclusiva a ofender. Todo comentario que sea denigrante u ofensivo es considerado como hostigamiento o acoso. El acto de destruir los artículos, desaparecer el nombre de un determinado autor, el 'delete'

de los nombres de las publicaciones de un intelectual, que realizan supuestos guardianes de “Wikipedia” es otra forma de acorralamiento o bullying digital, atentando contra los derechos humanos y la libertad de expresión, mientras no afecten a terceros.

1.3.3.5 Tráfico de Drogas en Internet

El narcotráfico se ha beneficiado especialmente de los avances del Internet y a través de éste promocionan y venden drogas ilegales a través de emails codificados y otros instrumentos tecnológicos. Muchos narcotraficantes organizan citas en cafés Internet. Como esta red facilita la comunicación de manera que la gente no se ve las caras, las mafias han ganado también su espacio en el mismo, haciendo que los posibles clientes se sientan más seguros con este tipo de contacto. Además, el Internet posee toda la información alternativa sobre cada droga, lo que hace que el cliente busque por sí mismo la información antes de cada compra.

1.3.3.6 Terrorismo Virtual

Desde 2001 el terrorismo virtual se ha convertido en uno de los novedosos delitos de los criminales informáticos los cuales deciden atacar masivamente el sistema de ordenadores de una empresa, compañía, centro de estudios, oficinas oficiales, etc. La difusión de noticias falsas en Internet (por ejemplo decir que va a explotar una bomba en el Metro), es considerado terrorismo informático y es procesable.

1.3.4 Delitos Informáticos en otros Países

1.3.4.1 Argentina

La Argentina sancionó el 4 de junio del 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

1.3.4.2 Colombia

En Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según estadísticas, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

En Colombia existen instituciones de educación como UNICOLOMBIA que promueven capacitaciones en temas relacionados con Delitos Informáticos, el mejor manejo y uso de la prueba digital, establecer altos estándares científicos y éticos para Informáticos Forenses, Llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e Instruir a los estudiantes en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática Forense, la investigación científica y el proceso tecnológico de las mismas.

1.3.4.3 España

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de Noviembre en el BOE número 281, de 24 de noviembre de 1995. Éstos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

A la hora de proceder a su investigación, debido a que una misma acción puede tener consecuencias en diferentes fueros, comenzará la investigación aquel partido judicial que primero tenga conocimiento de los hechos delictivos cometidos a través de un medio informático, si durante el transcurso de la investigación, se encuentra al autor del delito y pertenece a otro partido judicial, se podrá realizar una acción de inhibición a favor de este último para que continúe con la investigación del delito.

1.3.4.4 Venezuela

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.

La ley tipifica cinco clases de delitos:

- Contra los sistemas que utilizan tecnologías de información: acceso indebido; sabotaje o daño a sistemas; favorecimiento culposos del sabotaje o daño; acceso indebido o sabotaje a sistemas protegidos; posesión de equipos o prestación de servicios de sabotaje; espionaje informático; falsificación de documentos.
- Contra la propiedad: hurto; fraude; obtención indebida de bienes o servicios; manejo fraudulento de tarjetas inteligentes o instrumentos análogos; apropiación de tarjetas inteligentes o instrumentos análogos; provisión indebida de bienes o servicios; posesión de equipo para falsificaciones;
- Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal; violación de la privacidad de las comunicaciones; revelación indebida de data o información de carácter personal;
- Contra niños y adolescentes: difusión o exhibición de material pornográfico; exhibición pornográfica de niños o adolescentes;
- Contra el orden económico: apropiación de propiedad intelectual; oferta engañosa.

1.3.4.5 Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas y entre empresas y consumidores.

1.3.4.6 Chile

En Chile el 28 de mayo de 1993, se promulgó la ley 19.223 pero no fue hasta la fecha 07 de Junio de 1993 que ésta se publicó. Esta ley, tipifica y sanciona los denominados Delitos Informáticos.

Los delitos tipificados en la Ley 19.223 consideran como un bien jurídico la calidad, la pureza e idoneidad de la información que está contenida en cualquier sistema automatizado de tratamiento de la información. Además, no solo se protege el bien mencionado anteriormente sino que también los siguientes:

- El patrimonio, en el caso de los fraudes informáticos.
- La privacidad, intimidad y confidencialidad de los datos, en el caso de espionaje informático.
- La seguridad y fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos probatorios mediante algún sistema o medio informático.
- El derecho de propiedad sobre la información y sobre los elementos físicos y materiales de un sistema de información, en el caso de los delitos de daños.

Capítulo 2

“Conceptos Teóricos”

2.1 Definición de Indicio

Es aquello que nos permite inferir o conocer la existencia de algo que no se percibe al momento.

De acuerdo a los estudios llevados a cabo por el **lógico y filósofo Charles Sanders Peirce**, el indicio es un signo que estará determinado por su objeto dinámico como consecuencia de la relación que mantiene con éste. El indicio es uno de los tres niveles que presenta el signo; el mismo se encuentra inmediatamente relacionado con el objeto denotado, como por ejemplo, la aparición de un síntoma de una enfermedad, el movimiento de una veleta hacia una determinada dirección, lo cual nos dirá la dirección que presenta en ese momento el viento.

En el ámbito de la **criminalística**, el término indicio ocupa un lugar preferencial, ya que evoca un signo aparente y probable de la existencia de alguna cosa y al mismo tiempo es un sinónimo de señal, de indicación. Por eso es que un indicio, en estas circunstancias, será todo material sensible significativo que pueda ser percibido a través de los sentidos y que está en relación con el suceso delictivo que se investiga.

Al tratarse de un material sensible entendemos que se encuentra conformado por elementos que son aprehendidos y percibidos únicamente a partir de la utilización de los órganos de nuestros sentidos: el oído, los ojos, las manos. Para maximizar la captación del material sensible será necesario que nuestros órganos estén absolutamente abocados al mismo objeto. De esta manera evitaremos todo tipo de error o confusión en la selección del material a estudiar. Una vez que se ha comprobado su relación con el hecho que se investiga, pasará a ser una evidencia.

De acuerdo a la relación que presenten con los hechos, los indicios podrán ser: **indicios determinados** (aquellos que necesitan un análisis minucioso a simple vista y están directamente relacionados con la persona que los produce, tal es el caso de las huellas dactilares en armas) e **indicios indeterminados** (son

aquellos que necesitan de un análisis completo para así poder conocer tanto su composición como su estructura de acuerdo a su naturaleza física, como ser: pelos, fibras, orina, semen, vómito, huellas de sangre, entre otros).

Y a la **primera manifestación o la pequeña cantidad de algo** se la designa también con la palabra indicio.

2.2 Prueba en Derecho

Prueba, del latín *probo*, bueno, honesto y *probandum*, recomendar, aprobar, experimentar, patentizar, hacer fe.

- En sentido estricto, la prueba es la obtención del cercioramiento del juzgador acerca de los hechos, discutidos y discutibles, cuyo esclarecimiento resulte necesario para la resolución del conflicto sometido a proceso. En ese sentido, la prueba es la verificación o confirmación de las afirmaciones de hechos expresadas por las partes.
- En sentido amplio, se designa como prueba a todo el conjunto de actos desarrollados por las partes, los terceros y el propio juzgador, con el objeto de lograr la obtención del cercioramiento judicial sobre los hechos discutidos y discutibles. Por último, por extensión también se suele denominar pruebas a los medios, instrumentos y conductas humanas con las cuales se pretende lograr la verificación de las afirmaciones de hecho. Así se habla de la prueba confesional, testimonial, ofrecimiento de las pruebas, etc.

Para analizar el objeto de la prueba se distinguirá los siguientes rubros:

1. El objeto de la prueba: Que son los hechos sobre los que versa la prueba.
2. La carga de la prueba: Es la atribución impuesta por la ley para que cada una de las partes proponga y proporcione los medios de prueba que confirmen sus propias afirmaciones de hecho.

3. El procedimiento probatorio, o sea la secuencia de actos desplegados por las partes, los terceros y el juzgador para lograr el cercioramiento judicial.
4. los medios de prueba, que son los instrumentos- objetos o cosas y las conductas humanas- con las cuales se trata de lograr dicho cercioramiento.
5. Los sistemas consignados en la legislación para que los juzgadores aprecie o determinen el valor de las pruebas practicadas (sistema de valoración de la prueba).

La prueba, en Derecho, es la actividad necesaria que implica demostrar la verdad de un hecho, su existencia o contenido según los medios establecidos por la ley.

La prueba recae sobre quien alega algo, ya que el principio establece que quien alega debe probar. El que afirma algo debe acreditar lo que afirma mediante un hecho positivo, si se trata de un hecho negativo el que afirma deberá acreditarlo mediante un hecho positivo. Peirano sostiene que la prueba recae sobre ambas partes, se trate o no de un hecho positivo. Si no, puede recaer sobre quien esté en mejores condiciones de probar. Aquí se produce una distribución de la carga de la prueba.

En síntesis, la obligación de probar dependerá de la situación adquirida por las partes en un proceso. Cada una de ellas deberá probar los hechos sobre los que funda su defensa.

2.3 Prueba Electrónica

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

La Evidencia Digital o la prueba electrónica es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio.

Antes de aceptar la evidencia digital un tribunal determinará si la prueba es pertinente, auténtica, si es un rumor y si es aceptable una copia o el original es requerido.

Cuando hablamos de Relevancia en términos legales, es la tendencia de un determinado artículo de la evidencia para probar o refutar uno de los elementos legales del caso, o para tener valor probatorio para hacer uno de los elementos del caso más probable o no. Probatorio es un término usado en la ley para significar "que tiende a demostrar." Pruebas: "busca la verdad".

Por lo general en la legislación, la evidencia que carece de valor probatorio (no tiende a probar la proposición para que se le ofrecía) es inadmisible y las reglas de evidencia permiten que sea excluida de un procedimiento o afectadas por el expediente u objetada por oposición un abogado. Una prueba digital puede ser aceptada si el valor de la misma puede ser sopesado frente a su naturaleza perjudicial.

El siglo XXI está lleno de innovaciones tecnológicas, a primera vista nuestra sociedad puede parecer bastante avanzada. Sin embargo, las apariencias engañan. En realidad, sólo estamos a la vanguardia de lo que está en el almacén para el futuro próximo. Con el paso de cada día, nuestras vidas son cada vez más digitalizadas, una sociedad totalmente sin papel está en el horizonte. A medida que en el mundo digital se anuncia que será importante para un individuo proteger su identidad y la privacidad, de aquellos que acechan en la distancia.

Un juicio penal es un procedimiento contradictorio en el que tanto la fiscalía como la defensa prueban sus casos mediante la presentación de pruebas. La evidencia puede ser un testimonio de una persona que tiene conocimiento personal de hechos relacionados con el delito, o puede ser una evidencia física, que es un elemento tangible, como un arma homicida, un registro de servidor de seguridad o un disco duro que contiene datos.

El problema con los datos digitales es que es algo menos tangible que la mayoría de las pruebas físicas. Pertenece a la categoría de pruebas frágiles, junto con cosas tales como huellas en la nieve, porque son fácilmente destruidos o

modificados. De hecho, el acto mismo de la recogida o el examen se puede cambiar. El problema con esto es que para que la evidencia sea admisible, la parte que la introducción debe demostrar que no ha sido alterado o modificado desde que fue recogida en la escena del crimen.

2.4 Evidencia Digital

Se puede decir que el término “Evidencia Digital” abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor. Desde el punto de vista del derecho probatorio, puede ser comparable con “un documento” como prueba legal. Con el fin de garantizar su validez probatoria, los documentos deben cumplir con algunos requerimientos, estos son:

- Autenticidad: satisfacer a una corte en que: los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa (p.e. la fecha).
- Precisión: debe ser posible relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte. Adicionalmente, los procedimientos deben ser seguidos por alguien que pueda explicar, en términos “entendibles”, cómo fueron realizados y con qué tipo de herramientas se llevaron a cabo.
- Suficiencia (completa): debe por sí misma y en sus propios términos mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

No existen investigaciones iguales, no es posible definir un procedimiento único para adelantar un análisis en Informática forense. Pero, si es posible definir una aproximación metodológica que permita el manejo adecuado de la evidencia digital, minimice la posibilidad de cometer errores en su manejo y que en alguna medida garantice la admisibilidad de la misma en situaciones jurídicas. Dicha

aproximación incluye cinco etapas: planeación, recolección, aseguramiento, análisis y presentación de la Evidencia Digital.

Se espera que en esta etapa se detecte el incidente, el investigador se familiarice con dicho incidente y con el entorno en el que ocurrió y determine el proceso para la recolección de evidencia.

El primer paso consiste en determinar los presuntos actores involucrados, (máquinas y/o usuarios), identificar el problema aparente e indagar qué tanto contacto tuvieron los usuarios con el sistema involucrado en el incidente, para darse una idea de la contaminación de la escena.

Como segundo paso, el investigador se debe familiarizar con el entorno informático y con el incidente en cuestión. Para ello se sugiere el desarrollo de entrevistas al personal de la organización que tenga algún tipo de relación con el entorno informático, se busca determinar: Qué tipo de sistemas informáticos se usan, qué tipo de registros generan, si se cuenta con políticas de seguridad o no y quiénes son responsables del funcionamiento de los equipos y los servicios de la organización, etc.

Quienes llevamos algunos años en la universidad, sabemos que un cambio de plan de estudios -muy conveniente y necesario plantearlo al menos cada 10 años- conlleva varios años de duras batallas y, lo que es peor, muchas veces influyen además aspectos colaterales de tipo político en el sentido más amplio de la palabra, y la respuesta a lo que demanda el mercado y el sentido común universitario llega tarde y mal a quienes esperan de nosotros una formación de alto nivel, esto es la sociedad a través de nuestros alumnos. Como botón de muestra, basta leer algunos documentos sobre las nuevas tendencias en educación superior en Europa cuyo afán está en homogeneizar estos estudios y cómo han reaccionado de forma distinta los países, sus universidades, las facultades dentro de una misma universidad, etc., cado uno intentando mantener su status quo.

El investigador debe describir con detalle la escena. Incluyendo nombres de usuarios y roles, ubicación física de usuarios, equipos, puntos de red, etc. Si es

posible, se debe registrar información gráfica del lugar (fotos y videos), ya que muchas veces en ellos se encontrarán detalles que posteriormente pueden ser de utilidad en de la investigación, y que también pueden convertirse en evidencia digital: “Serán documentos todas aquellas formas de expresión producto del desarrollo de las técnicas de la comunicación y la informática”, incluyendo, por ejemplo: videos y fotografías.

2.5 Análisis de Evidencia Digital

Análisis detallado de escenarios resultado de acciones no autorizadas que se producen en los sistemas de información de la empresa, identificación del autor, las causas y el método empleado y definición de las medidas para prevenirlos en el futuro.

El análisis forense es la solución ideal para empresas que tienen la necesidad de investigar los incidentes de seguridad informática que se producen en sus sistemas de información. Permite tomar las medidas oportunas para que el suceso no vuelva a ocurrir, además de conocer en profundidad los detalles del mismo.

El análisis forense le ayudará a:

- Descubrir las vulnerabilidades que han hecho posible el ataque.
- Descubrir el origen y el autor del ataque.
- Identificar y determinar las acciones realizadas y las herramientas y métodos utilizados en el ataque.
- Establecer las medidas adecuadas para que la situación no se repita.
- Descubra las vulnerabilidades que han provocado un ataque en su empresa

Con el análisis forense, ayuda a descubrir las vulnerabilidades existentes que hacen posible que sus sistemas de información sean atacados. A través de un análisis exhaustivo del sistema de información de la empresa somos capaces de detectar las lagunas de seguridad que tienen sus sistemas de información como son:

Filtraciones de documentos confidenciales.

- Accesos no autorizados.
- Comportamiento anómalo del sistema.
- Problemas derivados del personal interno.
- Destrucción de datos.
- Uso no autorizado de material.

2.6 Cadena de Custodia

Resulta menester asimilar que el indicio es parte fundamental no sólo de la investigación criminal, sino igualmente lo es en todo el proceso penal acusatorio, habida cuenta que será a través de éste y de su legitimación, que se logrará el convencimiento en el ánimo del juzgador, siempre y cuando, por supuesto, dicho proceso investigativo se sujete a los procedimientos ordinarios que se refieren al registro inicial de la ubicación del indicio en sí, a su detallada y precisa descripción, marcaje numerado, fijación fotográfica, embalaje y etiquetado correspondientes, así como su posterior traslado y correcto llenado de los documentos o formatos legales que amparen tales acciones, vinculándolas con las personas involucradas en ello, procedimientos que en conjunto constituyen un requisito indispensable para el debido cumplimiento de la así llamada cadena de custodia.

Con lo anterior resulta importante entender que, más que una mera “acta” de cadena de custodia, el procedimiento de la cadena de custodia es una realidad del indicio mismo. Por tal motivo, la “cadena de custodia” se demuestra, no tanto se protocola.

Ya sea a nivel federal como también en las diversas entidades, la cadena de custodia hoy en día es más que un documento; es la realidad misma de la confianza que debe ofrecer el indicio. En este sentido incluso algunos jueces de control han rechazado la prueba en la audiencia intermedia por carecer esta del

documento que garantiza la cadena de custodia. De hecho la prueba no fue admitida por el juzgador aún sin que necesariamente hubiese tenido que demostrase que la cadena en efecto había sido violentada.

Con lo establecido hasta el momento, en términos generales podemos entender que la cadena de custodia equivale a la lista de personas que participan en la recabación del indicio, toman posesión de éste y lo tienen bajo su protección, lo que significa que dichas personas involucradas están a cargo de un medio de prueba relacionado con un probable hecho delictivo. Conviene por lo mismo tener presente que el indicio en referencia posteriormente podrá llegar a ser considerado -como se dijera- un medio de prueba dentro del proceso penal, por tal razón es que se anticipa que si su preservación, recabación y protección no fueron de acuerdo a protocolo, las consecuencias derivarán en su ilicitud o nulidad.

Lo anterior se vincula plenamente con lo que establece el artículo 20, apartado a), fracción primera de la Carta Magna, en donde se establece que el propósito del proceso penal tiene por objeto el esclarecimiento de los hechos, es decir, se obliga a los intervinientes a iniciar cualquier actuación con base en los medios de prueba y las normas. Ello habrá de orientar la etapa de investigación, de manera tal que con base en esos elementos será posible determinar qué diligencias se van a desplegar a efecto de esclarecer la notitia criminis, mismas que a su vez deberán estar registradas en la carpeta de investigación, la cual a su vez estará bajo la custodia del Ministerio Público, quien es el director de la investigación y por ende debe sujetarse a determinados principios y reglas procesales (al igual que la policía y los peritos).

En este contexto es posible advertir que las diligencias en la investigación, para que sean practicadas, se requiere identificar previamente si éstas requieren o no de la autorización judicial, así como cumplir con los requisitos legales establecidos en nuestro sistema jurídico. Y lo anterior se debe llevar a cabo sin perder de vista que la investigación se encuentra bajo la dirección del Ministerio Público, con la finalidad de acopiar todos los medios probatorios que demostrarán su hipótesis

fáctica y jurídica, medios probatorios que serán muy importantes en la preparación del caso.

A estas alturas resulta posible identificar que la cadena de custodia es el procedimiento controlado y sistematizado que se aplica a los medios de prueba relacionados con el delito, desde su localización hasta su valoración por los encargados de administrar justicia, y que tiene como fin el no viciarlos con el manejo que de ellos se haga, pretendiendo evitar en todo momento que estos medios de prueba sufran alteraciones, sustituciones, contaminaciones o destrucciones. Lo anterior encuentra su fundamento en el debido proceso cuando se le identifica como "…aquel razonablemente estructurado para averiguar la verdad". Pero también cuando se dice que "…es debido aquel proceso que satisface todos los requerimientos, condiciones y exigencias necesarias para garantizar la efectividad del derecho material."

Con base en lo dicho hasta el momento, al recolectar los medios de prueba lo importante es el significado y el valor que van a tener en el proceso penal acusatorio y oral, por lo que resulta relevante garantizar y preservar este valor por medio de la cadena de custodia, dada la trascendencia jurídica a la que pueden arribar en un momento dado.

Para tales propósitos resulta importante tomar en consideración que lo que en realidad se pretende es proporcionar un grado de certeza en el juzgador, en el sentido de que los indicios recolectados en el espacio físico de la investigación servirán de base para dictar su resolución, y que estos indicios que están frente a él al momento del dictado de sentencia son los mismos que se identificaron, recabaron y protegieron en la etapa de investigación.

Ahora bien, además de lo anterior, la cadena de custodia permite igualmente conocer en cualquier estado del proceso penal, dónde se encuentra el medio de prueba, o quién lo tiene, lo cual lógicamente garantiza la seriedad y transparencia del informe pericial efectuado por el o los expertos en los diferentes laboratorios criminalísticos, entregando los resultados en forma oportuna y con la calidad exigida por las leyes a efecto de constituir adecuadamente la prueba pericial.

En resumen tenemos que la cadena de custodia implica, necesariamente, los siguientes pasos:

1. Identificación del medio de prueba,
2. Recabación del medio de prueba.
3. Protección y preservación del medio de prueba,
4. Individualización del medio de prueba;
5. Transporte apropiado;
6. Entrega controlada.

En consecuencia, la cadena de custodia de los medios de prueba encuentra su fundamento en los siguientes principios probatorios:

- Principio de aseguramiento de la prueba.
- Principio de la licitud de la prueba.
- Principio de la veracidad de la prueba.
- Principio de la necesidad de la prueba.
- Principio de la obtención coactiva de la prueba.
- Principio de la inmediación, publicidad y contradicción de la prueba.

2.7 Informática Forense

También denominado Cómputo Forense, Computación Forense, Análisis Forense Digital o Exanimación Forense Digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnologías de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y

conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El conocimiento del informático forense abarca el conocimiento no solamente del software sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones o pistas de emails, chats.

La importancia de éstos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo.

Adicionalmente, un examinador forense digital, dentro del proceso del cómputo forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo.

Es muy importante mencionar que la informática forense o cómputo forense no tiene parte preventiva, es decir, la informática forense no se encarga de prevenir delitos, para ello que encarga la seguridad informática, es importante tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática.

2.7.1 Dispositivos a Analizar

La infraestructura informática que puede ser analizada puede ser toda aquella que tenga una Memoria (informática), por lo que se pueden analizar los siguientes dispositivos:

- Disco duro de una Computadora o Servidor
- Documentación referida del caso.
- Tipo de Sistema de Telecomunicaciones
- Información Electrónica MAC address
- Logs de seguridad.

- Información de Firewalls
- IP, redes Proxy. lmhost, host, Crossover, pasarelas
- Software de monitoreo y seguridad
- Credenciales de autentificación
- Trazo de paquetes de red.
- Teléfono Móvil o Celular, parte de la telefonía celular,
- Agendas Electrónicas (PDA)
- Dispositivos de GPS.
- Impresora
- Memoria USB
- Bios

2.7.2 Herramientas de Cómputo Forense

- Sleuth Kit (Forensics Kit)
- Py-Flag (Forensics Browser)
- Autopsy (Forensics Browser for Sleuth Kit)
- Dumpzilla (Forensics Browser: Firefox, Iceweasel and Seamonkey)
- dcfldd (DD Imaging Tool command line tool and also works with AIR)
- foremost (Data Carver command line tool)
- Air (Forensics Imaging GUI)
- md5deep (MD5 Hashing Program)
- netcat (Command Line)
- cryptcat (Command Line)
- NTFS-Tools
- Hetman software (Recuperador de datos borrados por los criminales)
- qtparted (GUI Partitioning Tool)
- regviewer (Windows Registry)
- Viewer
- X-Ways WinTrace

- X-Ways WinHex
- X-Ways Forensics
- R-Studio Emergency (Bootable Recovery media Maker)
- R-Studio Network Edtion
- R-Studio RS Agent
- Net resident
- Faces
- Encase
- Snort
- Helix
- NetFlow
- Deep Freeze
- hiren´s boot
- Canaima 3.1
- Mini XP

Herramientas para el análisis de discos duros

- AccessData Forensic ToolKit (FTK)
- Guidance Software EnCase
- Kit Electrónico de Transferencia de datos

Herramientas para el análisis de correos electrónicos

- Paraben
- AccessData Forensic ToolKit (FTK)

Herramientas para el análisis de dispositivos móviles

- AccessData Mobile Phone Examiner Plus (MPE+)

Herramientas para el análisis de redes

- E-Detective - Decision Computer Group
- SilentRunner - AccessData

Herramientas para filtrar y monitorear el tráfico de una red tanto interna como a internet

- USBDeview
- SilentRunner - AccessData
- WhireShark

Capítulo 3

“Legislación”

3.1 Legislación en México

La Cámara de Diputados de México aprobó el miércoles 28 de marzo de 2012 una serie de modificaciones legales que identificarán delitos informáticos como el *hacking*, el uso de engaños para obtener información como contraseñas, así como la obtención y divulgación de información contenida en sistemas informáticos protegidos.

A fines de febrero del mismo año, el diputado del Partido Verde Ecologista de México (PVEM), Rodrigo Pérez-Alonso, integrante de la Comisión de Justicia y uno de los dos proponentes de las reformas (junto con el diputado Juan José Guerra, del mismo partido) habló sobre la historia de esta legislación.

Fueron modificados apartados en varios artículos del Código Penal Federal (los artículos 205, 211, 282, 389 y 390) con el fin de definir una variedad de crímenes informáticos.

De acuerdo con el dictamen aprobado queda tipificado como delito de revelación de secretos, “a quien revele divulgue o utilice indebidamente o en perjuicio de otro, información, conversaciones o mensajes de texto, imágenes o archivos de voz, contenidos en sistemas o equipos informáticos” (Artículo 211 Bis).

Al artículo 211 se le agrega un capítulo entero dedicado a definir y sancionar el acceso ilícito a sistemas y equipos de informática (también llamado *cracking*), por el que se establece una pena de entre tres meses y un año de prisión a quien “sin autorización acceda, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática”. La pena se incrementa en dos terceras partes, en caso de que la penetración impida el uso o acceso del sistema afectado.

El *hackeo* (o penetración sin daño a un sistema informático) también está contemplado en el mismo artículo 211 para el que aplica “un año de prisión y de cien a ciento cincuenta días de multa al que sin autorización conozca o copie

información contenida en sistemas o equipos de informática no protegidos por algún mecanismo de seguridad".

Las modificaciones legales establecen también sanciones de hasta tres años de prisión por amenazas e intimidación a través de sistemas digitales (conocido como *cyberbullying*) y el uso de imágenes de otros como forma de chantaje: "al que amenace a otro (...), haciendo uso o empleo de comunicados o mensajes enviados a través de medios o sistemas informáticos o le amenace con divulgar la información, datos o imágenes obtenidos a través del acceso ilícito a dichos medios o sistemas informáticos" (artículo 282 del Código Penal Federal).

Por primera vez se tipifica el acto de contactar víctimas por internet, como ha ocurrido en varias ocasiones: "el empleo de medios informáticos para generar relación de confianza o amistad con la víctima", según establece la modificación al artículo 205 del Código Penal.

Todos los delitos informáticos se verían agravados si su propósito es realizar operaciones con recursos de procedencia ilícita, lo que se conoce como lavado de dinero, según lo que establece el apartado 211 Bis 5.

3.2 Fundamentación Legal

3.2.1 Constitución Política de los Estados Unidos Mexicanos

Artículo 21.- La imposición de las penas es propia y exclusiva de la autoridad judicial. La investigación y persecución de los delitos incumbe al Ministerio Público, el cual se auxiliara con una Policía que estará bajo su autoridad y mando inmediato. Compete a la autoridad administrativa la aplicación de sanciones por las infracciones de los reglamentos gubernativos y de Policía, las que únicamente

consistirán en multa o arresto hasta por treinta y seis horas; pero si el infractor no pagare la multa que se le hubiese impuesto, se permutara esta por el arresto correspondiente, que no excederá en ningún caso de treinta y seis horas.

Si el infractor fuese jornalero, obrero o trabajador, no podrá ser sancionado con multa mayor del importe de su jornal o salario de un día.

Tratándose de trabajadores no asalariados, la multa no excederá del equivalente a un día de su ingreso.

Las resoluciones del Ministerio Publico sobre el no ejercicio y desistimiento de la acción penal, podrán ser impugnadas por vía jurisdiccional en los términos que establezca la ley.

La Seguridad Pública es una función a cargo de la Federación, el Distrito Federal, los Estados y los Municipios, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones policiales se regirá por los principios de legalidad, eficiencia, profesionalismo y honradez.

La Federación, el Distrito Federal, los Estados y los Municipios se coordinaran, en los términos que la ley señale, para establecer un Sistema Nacional de Seguridad Pública.

3.2.2 Ley Orgánica de la Administración Pública Federal

Artículo 27.- A la Secretaría de Gobernación corresponde el despacho de los siguientes asuntos:

XV. Conducir las relaciones del gobierno federal con el Tribunal Federal de Conciliación y Arbitraje de los Trabajadores al Servicio del Estado;

3.2.3 Ley General del Sistema Nacional de Seguridad Pública

Artículo 1.- La presente Ley es reglamentaria del artículo 21 de la Constitución Política de los Estados Unidos Mexicanos en materia de Seguridad Pública y tiene por objeto regular la integración, organización y funcionamiento del Sistema Nacional de Seguridad Pública, así como establecer la distribución de competencias y las bases de coordinación entre la Federación, los Estados, el Distrito Federal y los Municipios, en esta materia.

Sus disposiciones son de orden público e interés social y de observancia general en todo el territorio nacional.

Artículo 2.- La seguridad pública es una función a cargo de la Federación, el Distrito Federal, los Estados y los Municipios, que tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos y comprende la prevención especial y general de los delitos, la investigación para hacerla efectiva, la sanción de las infracciones administrativas, así como la investigación y la persecución de los delitos y la reinserción social del individuo, en términos de esta Ley, en las respectivas competencias establecidas en la Constitución Política de los Estados Unidos Mexicanos.

El Estado desarrollará políticas en materia de prevención social del delito con carácter integral, sobre las causas que generan la comisión de delitos y conductas antisociales, así como programas y acciones para fomentar en la sociedad valores culturales y cívicos, que induzcan el respeto a la legalidad y a la protección de las víctimas.

Artículo 41. Además de lo señalado en el artículo anterior, los integrantes de las Instituciones Policiales, tendrán específicamente las obligaciones siguientes:

IV. Ejecutar los mandamientos judiciales y ministeriales.

3.2.4 Ley Orgánica de la Procuraduría General de la República

Artículo 22.- Son auxiliares del Ministerio Público de la Federación:

I. Directos:

c) La policía federal, en términos de lo dispuesto por el artículo 21 constitucional.

3.2.5 Código Federal de Procedimientos Penales

Artículo 3.- Las Policías actuarán bajo la conducción y el mando del Ministerio Público en la investigación de los delitos, en términos de lo dispuesto por el artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, y quedarán obligadas a:

II. Practicar las diligencias necesarias que permitan el esclarecimiento de los delitos y la identidad de los probables responsables, en cumplimiento de los mandatos del Ministerio Público;

IV. Participar, en auxilio del Ministerio Público, en la investigación y persecución de los delitos, en la detención de personas o en el aseguramiento de bienes relacionados con la investigación de los delitos, cumpliendo sin excepción los requisitos previstos en los ordenamientos constitucionales y legales aplicables;

VI. Preservar el lugar de los hechos y la integridad de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito. Las unidades de la Policía facultadas para el procesamiento del lugar de los hechos deberán fijar, señalar, levantar, embalar y entregar la evidencia física al Ministerio Público, conforme a las instrucciones de éste y en términos de las disposiciones aplicables;

IX. Emitir los informes, partes policiales y demás documentos que se generen, con los requisitos de fondo y forma que establezcan las disposiciones aplicables, para tal efecto se podrán apoyar en los conocimientos científicos y técnicos que resulten necesarios;

XI. Dar cumplimiento a las órdenes de aprehensión y demás mandatos ministeriales y jurisdiccionales;

XIV. Las demás que le confieran este Código y demás disposiciones aplicables.

En el ejercicio de la función investigadora a que se refiere este artículo, queda estrictamente prohibido a la Policía recibir declaraciones del indiciado o detener a alguna persona, fuera de los casos de flagrancia, sin que medien instrucciones escritas del Ministerio Público, del juez o del tribunal.

Artículo 123 Quintus.- Los peritos se cerciorarán del correcto manejo de los indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito y realizarán los peritajes que se le instruyan. Los dictámenes respectivos serán enviados al Ministerio Público para efectos de la averiguación. La evidencia restante será devuelta al Ministerio Público, quien ordenará su resguardo para posteriores diligencias o su destrucción, si resulta procedente.

Los peritos darán cuenta por escrito al Ministerio Público cuando los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito no hayan sido debidamente resguardados, de conformidad con lo dispuesto en los artículos anteriores y demás aplicables, sin perjuicio de la práctica de los peritajes que se les hubiere instruido.

Artículo 220. .- Siempre que para el examen de personas, hechos u objetos, se requieran conocimientos especiales se procederá con intervención de peritos.

Artículo 223. .- Los peritos deberán tener título oficial en la ciencia o arte a que se refiere el punto sobre el cual deba dictaminarse, si la profesión o arte están legalmente reglamentadas; en caso contrario, se nombrarán peritos prácticos. Cuando el inculpado pertenezca a un grupo étnico indígena, podrán ser peritos prácticos, personas que pertenezcan a dicho grupo étnico indígena.

Artículo 225. .- La designación de peritos hecha por el tribunal o por el Ministerio Público deberá recaer en las personas que desempeñen ese empleo por nombramiento oficial y a sueldo fijo, o bien en personas que presten sus servicios en dependencias del Gobierno Federal, en Universidades del país, o que pertenezcan a Asociaciones de Profesionistas reconocidas en la República.

Artículo 227. .- Los peritos que acepten el cargo, con excepción de los oficiales titulares, tiene obligación de protestar su fiel desempeño ante el funcionario que practique las diligencias.

En casos urgentes la protesta la rendirán al producir o ratificar su dictamen.

Artículo 278 Bis. Las comunicaciones entre particulares podrán ser aportadas voluntariamente a la averiguación previa o al proceso penal, cuando hayan sido obtenidas directamente por alguno de los participantes en la misma.

El tribunal recibirá las grabaciones o video filmaciones presentadas como prueba por las partes y las agregará al expediente.

Las comunicaciones que obtenga alguno de los participantes con el apoyo de la autoridad, también podrán ser aportadas a la averiguación o al proceso, siempre que conste de manera fehaciente la solicitud previa de apoyo del particular a la autoridad. De ser necesario, la prueba se perfeccionará con las testimoniales o periciales conducentes.

En ningún caso el Ministerio Público o el juez admitirán comunicaciones que violen el deber de confidencialidad que establezca la Ley, ni la autoridad prestará el apoyo a que se refiere el párrafo anterior cuando se viole dicho deber.

No se viola el deber de confidencialidad cuando se cuente con el consentimiento expreso de la persona con quien se guarda dicho deber.

Las empresas concesionarias y permisionarias del servicio de telecomunicaciones o de internet, estarán obligadas a colaborar con las autoridades para la obtención de dichas pruebas cuando así lo soliciten. Cualquier omisión o desacato a esta disposición será sancionada por la autoridad, en los términos del artículo 178 del Código Penal Federal.

Carecen de todo valor las comunicaciones que sean obtenidas y aportadas en contravención a las disposiciones señaladas en este Código.

Artículo 278 Ter. Cuando la solicitud de intervención de comunicaciones privadas sea formulada por el Procurador General de la República o los servidores públicos en quienes delegue la facultad, la autoridad judicial otorgará la autorización cuando se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves.

El Ministerio Público será responsable de que la intervención se realice en los términos de la autorización judicial. La solicitud de autorización deberá contener los preceptos legales que la funda, el razonamiento por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos, así como el periodo durante el cual se llevarán a cabo las intervenciones, el cual podrá ser prorrogado, sin que el periodo de intervención, incluyendo sus prórrogas, pueda exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.

En la autorización, el juez determinará las características de la intervención, sus modalidades, límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.

En la autorización que otorgue el juez deberá ordenar que, cuando en la misma práctica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá

presentar ante el propio juez, una nueva solicitud; también ordenará que al concluir cada intervención se levante un acta que contendrá un inventario pormenorizado de las cintas de audio y video que contengan los sonidos o imágenes captadas durante la intervención, así como que se le entregue un informe sobre sus resultados, a efecto de constatar el debido cumplimiento de la autorización otorgada.

El juez podrá, en cualquier momento, verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.

En caso de no ejercicio de la acción penal y una vez transcurrido el plazo legal para impugnarlo, sin que ello suceda, el juez que autorizó la intervención, ordenará que se pongan a su disposición las cintas resultado de las investigaciones, los originales y sus copias, y ordenará su destrucción en presencia del Ministerio Público.

3.2.6 Ley de la Policía Federal

Artículo 8. La Policía Federal tendrá las atribuciones y obligaciones siguientes:

IX. Realizar bajo la conducción y mando del Ministerio Público las investigaciones de los delitos cometidos, así como las actuaciones que le instruya éste o la autoridad jurisdiccional conforme a las normas aplicables;

XIV. Participar en la investigación ministerial, en la detención de personas y en el aseguramiento de bienes que el Ministerio Público considere se encuentren relacionados con los hechos delictivos, así como practicar las diligencias necesarias que permitan el esclarecimiento de los delitos y la identidad de los probables responsables, en cumplimiento de los mandatos del Ministerio Público;

XVII. Preservar el lugar de los hechos y la integridad de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito, dando aviso de inmediato al Ministerio Público. Las unidades facultadas para el procesamiento del lugar de los hechos, deberán fijar, señalar, levantar, embalar y entregar la evidencia física al Ministerio Público, conforme al procedimiento previamente establecido por éste y en términos de las disposiciones aplicables;

XX. Emitir los informes, partes policiales y demás documentos que se generen, con los requisitos de fondo y forma que establezcan las disposiciones aplicables, para tal efecto se podrán apoyar en los conocimientos que resulten necesarios;

XXII. Dar cumplimiento a las órdenes de aprehensión y demás mandatos ministeriales y jurisdiccionales de que tenga conocimiento con motivo de sus funciones;

XXIV. Reunir la información que pueda ser útil al Ministerio Público que conozca del asunto, para acreditar el cuerpo del delito y la probable responsabilidad del imputado, conforme a las instrucciones de aquél;

XLVII. Las demás que le confieran ésta y otras leyes.

Artículo 19. Son deberes de los integrantes:

VII. Desempeñar su misión sin solicitar ni aceptar compensaciones, pagos o gratificaciones distintas a las previstas legalmente. En particular se opondrán a cualquier acto de corrupción y, en caso de tener conocimiento de alguno, deberán denunciarlo;

Artículo 47.- Si se tratare de delito flagrante, la Policía Federal dictará las medidas y providencias necesarias para el debido cumplimiento de lo que en materia de preservación de indicios dispone el Código Federal de Procedimientos

Penales; en todos los casos, y bajo su más estricta responsabilidad, informará de inmediato de lo acaecido al Ministerio Público, y pondrá a su disposición las personas, bienes u objetos relacionados con los hechos.

En estos casos, la Policía Federal actuará de conformidad con los protocolos que al efecto se establezcan conforme a las disposiciones legales aplicables.

3.2.7 Reglamento de la Ley de la Policía Federal

Artículo 5.- La Institución, para el despacho de los asuntos de su competencia, contará con las unidades siguientes:

II. DIVISIONES DE:

d) Científica.

V. COORDINACIONES:

g) Para la Prevención de Delitos Electrónicos.

VII. DIRECCIONES GENERALES:

22) Prevención de Delitos Cibernéticos.

Las áreas de investigación y servicios técnicos especializados a que se refiere el artículo 54 de la Ley, serán:

a) Inteligencia;

b) Investigación;

c) Antidrogas, y

d) Científica.

Además, la Institución contará con un Órgano Interno de Control que se regirá conforme al artículo 107 del presente Reglamento.

El Secretario expedirá los manuales que sean necesarios para la conformación de la estructura y las funciones que deberán desarrollar las Divisiones, Coordinaciones y el Consejo Federal.

La Institución contará para su debido funcionamiento con los servidores públicos siguientes: Comisionado General, Secretario General, jefes de división, coordinadores, coordinadores estatales, directores generales, directores generales adjuntos, directores de área, subdirectores de área, jefes de departamento, analistas y demás personal que se requiera para satisfacer las necesidades del servicio, así como unidades correspondientes, de conformidad con el presupuesto autorizado.

Asimismo, el Comisionado General se auxiliará de una Oficina de Apoyo que se integrará con la Coordinación de Asesores, la Secretaría Particular y demás unidades de apoyo; tendrán las atribuciones que determinen el Comisionado General y la normatividad aplicable. Las unidades administrativas estarán obligadas a auxiliar a la Oficina de Apoyo en términos de sus respectivas atribuciones.

Artículo 10.- Los Integrantes, cualquiera que sea su jerarquía y lugar de adscripción, ejercerán dentro del ámbito de su competencia, las atribuciones siguientes:

IV. Elaborar los informes y demás documentos que se generen con motivo de sus funciones;

Artículo 15.- Corresponde a la División Científica:

III. Auxiliar a las unidades de la Institución y a las autoridades competentes que lo soliciten, en la búsqueda, preservación y obtención de indicios y medios de pruebas necesarios en la investigación de delitos;

IV. Identificar y preservar, en el ámbito de su competencia y conforme a las disposiciones aplicables, la integridad de los indicios, huellas o vestigios

del hecho delictuoso, así como los instrumentos, objetos o productos del delito;

V. Preservar el lugar del hecho delictuoso, fijar, señalar, levantar, embalar y entregar la evidencia física a las autoridades competentes, conforme al procedimiento previamente establecido por éstas y en términos de las disposiciones aplicables;

VI. Proporcionar la información que requieran las autoridades competentes, a fin de apoyar el cumplimiento de las funciones constitucionales de investigación para la prevención y combate de los delitos;

XIV. Supervisar que las opiniones cumplan con las formalidades científicas y técnicas aplicables y acaten la normativa vigente;

Artículo 27.- Corresponde a la Coordinación para la Prevención de Delitos Electrónicos:

V. Observar los procedimientos de cadena de custodia para preservar la integridad y confidencialidad de las evidencias, indicios y pruebas contenidas en medios electrónicos;

XX. Las demás que le confieran este Reglamento, otras disposiciones legales aplicables o aquéllas que le encomiende el inmediato superior de quien dependa.

Artículo 65.- Corresponde a la Dirección General de Prevención de Delitos Cibernéticos:

IV. Preservar los indicios, huellas o vestigios, los instrumentos, objetos o productos del delito materia de su competencia; recolectar, levantar, embalar técnicamente y etiquetarlos, describiendo la forma en que se haya realizado la recolección y levantamiento respectivos, así como las medidas tomadas para asegurar la integridad de los mismos, todo ello en términos del Código Federal de Procedimientos Penales;

V. Aplicar las técnicas científicas y analíticas especializadas en la recuperación de evidencias o indicios digitales;

XIV. Proporcionar, en el ámbito de sus atribuciones, la información que le sea solicitada por las autoridades competentes;

XV. Analizar los sistemas y equipos informáticos, electrónicos y tecnológicos, vinculados con cualquier hecho ilícito, a efecto de prevenir su comisión o investigarlo de conformidad con las disposiciones aplicables;

XXIII. Las demás que le confieran este Reglamento, otras disposiciones legales aplicables o aquéllas que le encomiende el inmediato superior de quien dependa.

3.3 Acuerdo 009/15

Acuerdo por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia.

Capítulo I.- Disposiciones Preliminares

PRIMERO. El presente Acuerdo tiene por objeto establecer las directrices que deberán observar los servidores públicos de la Procuraduría General de la República que intervengan en materia de cadena de custodia de los indicios o elementos materiales probatorios.

SEGUNDO. Para el procedimiento de cadena de custodia se entenderá por:

- **Acordonamiento.** La acción de delimitar el lugar de intervención mediante el uso de cintas, cuerdas u otro tipo de barreras físicas con el fin de preservarlo.
- **Bodega de indicios.** Lugar con características específicas que tiene como finalidad el resguardo de indicios o elementos materiales probatorios para garantizar su integridad.
- **Cadena de custodia.** Sistema de control y registro que se aplica al indicio o elemento material probatorio, desde su localización, descubrimiento o aportación, en el lugar de intervención, hasta que la autoridad competente ordene su conclusión.
- **Dictamen.** Opinión científico técnica que emite por escrito un perito o experto en cualquier ciencia, arte, técnica u oficio, como resultado del examen de personas, hechos, objetos o circunstancias sometidos a su consideración.

- **Documentación.** Registro fidedigno de la condición que guardan lugares, personas, objetos, indicios o elementos materiales probatorios en el lugar de intervención.
- **Elemento material probatorio.** Evidencia física, objeto, instrumento o producto relacionado con un hecho delictivo y que puede constituirse como prueba.
- **Embalaje.** Conjunto de materiales que envuelven, soportan y protegen al indicio o elemento material probatorio con la finalidad de identificarlos, garantizar su mismidad y reconocer el acceso no autorizados durante su traslado y almacenamiento. El embalaje constituye un refuerzo del empaque y, en algunos casos, podrá fungir como empaque del indicio o elemento material probatorio.
- **Empaque.** Todo aquel material que se utiliza para contener, proteger y/o preservar indicios o elementos materiales probatorios permitiendo que llegue íntegro a los servicios periciales, la bodega de indicios o, en
- su caso, a algún otro lugar en condiciones de preservación o conservación.
- **Equipamiento.** Materiales para el procesamiento de indicios o elementos materiales probatorios y equipo de protección personal.
- **Equipo de protección personal.** Cualquier equipo, objeto o instrumento que emplea el interviniente para crear una barrera física entre él, el sitio de intervención, los indicios y las personas involucradas en un hecho, con la finalidad de evitar riesgos a la salud y la perdida, alteración, destrucción o contaminación de los indicios o elementos materiales probatorios.
- **Etiqueta.** Letrero escrito o impreso que se añade al embalaje para identificarlo (**Anexo 5 Formato de etiqueta para embalaje**).
- **Guía.** La Guía de Cadena de Custodia (**Anexo 1 Guía de Cadena de Custodia**).
- **Identificación.** Término utilizado para asignar un número, letra o una combinación de ambos a los indicios o elementos materiales probatorios en el momento de su localización, descubrimiento o aportación, hasta que la autoridad competente ordene la conclusión de la cadena de custodia.
- **Indicio.** Término genérico empleado para referirse a huellas, vestigios, señales, localizados, descubiertos o aportados que pudieran o no estar relacionados con un hecho probablemente delictivo y, en su caso, constituirse en un elemento material probatorio.
- **Lugar de intervención.** Sitio en el que se ha cometido un hecho presuntamente delictivo o en el que se localizan o aportan indicios relacionados con el mismo.
- **Recolección.** Acción de levantar los indicios o elementos materiales probatorios mediante métodos y técnicas que garanticen su integridad.
- **Registro de Cadena de Custodia.** Documento en el que se registran los indicios o elementos materiales probatorios y las personas que intervienen desde su localización, descubrimiento o aportación en el lugar de intervención hasta que la autoridad ordene su conclusión (**Anexo 3 Registro de Cadena de Custodia**).

- **Sellado.** Consiste en cerrar el embalaje empleando medios adhesivos o térmicos que dejen rastros visibles cuando sea abierto indebidamente o sin autorización.

TERCERO. Toda persona que tenga contacto directo con los indicios o elementos materiales probatorios deberá dejar constancia de su intervención en el Registro de Cadena de Custodia.

CUARTO. Son sujetos que intervienen en la aplicación de la cadena de custodia, según corresponda, los siguientes:

I. **Agente del Ministerio Público de la Federación:** verifica que la actuación de los intervinientes en la cadena de custodia se haya realizado dentro de la estricta legalidad y respeto a los derechos humanos. Asimismo, se coordina con otros intervinientes y organiza las actividades de la Policía Federal Ministerial relacionadas con la preservación del lugar de intervención, traslado y entrega de los indicios o elementos materiales probatorios;
II. **Coordinador del grupo de peritos:** revisa las actividades relacionadas con la preservación efectuada por los intervinientes, se coordina con estos y organiza a los peritos en el procesamiento de los indicios o elementos materiales probatorios;
III. **Perito:** es la persona con conocimientos especiales en alguna ciencia, arte, técnica u oficio que ejecuta las actividades del procesamiento de los indicios o elementos materiales probatorios y emite recomendaciones para su traslado. Asimismo, recibe y analiza los indicios o elementos materiales probatorios en las instalaciones de los servicios periciales y emite el informe, requerimiento o dictamen correspondiente;
IV. **Policía Federal Ministerial:** ejecuta las actividades relacionadas con la preservación del lugar de intervención, en su caso, con el procesamiento, traslado y entrega de indicios o elementos materiales probatorios;
V. **Policía Federal Ministerial Responsable**: encargado de la coordinación con otros intervinientes y de la organización de las actividades de la Policía Federal Ministerial relacionadas con la preservación del lugar de intervención, en su caso, con el procesamiento, traslado y entrega de los indicios o elementos materiales probatorios;
VI. **Primer respondiente:** interviene como primera autoridad en el lugar de la probable comisión de un hecho delictivo, y
VII. **Responsable de la recepción de indicios en la bodega:** realiza el registro de los indicios o elementos materiales probatorios durante su recepción, almacenamiento y entrega.

QUINTO. La cadena de custodia deberá comprender las siguientes etapas y en todas ellas se debe llevar a cabo el registro correspondiente:

I. **Procesamiento de los indicios.** Inicia con las técnicas de búsqueda y comprende además las fases de identificación; documentación; recolección; empaque y/o embalaje de los indicios o elementos materiales probatorios y finaliza con su entrega al Policía Federal Ministerial responsable con el Registro de Cadena de Custodia correspondiente. En estas actividades

deberán participar los peritos o, en su caso, la Policía Federal Ministerial haciendo uso del equipamiento necesario.

Tratándose de indicios o elementos materiales probatorios que resulten de la inspección de las personas detenidas en flagrancia, se aplicarán las fases del procesamiento a las que se refiere el párrafo anterior. En el registro de estas actividades deberá participar la Policía Federal Ministerial.

En el caso de muestras de fluido corporal, vello o cabello, exámenes corporales de carácter biológico y extracciones de sangre que resulten de la revisión corporal a la víctima o imputado, deberán participar los peritos.

Cuando se encuentren materiales que por su cantidad o tamaño impliquen un alto costo o peligrosidad por su conservación, sólo entrará en Registro de Cadena de Custodia el muestreo realizado, siendo el resto materia de aseguramiento.

II. **Traslado**. Inicia cuando la Policía Federal Ministerial recibe los indicios o elementos materiales probatorios embalados y finaliza con su entrega a los servicios periciales para su estudio o a las bodegas de indicios para su almacenamiento.

III. **Análisis**. Inicia con la recepción de los indicios o elementos materiales probatorios; continúa con los estudios que se aplican a estos y termina con su entrega para el traslado a la bodega de indicios o, en su caso, a algún otro lugar en condiciones de preservación o conservación. Para el desarrollo de estas actividades el perito deberá utilizar el equipamiento correspondiente.

El personal pericial se abstendrá de recibir indicios o elementos materiales probatorios que no estén embalados, sellados, etiquetados y con Registro de Cadena de Custodia de conformidad con los establecidos oficialmente, salvo que haya existido imposibilidad para ello.

IV. **Almacenamiento.** Inicia con la recepción de los indicios o elementos materiales probatorios en la bodega de indicios o, en su caso, a algún otro lugar en condiciones de preservación o conservación; comprende además el registro, manejo y control de los mismos, y termina con su salida definitiva.

V. **Disposición final.** Inicia con la determinación por la autoridad competente al concluir su utilidad en el procedimiento penal y finaliza con su cumplimiento, mediante el decomiso, destrucción, devolución o abandono u otro.

Capítulo II.- Preservación del lugar de la intervención

SEXTO. La preservación del lugar de intervención, previo a la cadena de custodia, inicia con el arribo del primer respondiente, incluye la evaluación inicial; la protección del lugar y la administración del sitio, y finaliza con su liberación una vez agotados los trabajos de investigación.

SÉPTIMO. La evaluación inicial se llevará a cabo para conocer a detalle las particularidades del lugar y del hecho del que se trata; el nivel de investigación que deberá conducirse; el tipo de indicio o elemento material probatorio que se espera

encontrar y procesar; los riesgos asociados a su pérdida, alteración, destrucción o contaminación; la identificación de los riesgos a la salud y seguridad de las personas que intervienen así como para seleccionar el equipamiento adecuado para la preservación y el procesamiento.

OCTAVO. En el caso de lugares abiertos, con la evaluación inicial se determinará el área que será aislada mediante el acordonamiento. Tratándose de lugares cerrados, se resguardarán puertas y ventanas.

El objetivo de la preservación es evitar la pérdida, alteración, destrucción o contaminación del lugar de la intervención y de sus indicios o elementos materiales probatorios. Como resultado de estas actividades deberá requisitarse el formato correspondiente (**Anexo 2. Formato de entrega-recepción del lugar de intervención**).

Capítulo III.- **Procesamiento de los indicios o elementos materiales probatorios en el lugar de intervención**

NOVENO. La observación comprende la detección de los indicios o elementos materiales probatorios mediante la aplicación de las técnicas de búsqueda que se seleccionen para cada caso.

DÉCIMO. Para la identificación de los indicios o elementos materiales probatorios deberá asignarse un número, letra o combinación de ambos, el cual deberá ser único y sucesivo.

DÉCIMO PRIMERO. La documentación de los indicios o elementos materiales probatorios deberá incluir los registros precisos de su localización en el lugar de intervención así como de sus características generales.

DÉCIMO SEGUNDO. Para garantizar la integridad, autenticidad e identidad de los indicios o elementos materiales probatorios, se realizará la recolección, empaque y/o embalaje de acuerdo con su tipo. Dicho embalaje deberá ser sellado y etiquetado con la finalidad de enviarlo a los servicios periciales, a las bodegas de indicios o en su caso, a algún otro lugar, en condiciones de preservación o conservación.

DÉCIMO TERCERO. El requisitado del Registro de Cadena de Custodia se realizará con el fin de garantizar la continuidad y trazabilidad del indicio o elemento material probatorio y asentar la información del personal que interviene desde su localización, descubrimiento o aportación hasta que la autoridad competente orden su conclusión (**Anexo 3. Registro de Cadena de Custodia**).

Capítulo IV.- **Traslado de los indicios o elementos materiales probatorios**

DÉCIMO CUARTO. La Policía Federal Ministerial trasladará los indicios o elementos materiales probatorios hacia los servicios periciales para su análisis correspondiente y a la bodega de indicios o a algún otro lugar en condiciones de preservación o conservación para su almacenamiento. En su caso, esta actividad deberá realizarse atendiendo a las recomendaciones de los peritos.

DÉCIMO QUINTO. La Policía Federal Ministerial, en el traslado de los elementos materiales probatorios a la sede judicial para su incorporación en audiencia deberá atender las recomendaciones establecidas por los peritos en el Registro de Cadena de Custodia, en términos de sus atribuciones.

Capítulo V.- **Análisis de los indicios o elementos materiales probatorios en los servicios periciales**

DÉCIMO SEXTO. El análisis de los indicios o elementos materiales probatorios inicia con su recepción, comprende su examen y finaliza con su entrega para el traslado a la bodega de indicios o a algún otro lugar en condiciones de preservación o conservación para su almacenamiento.

DÉCIMO SÉPTIMO. Durante el análisis se deberán tomar las medidas necesarias para evitar la contaminación de los indicios o elementos materiales probatorios.

Capítulo VI.- **Almacenamiento de los indicios o elementos materiales probatorios**

DÉCIMO OCTAVO. Los responsables de la recepción de indicios en la bodega y, en su caso, el servidor público que envíe o solicite algún indicio o elemento material probatorio para realizar diligencias ministeriales o judiciales, con el fin de garantizar la integridad y autenticidad de los indicios o elementos materiales probatorios, llevarán a cabo su almacenamiento, mismo que comprenderá el registro, manejo y control de los mismos.

Capítulo VII.- **Disposición final de los indicios o elementos materiales probatorios**

DÉCIMO NOVENO. La disposición final de los indicios o elementos materiales probatorios la determinará la autoridad competente y podrá comprender alguno de los siguientes supuestos, decomiso, devolución, destrucción o abandono.

Capítulo VIII.- **De la Guía**

VIGÉSIMO. Los procedimientos para el cumplimiento y desarrollo del presente Acuerdo se encuentran previstos en la Guía de Cadena de Custodia (**Anexo 1**).

TRANSITORIOS

PRIMERO.- El presente Acuerdo entrará en vigor a los 15 días naturales de su publicación en el Diario Oficial de la Federación.

SEGUNDO.- Se abrogan los Acuerdos A/002/10 y A/078/12, así como todas las disposiciones normativas que se opongan a lo previsto en el presente Acuerdo.

TERCERO.- Se instruye a los servidores públicos previstos en el presente Acuerdo a realizar las acciones necesarias para la aplicación del presente instrumento, en el ámbito de sus atribuciones.

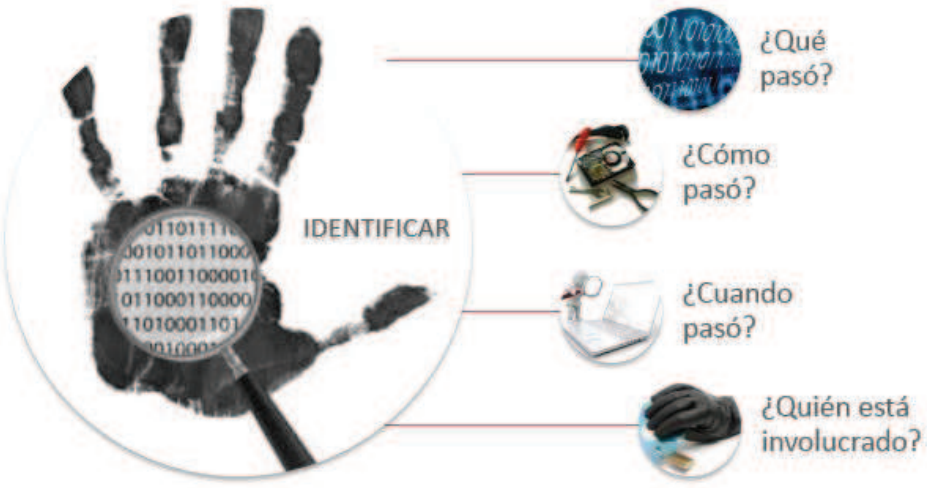
3.4 Cadena de Custodia en México

La autoridad policial deberá asegurar por cualquier medio el lugar de los hechos, lugar de hallazgo o el lugar de enlace mediante el Registro de Cadena de Custodia; documento en el que se registran los indicios o elementos materiales probatorios y las personas que intervienen desde su localización, descubrimiento o aportación en el lugar de intervención hasta que la autoridad ordene su conclusión.

El Registro de Cadena de Custodia son los pasos que deben ser observados por todos los servidores públicos (policías municipales, Policías Federales etcétera) para la debida preservación y procesamiento del lugar de los hechos o del hallazgo y de los indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, producto del delito. En resumen es “el procedimiento de control que se aplica al indicio material, ya sea vestigio, huella, medio de comisión, objeto material o producto relacionado con el delito, desde la localización por parte de una autoridad, policía o Agente del Ministerio Público, hasta que la autoridad competente ordene su conclusión, según se trate de la averiguación previa o el proceso penal”.

Capítulo 4

“Conclusiones y Recomendaciones”



4.1 Conclusión

Hoy de día cualquier tipo de delito puede tener indicios digitales debido a que dichos dispositivos son usados en cada paso de nuestra vida cotidiana y para las personas que infringen la ley también son medios que facilitan cometer estos delitos.

Así como nuestra vida ha pasado al mundo virtual también los delitos se han trasladado a este mundo, pero esto ha hecho que los investigadores tenga que preparase mas debido a los indicios digitales son muy fácil alterar y/o modificar.

En actualidad se usan distintos dispositivos para realizar las tareas cotidianas, en el pasado pocas personas tenia accesos a estas tecnologías pero hoy estudios que se han realizado han demostrado que la mayoría de las personas utiliza más de un dispositivo de comunicación y/o almacenamiento digital, así como que a mas temprana edad se adquieren y se aprender a utilizar estas tecnologías.

También las personas que utilizan estos dispositivos o que realizan los denominado delitos informáticos tienen una motivación diferente, ya no solo es un económicamente si no muchas de las ocasiones es por demostrar que tienen el conocimiento o demostrar fallas en los sistemas informáticos.

La Delincuencia Organizada también utiliza los avances tecnológicos para su beneficio, ya que sus recursos económicos son grandes. Ellos utilizan los medios de comunicación modernos, sistemas informáticos y el Internet, para realizar todos sus movimientos por las bondades y discreción que ofrecen.

La Legislación en México aún falta mucho camino por recorrer para lograr combatir estos delitos y poder sancionarlos, pues muchas de las ocasiones por falta de conocimientos de ellos no se sean sancionadas como debería ser.

Pero lo más importante es que la Sociedad también carece del conocimiento de estos delitos, muchas de las ocasiones las personas incurren en ellos y ni siquiera saben que lo que están haciendo es un delito.

Los movimientos financieros, manejo de datos personales, compras en Internet son muchas blancos de estos delitos debido a que los usuarios no se documentas sobre las políticas de uso de los websites que ofrecen estos servicios y por lo tantos lo proveedores de estos servicio no pueden ayudar al usuario o a la investigación por qué no se respetaron estas políticas.

En México muchos son los delitos en los que se usan los medios informáticos para cometerse y poco a poco se sea venido combatiendo por medios de la prevención, modificaciones en las leyes y procedimientos, capacitaciones a los Funcionarios Encargados de Hacer Cumplir las Leyes y difundir medios de prevención e información de los Delitos Informáticos a la Sociedad; pero aún falta mucho por la parte de la Legislación.

Y algunos delitos como la Pornografía Infantil, a pesar que es un delito que logrado combatir en nuestro país, tomando mucho en cuenta la Evidencia Digital, es un delito que perjudica a la población infantil de la sociedad, el cual deja marcado de por vida a estas personas importantes de la sociedad. No solo que el trauma que pude causar sino porque estos individuos pueden convertirse en el futuro en posibles infractores de este delitos y seguir dañado a la sociedad; por eso es más importante la prevención de este delitos cuidando los hijos e informándolos de ellos de manera que entiendo el peligro que corren en las redes sociales, en Internet.

4.2 Equipos de Comunicación Móvil

Los dispositivos móviles comenzaron siendo un lujo en el que el color, marca, modelo y dimensiones, daban estatus social. A medida que pasó el tiempo, se convirtieron en una necesidad, pues son un medio de comunicación al alcance de casi cualquier bolsillo. Los sociólogos comentan que un dispositivo móvil es parte de la vida de una persona, tanto que al momento de adquirirlo y con la gran variedad existente en el mercado, la mayoría de las personas eligen un dispositivo móvil pensando más en su aspecto físico que en las características internas; no obstante, aseguran que esto va cambiando, pues la tecnología ha sabido

combinar el potencial interno con las características físicas. Esto hace que el número de dispositivos móviles con capacidad de conectarse a Internet se incremente de forma considerable.

El reto de la tecnología no sólo será innovar sobre dispositivos móviles que sean de dimensiones pequeñas para que sea fácil portarlos, o crear dispositivos con materiales que alarguen su vida útil, sino también deberá innovarse para crear dispositivos móviles que brinden seguridad a sus usuarios, esto es: que puedan almacenar información sin la incertidumbre de que cualquier persona en alguna parte del mundo -y sin conocimiento del usuario -, pueda acceder, crear o modificar dicha información.

En muchos países se ha invertido más en tener acceso a la tecnología que en leyes que ayuden a regular su uso. Esta crisis ha provocado que los intrusos diseñen sus ataques desde países en donde una demanda no procedería. En la medida en la que un país no tome en cuenta la importancia del derecho informático, los intrusos seguirán viendo como blanco de ataque los dispositivos móviles, incrementando la amenaza a la que están expuestos los usuarios.

Cada vez más usuarios disponen de conexión a Internet en sus 'smartphones' (Figura 4.1.) y las redes sociales son uno de los servicios estrella. El 73% de quienes utilizan Internet en el móvil acceden a redes sociales desde su terminal.

Figura 4.1.- Dispositivos de Comunicación Móvil “smartphones”.

El 29% de los usuarios de esta nueva tecnología visitan sus redes sociales desde el móvil todos los días. Los nuevos smartphones (con sus tarifas planas) y las aplicaciones relacionadas con estos servicios, han “levantado”; las barreras de uso tradicionales.

Facebook es la red social que presenta un mayor acceso en movilidad (usada por un 60% de usuarios de Internet móvil). Sin embargo, Twitter es la que muestra una tasa más elevada de conversión entre uso en el ordenador convencional y el móvil: del total de usuarios de Twitter, un 40% acceden vía Internet móvil (bajando a un 30% en Facebook).

Tres de cada diez usuarios de Internet en movilidad utiliza algún servicio de geolocalización. Dentro del repertorio, destacan Google Maps y Foursquare.

Figura 4.2.- Servicios de Geolocalización.

Además, destaca el uso de las herramientas de mensajería instantánea en movilidad, Skype y Messenger, y novedades como el chat Whats'app, que comienzan a suponer un “boom”; entre ciertos perfiles.

Figura 4.3.- Herramienta de mensajería instantánea en movilidad.

4.3 Cadena de Custodia

Al analizar someramente aspectos esenciales de la cadena de custodia, es posible advertir que se trata de un mecanismo de control que sirve para preservar los medios de prueba obtenidos en la etapa de investigación, desde el momento en que el Ministerio Público tiene conocimiento de la noticia del hecho delictivo para tomar la decisión sobre el ejercicio o no de la acción penal. Por tanto, se debe entender que la debida preservación de los medios de prueba (indicio, dato de prueba y prueba), implica, por un lado, consolidar el derecho de defensa, y por el otro, integrar la carpeta de investigación. Así pues, a efecto de conciliar ambas exigencias, todo indicio que sea sujeto a cadena de custodia, debe incluir el o los documentos que acrediten la misma. Sin embargo, se deberá de tener especial cuidado por las particularidades de los informes periciales y la prueba pericial.

La lógica de la cadena de custodia, en consecuencia, radica en establecer y demostrar que en el proceso penal los medios de prueba no han sido manipulados, y que los principios de transferencia, relación y causalidad han sido respetados a cabalidad. Lo anterior con la finalidad de acreditar la identidad y el estado original en que fueron hallados los medios de prueba en el espacio físico de la investigación, así como también a efecto de dejar constancia de las condiciones y cambios hechos en dichos medios de prueba por todas y cada una de las personas que participaron en calidad de “custodios” de los mismos.

Es prudente, pues, mencionar que la relevancia de la continuidad de la posesión radica en dejar constancia escrita respecto del cuidado del índico, los estudios efectuados a éste, su almacenaje y traslado en general, con claridad suficiente desde el inicio de la investigación, a efecto de evitar la posible invalidación de la prueba. En tal dinámica es factible establecer que la cadena de custodia tiene como teleología demostrar la identidad, el estado original, las condiciones de su recabación, preservación, embalaje, traslado, licitud y autenticidad de los medios de prueba, evitando con ello su alteración, modificación, destrucción, sustracción, substituciones, e incluso para estar en capacidad de identificar, en su caso,

cualesquiera indebida manipulación a través de la cadena de posesión de dichos medios de prueba por las personas que estaban obligadas a garantizar las condiciones debidas de preservación, así como el tiempo de almacenamiento, refiriendo quiénes tuvieron acceso a los mismos.

También se puede describir la cadena de custodia como: el sistema de control y registro que se aplica al indicio relacionado con el hecho que se presume delictivo, desde su avistamiento o incorporación al proceso penal hasta que la autoridad competente ordene su conclusión. Por lo tanto, no huelga decir que una vez que el Ministerio Público o las policías, o aquellos funcionarios encargados de practicar diligencias de investigación en auxilio del M.P. tengan conocimiento de la probable existencia de un delito, se deberán dictar todas las medidas posibles para impedir que se pierdan, destruyan o alteren los indicios del hecho delictuoso. En este sentido, la cadena de custodia viene a conformar el conjunto de etapas desarrolladas en forma legítima y científica durante la investigación, con el fin de cuidar que no se alteren, o se destruyan los indicios materiales al momento de su recopilación y posterior análisis científico, hasta su incorporación a juicio.

Para concluir es dable entender que, en un sistema de garantías como lo es aquel al que estamos transitando, resulta necesaria la construcción de mecanismos de legalidad que permitan garantizar un debido proceso penal, si entendemos que la preservación de los medios de prueba es parte de una garantía máxima para el imputable y para que la prueba sirva de base para su correcto enjuiciamiento, asegurando, desde luego, que éstos medios de prueba hayan sido obtenidos mediante procesos lícitos. Resulta importante señalar, por lo tanto, que garantizando la igualdad de partes y de contradicción en los dispositivos legales, se les brinda la posibilidad a los intervinientes de tener acceso al material probatorio, para que de la misma manera puedan las partes practicar los análisis que deriven en los correspondientes informes periciales, que en un determinado momento serán la base de la prueba pericial para sustentar sus pretensiones, estableciéndose además la forma de impugnación a la violación de estos derechos frente al Juez.

4.4 Internet para Personas Menores de Edad

Hoy en día los menores se comunican por Internet a través de un sinnúmero de medios –MySpace, Xanga, y Facebook son tan sólo algunos de los más de 200 sitios de Internet para formar Conexiones Sociales. Si agregamos a esa lista mensajes instantáneos, salas de Chat, publicaciones instantáneas en páginas Web, el desafío para los padres se torna abrumador. El Internet es una herramienta poderosa, pero es importante poner en práctica algunas medidas de seguridad y el sentido común. Por ello, hemos tomado la iniciativa de brindarle un marco de referencia para que pueda instruir a sus hijos sobre el uso responsable del Internet.

La clave de la seguridad radica en entender la responsabilidad que conlleva el uso de la tecnología. Es poco probable que usted le diga a su hijo/a que cruce la calle sin antes darle una lección de cómo cruzar la calle de manera segura. Tampoco le daría las llaves de su automóvil a un adolescente que no sabe conducir ni tiene licencia de manejo. Así también las consecuencias de un error de juicio al usar el Internet, podrían ser igual de serias y duraderas.

4.4.1 Consejos para los Usos Comunes del Internet

4.4.1.1 Navegación

La lectura de documentos y visita de páginas Web por Internet se denomina comúnmente como “navegación” o “búsqueda”. Visitar museos virtuales, tener acceso a documentos públicos del estado, leer libros completos, y ver películas cortas, son sólo algunas de las actividades que puede realizar por Internet.

Debe tener en cuenta, sin embargo, que una computadora sin supervisión puede darle a su hijo/a acceso a material inapropiado.

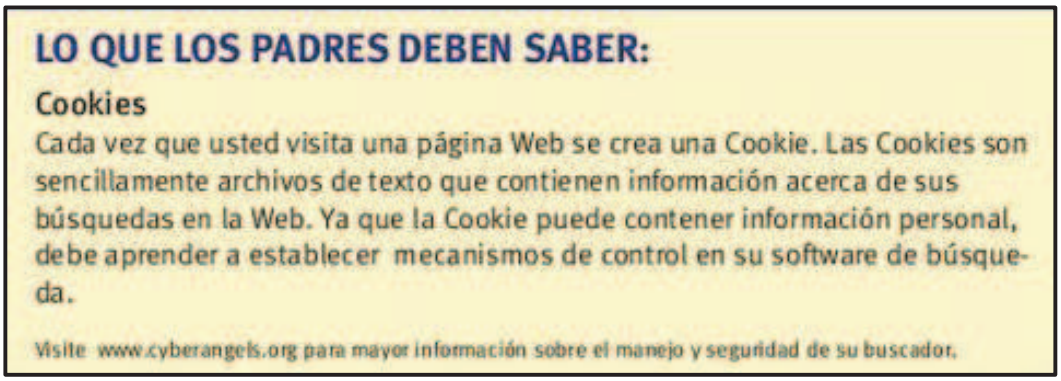


Figura 4.4.- Consejo 1 para Padres o Tutores.

4.4.1.2 Salas de Chat

"Chatear" (o sea, conversar) en línea se ha convertido en la forma preferida de las personas de conectarse a un grupo (sala de Chat) por Internet para compartir intereses similares. Chatear es como conversar, pero en lugar de hablar se escriben las palabras. Normalmente en la sala de Chat hay más de una conversación a la vez. Existen dos clases de salas de Chat– moderadas y no moderadas. El moderador de una sala de Chat hace cumplir las reglas sobre conversaciones apropiadas en una sala de Chat en particular. Recomendamos que solamente permita que sus hijos visiten salas de Chat moderadas que usted haya autorizado.

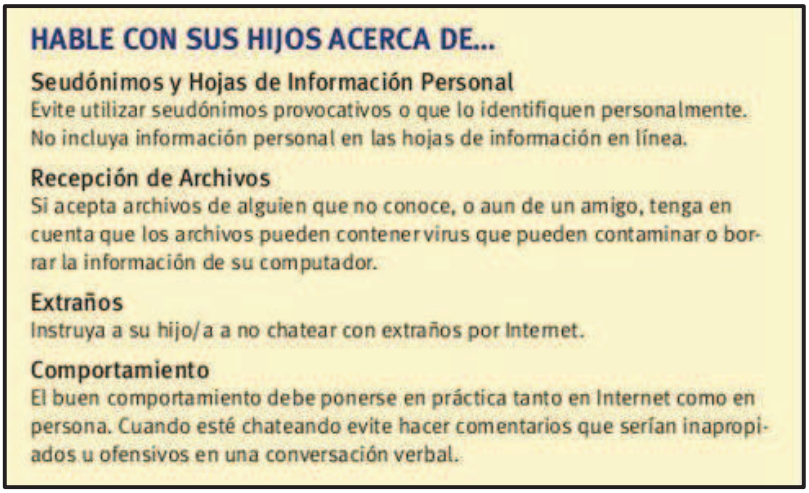


Figura 4.5.- Consejo 2 para Padres o Tutores.

4.4.1.3 E-mail–Correo Electrónico

El correo electrónico es una de las funciones más utilizadas en los computadores con conexión a Internet. Los menores pueden utilizar el Correo Electrónico de manera eficiente de muchas formas – para escribirles a miembros de su familia y amigos, para comunicarse con sus maestros, y aun para escribir a personas famosas y a expertos en varias ramas.

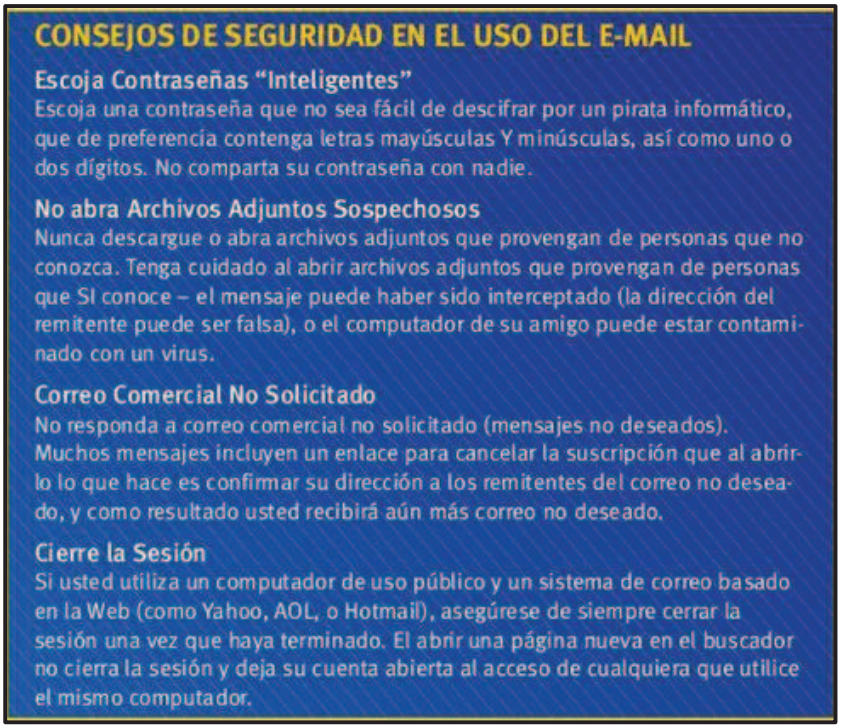


Figura 4.6.- Consejo 3 para Padres o Tutores.

4.4.1.4 Mensajes Instantáneos

Un mensaje instantáneo (IM) permite que dos o más personas se comuniquen escribiéndose unos a otros en tiempo real. Los programas de Mensajes Instantáneos usualmente aparecen en la pantalla como una especie de cuadros, una pantalla dividida, o una pantalla pequeña donde los mensajes van y vienen.

Algunos de estos programas le permiten ver lo que la persona está escribiendo mientras lo hace. Estos programas usualmente son gratuitos, fáciles de descargar, y relativamente fáciles de operar. Muchos programas de Mensajes Instantáneos también le permiten transferir archivos como fotografías, archivos de música (ej. Archivos mp3.).

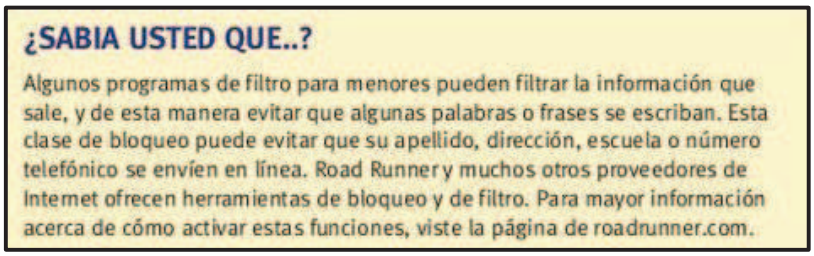


Figura 4.7.- Consejo 4 para Padres o Tutores.

4.4.1.5 Descarga/Uso Compartido de Archivos

Compartir archivos es otra de las actividades preferidas de los adolescentes. Se puede compartir archivos por medio de programas relativamente fáciles de obtener los cuales permiten a los usuarios conectarse directamente a otro computador y copiar (compartir) archivos de música, películas, y otros programas y archivos. El uso del Internet con este fin pone en riesgo la seguridad ya que los archivos pueden estar infectados, o puede que se estén violando algunos derechos de autor.

Para tener en cuenta

Riesgos de Seguridad Existe un riesgo de seguridad real para cada usuario que decida compartir archivos mediante software de tipo P2P (peer to peer) [redes par a par]. El software P2P deja a su computador abierto a otros usuarios, y los archivos que usted descarga pueden estar infectados con virus troyanos (trojans), gusanos informáticos u otros virus, dejando a su computador vulnerable al ataque o al mal uso.

Consecuencias Legales Las personas que compartan copias personales de archivos de películas, televisión, o música en el Internet corren el riesgo de ser demandados legalmente.

4.4.1.6 Conexiones Sociales en la Red: Publicaciones Instantáneas en Páginas Web y Otros Diarios en Internet

Para conocer gente los menores no están limitados solamente a parques infantiles, equipos deportivos o centros comerciales. El mundo a su alrededor es ahora digital y MUY accesible. Los estudiantes pueden abrir cuentas gratuitas de correo electrónico, páginas Web y álbumes de fotos en Internet en sólo minutos. Las publicaciones instantáneas en Páginas Web (Blog abreviado de Web Log o Registro Web) son una especie de diarios en Internet que permiten que las personas compartan sus pensamientos más íntimos con una audiencia mundial. Muchos menores han descubierto que MySpace, Facebook, LiveJournal, y muchos otros sitios de conexiones sociales en la red son una excelente forma de comunicarse con amigos en todo el planeta. Los usuarios pueden publicar mensajes, fotos, y enumerar sus características personales favoritas. Lo que los menores no siempre comprenden es qué tan pública es toda esta información. Como padres, la mejor manera de mantener a sus hijos seguros es recordándoles que el tener una hoja de personalidad en Internet los pone en un posible riesgo. El tener información publicada en Internet implica estar expuesto a todo el mundo.

Temas sobre seguridad en el uso de conexiones sociales en la red que puede comentar con su hijo/a:

- Asuma que todo el mundo tiene acceso a su sitio, y siempre lo tendrá.
- Piense cuidadosamente antes de publicar información o fotos.
- Asuma que los depredadores están observando todo lo que usted escribe y publica.

4.4.1.7 Juegos

Los juegos son otra opción para los jóvenes, y los juegos por Internet pueden ser muy llamativos. La emoción de la competencia, el fácil acceso a nuevos juegos y los excelentes efectos gráficos hacen que los menores disfruten mucho de esta actividad. Pero debido a que también tienen la capacidad de chatear con otros jugadores, usted debe examinar los temas de seguridad con la misma seriedad que en el caso del Chat y los mensajes instantáneos.

CONSEJOS PARA PADRES DE MENORES QUE JUEGAN

Edúquese a sí mismo

- Lea cuidadosamente la censura del juego para obtener recomendaciones en cuanto a la edad apropiada del jugador.
- Lea las cláusulas de privacidad de cada sitio.
- Lea las condiciones de uso aceptable junto con su hijo/a (también puede aparecer como Código de Conducta).

Establezca Límites

Sugerimos limitar el tiempo de juego, jamás permitir el chateo con extraños o el envío de información personal, incluyendo el nombre verdadero de su hijo/a, o donde él o ella viven.

Supervise a su Hijo/a

Lea sus conversaciones en el Chat y comente sobre cualquier tipo de lenguaje o comportamiento inapropiado. Señale ejemplos dentro de la conversación, y dé usted también ejemplos de cómo manejar situaciones potencialmente peligrosas.

Ayúdele a Escoger Seudónimos Seguros

Anime a su hijo/a a escoger seudónimos que no especifiquen su género, y asegúrese de que sus hojas de personalidad no contengan información que los pueda identificar.

Proteja su Contraseña

Instruya a su hijo/a a que nunca comparta su contraseña con un amigo o permita que alguien más tenga acceso a su cuenta.

Sea Parte del Juego

Pídale a su hijo/a que le enseñe a jugar el juego. Este ejercicio anima a su hijo/a enseñar a otros, y le permite identificar posibles riesgos de seguridad mientras juega con él/ella.

Figura 4.8.- Consejo 5 para Padres o Tutores.

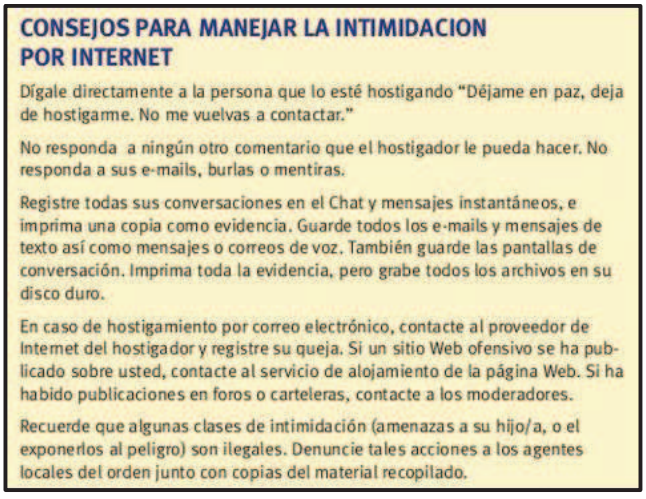
4.4.1.8 Instigación de Menores en el Internet

El mayor peligro para los menores en el Internet es el riesgo de que sean víctimas de un depredador sexual. Los menores sin supervisión pueden entrar a salas de Chat o foros, que, como ha sido demostrado, son sitios usados por pedófilos para seducir a sus víctimas.

Si sospecha que un depredador se ha comunicado con su hijo/a a través del Internet, guarde todos los registros de conversaciones por Internet o por teléfono, y denúncielo. Póngase en contacto con el departamento de policía local si sospecha que su hijo/a se encuentra en peligro inminente.

4.4.1.9 Intimidación, Hostigamiento y Acoso en Internet

La anonimidad en la Web la hace el campo perfecto para que estudiantes se comporten de manera cruel. Un estudio realizado por el Consejo Nacional de Prevención Contra el Crimen (NCPC) en el 2007, demuestra que el 43 por ciento de adolescentes indicaron haber sido víctimas de intimidación por Internet. La intimidación por Internet consiste en la propagación de mentiras y rumores acerca de una persona, insultos y ataques a la sexualidad de un estudiante o a su apariencia física, el engaño a estudiantes para que revelen información personal que después es publicada, y la publicación de información personal identificable o de fotografías sin el consentimiento de la víctima. La tecnología utilizada incluye teléfonos celulares, programas de mensajes instantáneos, salas de Chat, e-mail, sitios Web, encuestas y publicaciones instantáneas en Internet.



CONSEJOS PARA MANEJAR LA INTIMIDACION POR INTERNET

Dígale directamente a la persona que lo esté hostigando "Déjame en paz, deja de hostigarme. No me vuelvas a contactar."

No responda a ningún otro comentario que el hostigador le pueda hacer. No responda a sus e-mails, burlas o mentiras.

Registre todas sus conversaciones en el Chat y mensajes instantáneos, e imprima una copia como evidencia. Guarde todos los e-mails y mensajes de texto así como mensajes o correos de voz. También guarde las pantallas de conversación. Imprima toda la evidencia, pero grabe todos los archivos en su disco duro.

En caso de hostigamiento por correo electrónico, contacte al proveedor de Internet del hostigador y registre su queja. Si un sitio Web ofensivo se ha publicado sobre usted, contacte al servicio de alojamiento de la página Web. Si ha habido publicaciones en foros o carteleras, contacte a los moderadores.

Recuerde que algunas clases de intimidación (amenazas a su hijo/a, o el exponerlos al peligro) son ilegales. Denuncie tales acciones a los agentes locales del orden junto con copias del material recopilado.

Figura 4.9.- Consejo 6 para Padres o Tutores.

4.4.2 Señales de Alerta

Existen varios indicios de que hay problemas. Usted conoce a su hijo/a mejor que nadie, así que siga sus instintos.

Cambio de Pantalla

Si su hijo/a repentinamente cambia de pantalla o apaga el monitor cuando usted entra en la habitación, lo más probable es que él/ella está viendo algo que no quiere que usted vea. Mantenga la calma y pídale que se retire para que usted pueda ver qué hay en la pantalla.

Llamadas Sospechosas

Si repentinamente su hijo/a empieza a recibir llamadas telefónicas de adultos extraños (o aun de otros menores) puede que haya problemas. Instale un programa de identificación de llamadas para que sepa de donde provienen las llamadas y pídale a su hijo/a que explique las llamadas.

A Altas Horas de la Noche

Si su hijo/a está despierto/a escribiendo a altas horas de la noche, él/ella puede estar chateando en el Internet. Esta actividad debe limitarse a horas y lugares donde haya supervisión.

Ingreso Repentino de Dinero Efectivo

Si repentinamente su hijo tiene más dinero del que debería, o aparece con ropa que no le es familiar a ud., o recibe regalos que no puede explicar, este puede ser un indicio de alguna actividad sospechosa. Los pedófilos a menudo gastan una gran cantidad de dinero para entablar una relación con un menor.

Inusualmente Molesto por una Interrupción en el Internet

No es normal que alguien se ponga a llorar o se enfade demasiado porque el Internet no funciona por una o dos horas. Esta clase de comportamiento representa una alerta roja y debe dar lugar a un diálogo abierto con su hijo/a.

Distanciamiento de Familiares y Amigos

Los pedófilos se empeñan en crear una brecha entre los hijos y las personas que los cuidan y apoyan. Mientras más distanciamiento haya entre el hijo y su familia, más fácil es que el depredador pueda entablar una relación.

4.4.3 Consejos para Padres– Hable con su Hijo/a

No espere que los programas de software hagan su trabajo

Los programas que filtran y bloquean información pueden ser parte de su plan de seguridad en el Internet en casa, pero no reemplazan la participación de un padre bien informado e involucrado.

Tome la iniciativa

Asista a clases de seguridad en el Internet y pase tiempo escuchando y hablando con otros padres que comparten la misma preocupación.

Participe con su hijo/a en el Internet

Familiarícese con los servicios y programas que su hijo/a utiliza.

Planifique con anticipación

Hable con su hijo/a acerca de las cosas que puede encontrar en Internet y lo que él/ella puede hacer al respecto.

Estimule otros interese de su hijo/a

Los menores no deben pasar demasiado tiempo en el Internet. Anímelos a participar en otro tipo de actividades también.

Piense en el "centro comercial"

Usted no dejaría solo a su hijo/a en el centro comercial, así que tampoco lo deje solo en el Internet. Recuerde mantenerlo supervisado.

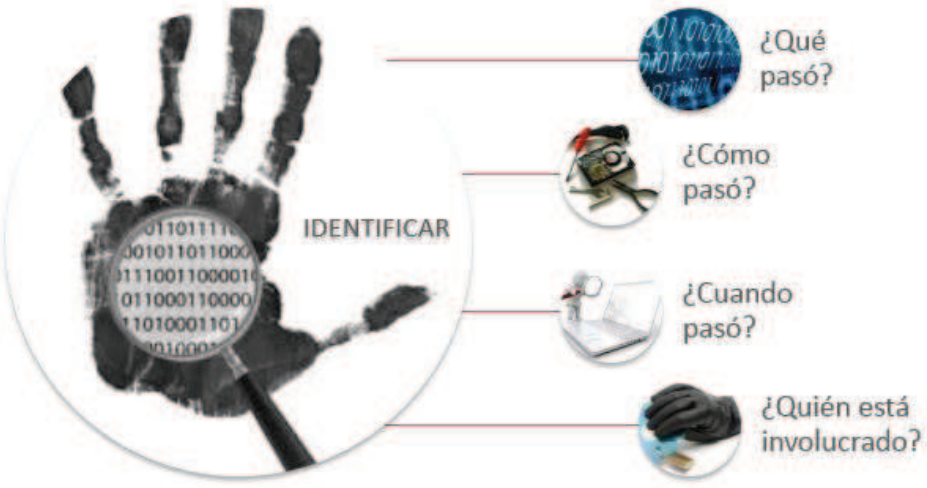
Hay un tiempo y una hora para todo

Mantenga su computador en una habitación familiar–donde pueda supervisarlo. Dele acceso a su hijo/a al Internet solamente cuando usted se encuentre en casa y esté despierto/a.

Explore el Internet

Tómese el tiempo para explorar el uso de su computador y del Internet. Ambos son herramientas valiosas que pueden enriquecer las vidas de todos los miembros de su familia. Mientras más conocimiento tenga, mejor puede proteger a su familia.

“Referencias”



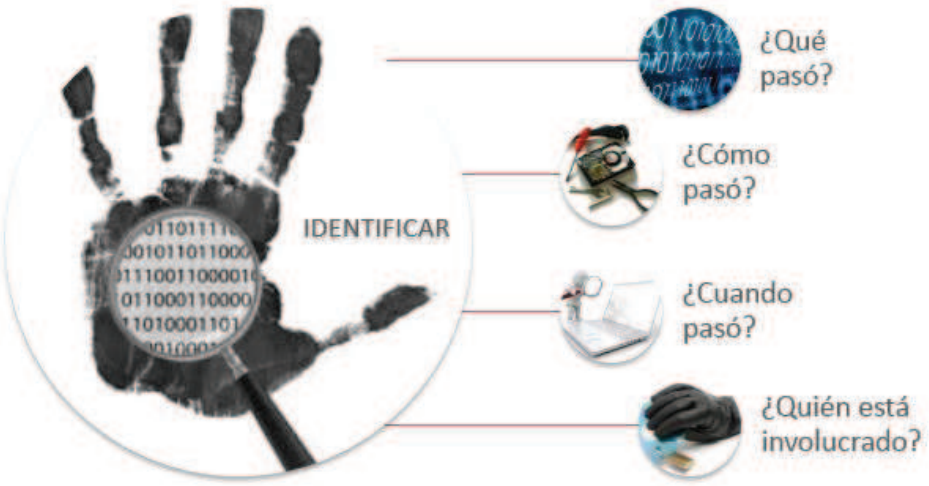
Referencias:

- **ACUERDO A/009/15 por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia.** Publicada el 12 de febrero de 2015.
- **Ayers Rick, Cilleros Nicolas, Daniellou Ronan, Jansen Wayne. (s.f.). "Cell Phone Forensic Tools: An Overview and Analysis".** Recuperado el 27 de febrero de 2015, del National Institute of Standard and Technology (NISTIR) 7387: http://csrc.nist.gov/publications/nistir/nistir-7387.pdf
- **Código Federal de Procedimientos Penales**, publicada en el Diario Oficial de la Federación el 02 de enero de 1934, Última reforma publicada el 30 de agosto de 2014.
- **Constitución Política de los Estados Unidos Mexicanos**, Constitución publicada en el Diario Oficial de la Federación el 5 de febrero de 1917, Última reforma publicada el 07 de julio de 2014.
- **Delito Informático.** (s.f.). Recuperado el 15 marzo de 2015, de http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico
- **Delitos Informáticos.** Recuperado el 20 de febrero de 2015, de la Universidad de Concepción, Republica de Chile: http://www2.udec.cl/contraloria/docs/materias/delitosinformaticos.pdf
- **Jansen Wayne. (s.f.). "Guidelines on Cell Phone Forensics".** Recuperado el 27 de febrero de 2015, del National Institute of Standard and Technology: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.
- **La Importancia de la Evidencia Digital y el Análisis Forense Digital. (s.f.).** Recuperado el 02 febrero de 2015, de http://www.bsecure.com.mx/opinion/la-importancia-de-la-evidencia-y-el-analisis-forense-digital/
- **Ley de la Policía Federal**, publicada en el Diario Oficial de la Federación el 01 de junio de 2009, Última reforma publicada el 25 de mayo de 2011.

- **Ley de Protección de la Información y de los Datos.** Recuperado el 20 de febrero de 2015, de la Alcaldía de Bogotá, Colombia: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
- **Ley Especial de Delitos Informáticos.** Recuperado el 20 de febrero de 2015, del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela: http://www.tsj.gob.ve/legislacion/ledi.htm
- **Ley General de Telecomunicaciones, Tecnologías de Información y comunicación.** Recuperado el 20 de febrero de 2015, del Gobierno de Bolivia: http://www.gacetaoficialdebolivia.gob.bo/normas/view/139394
- **Ley General del Sistema Nacional de Seguridad Pública**, publicada en el Diario Oficial de la Federación el 02 de enero de 2009, Última reforma publicada el 29 de octubre de 2013.
- **Ley Orgánica de la Administración Pública Federal**, publicada en el Diario Oficial de la Federación el 29 de diciembre de 1976, Última reforma publicada el 27 de enero de 2015.
- **Ley Orgánica de la Procuraduría General de la República**, publicada en el Diario Oficial de la Federación el 29 de mayo de 2009, Última reforma publicada el 05 de mayo de 2013.
- **Modificación al Código Penal sobre la Incorporación de los Delitos Informáticos.** Recuperado el 20 de febrero de 2015, de Información Legislativa, Centro de Documentación e Información, Ministerio de Economía y Finanzas Públicas, de la Nación Argentina: http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm
- **Reglamento de la Ley de la Policía Federal**, publicada el 17 de mayo de 2010.
- **Seguridad en Informática. (s.f.).** Recuperado el 10 febrero de 2015, de http://www.revista.unam.mx/vol.9/num4/art26/int26.htm
- **Seguridad en la Red. (s.f.).** Recuperado el 10 febrero de 2015, de http://www.seguridadenlared.org/

- **Seguridad Web. (s.f.).** Recuperado el 12 febrero de 2015, de http://www.seguridadweb20.es
- **Suárez Gutiérrez, Carlos. (s.f.). "Celulares y privacidad" ENTER@TE. Año 6 Núm. 6 2007.** Recuperado el 27 de febrero de 2015, de la Universidad Nacional Autónoma de México: http://www.enterate.unam.mx/Articulos/2007/junio/art4.html.

“Anexos”


IDENTIFICAR
¿Qué pasó?
¿Cómo pasó?
¿Cuando pasó?
¿Quién está involucrado?

Anexo 1.- Guía de Cadena de Custodia

Anexo 1

GUÍA DE CADENA DE CUSTODIA

PROCURADURÍA GENERAL DE LA REPÚBLICA

PRESENTACIÓN

A la luz de la entrada en vigor del sistema de justicia penal acusatorio, las autoridades de procuración y administración de justicia deben de estar preparadas para desempeñar una serie de atribuciones en aras del adecuado desempeño de su labor como servidores públicos. Particularmente, la actuación de la Procuraduría General de la República en materia de investigación de los delitos tiene una gran relevancia, y por tal motivo, la exigencia en cuanto al manejo que se le debe dar a los indicios o elementos materiales probatorios que puedan servir de prueba durante el procedimiento penal.

En ese sentido y en virtud de la expedición del Acuerdo A/009/15 resulta necesario desarrollar las actividades relacionadas con la documentación del indicio o elemento material probatorio a través del procedimiento de cadena de custodia que garantice su integridad, mismidad y autenticidad.

Derivado de lo anterior, la finalidad de esta Guía, consiste en ser un instrumento que articule los esfuerzos de todos servidores de la Procuraduría General de la República que participan durante la preservación del lugar de intervención y el procesamiento de los indicios o elementos materiales probatorios; fortalezca los conocimientos y las habilidades de los servidores públicos, y que, sobre todo, genere las bases para la estandarización de las actividades que garanticen la trazabilidad y continuidad de los indicios o elementos materiales probatorios en la cadena de custodia.

OBJETIVOS

General

Garantizar la mismidad y autenticidad de los indicios o elementos materiales probatorios, mediante los registros que demuestren la continuidad y trazabilidad de la cadena de custodia, con la finalidad de constituirse como prueba.

Específicos

- Homologar las actuaciones de la Policía Federal Ministerial y de la Coordinación General de Servicios Periciales.
- Establecer los tramos de control entre la Policía Federal Ministerial y la Coordinación General de Servicios Periciales.
- Fortalecer la comunicación y coordinación entre los intervinientes.
- Aplicar las técnicas de protección y/o preservación adecuadas desde la localización hasta el destino final de los indicios o elementos materiales probatorios.
- Determinar las actividades y responsabilidades de los intervinientes.
- Determinar el proceso de documentación de las actividades de los intervinientes.

POLÍTICAS DE OPERACIÓN

- Para el desarrollo de la cadena de custodia deberán establecerse los mecanismos de coordinación entre los diferentes intervinientes.
- Todas las actividades desarrolladas durante el procesamiento, traslado, análisis, almacenamiento y presentación de los indicios o elementos materiales probatorios deberán constar en el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15).
- Todo acto de entrega-recepción de los indicios o elementos materiales probatorios entre los intervinientes en el procesamiento, traslado, análisis, almacenamiento y presentación de los indicios o elementos materiales probatorios deberá constar en el "Registro de Cadena de Custodia" y en el "Formato de entrega-recepción de los indicios o elementos materiales probatorios" (anexos 3 y 4 del Acuerdo A/009/15).

- El almacenamiento de los indicios o elementos materiales probatorios deberá estar garantizado por la bodega de indicios.
- Los responsables de la recepción de indicios deberán dejar registro de su intervención en la cadena de custodia, asumiendo las responsabilidades que les correspondan.
- El traslado de los indicios o elementos materiales probatorios deberá realizarse bajo condiciones de seguridad desde una perspectiva integral.
- Cuando un indicio o elemento material probatorio se pierda, altere o destruya, el interviniente en la cadena de custodia deberá informarlo de manera inmediata al agente del Ministerio Público de la Federación y lo asentará en el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15).
- Cuando un indicio o elemento material probatorio sea aportado a través de algún agente de la Policía Federal Ministerial, éste deberá incorporarlo inmediatamente al "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15).
- Verificar que la información relativa a los indicios o elementos materiales probatorios que se asienta en el "Registro de Cadena de Custodia", el Informe Policial Homologado y el Informe de Puesta a Disposición es la misma (Anexo 3 del Acuerdo A/009/15).

GENERALIDADES

La presente Guía desarrolla las principales acciones que deberán realizar los servidores públicos que intervengan en el procedimiento penal para el debido cumplimiento de las disposiciones en materia de cadena de custodia.

DESTINATARIOS DE LA GUÍA

Esta Guía está dirigida a los Ministerios Públicos de la Federación, los Policías Federales Ministeriales y Peritos que intervienen en el procedimiento penal en materia de cadena de custodia.

PRESERVACIÓN DEL LUGAR DE INTERVENCIÓN

DEFINICIÓN: acciones de la Policía Federal Ministerial para custodiar y vigilar el lugar de intervención con el fin de evitar cualquier acceso indebido que pueda causar la pérdida, destrucción, alteración o contaminación de los indicios o elementos materiales probatorios.

LÍMITES: inicia con el arribo al lugar de intervención del primer respondiente y finaliza con la liberación del sitio una vez agotados los trabajos de investigación.

RESPONSABLES: Policía Federal Ministerial como primer respondiente y coordinador del grupo de peritos.

ACTIVIDADES RELEVANTES:

a) Arribo al lugar.- Los primeros respondientes realizarán las acciones tendentes a salvaguardar la vida, la salud, la libertad y la propiedad de las personas e impedir la pérdida, alteración, destrucción o contaminación de los indicios o elementos materiales probatorios. Para tal efecto deberán:

- Informar al agente del Ministerio Público de la Federación;
- Atender o canalizar las emergencias;
- Brindar seguridad en el sitio, y
- Detener e inspeccionar personas.

b) Evaluación inicial del sitio.- Se llevará a cabo para conocer a detalle las particularidades del lugar de intervención y del hecho de que se trata; el nivel de investigación que deberá conducirse; el tipo de indicio o elemento material probatorio que se espera encontrar y procesar; los riesgos que pueden ocasionar su pérdida, alteración destrucción o contaminación; identificar los riesgos a la salud y seguridad de las personas que intervienen, y seleccionar el equipamiento adecuado. Para tal efecto deberán:

- Documentar el lugar de intervención (ubicación, características, fecha y hora);
- Detectar riesgos (químicos, biológicos, físicos o condiciones ambientales);
- Identificar los límites iniciales del lugar de intervención y del acordonamiento;

- Identificar lugares conexos que también deberán ser procesados por grupos multidisciplinarios de especialistas, y

- Priorizar el procesamiento anticipado de los indicios o elementos materiales probatorios cuando existan riesgos inmediatos de pérdida, destrucción, alteración o contaminación.

c) Protección del lugar.- Los primeros respondientes realizarán las actividades para resguardar el lugar previniendo su modificación. Para tal efecto deberán:

- Procesar los indicios de manera inmediata cuando existan riesgos inminentes de pérdida, alteración, destrucción o contaminación;

- Restringir el acceso al personal no esencial;

- Documentar las actividades de los intervinientes;

- Acordonar el lugar (dependerá del tipo de hecho, características del lugar y recursos disponibles, si es necesario, esta actividad podrá realizarse por niveles), y

- Establecer la ruta única de entradas y salidas con la finalidad de evitar desplazamientos que pueden causar modificaciones sustanciales, innecesarias o contaminación.

DOCUMENTOS:

- "Formato de entrega-recepción del lugar de Intervención" (Anexo 2 del Acuerdo A/009/15), y

- "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15) (Este formato sólo deberá ser requisitado cuando por riesgo inmediato de pérdida, alteración, destrucción o contaminación de indicios se requiera la documentación y recolección inmediata de los indicios o elementos materiales probatorios del sitio).

ETAPAS DE LA CADENA DE CUSTODIA

I. PROCESAMIENTO

DEFINICIÓN: procedimiento realizado por personal especializado para detectar, preservar y conservar los indicios o elementos materiales probatorios desde su localización, descubrimiento o aportación, hasta su entrega a la autoridad responsable de su traslado comprendiendo las siguientes etapas, identificación, documentación, recolección, empaque y/o embalaje.

LÍMITES: inicia con las técnicas de búsqueda de los indicios o elementos materiales probatorios y finaliza con su entrega a la autoridad responsable del traslado.

RESPONSABLES: peritos y policías federales ministeriales.

ACTIVIDADES RELEVANTES

I.1. Observación, identificación y documentación:

- **Observación:** detectar o reconocer los indicios o elementos materiales probatorios mediante la aplicación de las técnicas de búsqueda seleccionadas, como son líneas o franjas, criba, espiral, entre otras.

- **Identificación:** asignar número, letra o ambos al indicio o elemento material probatorio, el cual deberá ser único y sucesivo.

- **Documentación:** asentar la información relacionada con la ubicación y características de los indicios o elementos materiales probatorios en el lugar de la intervención, en el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15). Para esta actividad se deben emplear complementariamente diversos métodos como son el fotográfico, videográfico, planimétrico o croquis simple, escrito, etc. Siempre que sea posible la documentación fotográfica y videográfica deberá realizarse antes, durante y después de aplicar las técnicas en cada etapa del procesamiento.

I.2. Recolección; empaque y/o embalaje; sellado y etiquetado:

- **Recolección**: emplear el equipamiento necesario para levantar el indicio o elemento material probatorio de acuerdo a su tipo, con el fin de garantizar su integridad, autenticidad e identidad. Si al recolectar un indicio éste se daña, se deberá especificar dicha condición en el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15).

- **Empaque y/o embalaje**: colocar los indicios o elementos materiales probatorios en bolsas, envases, cajas u otro contenedor nuevo de acuerdo con su tipo considerando las condiciones especiales que sean necesarias para garantizar su integridad física durante el traslado. Asimismo, deberá realizarse de manera individual, salvo cuando estos puedan ser agrupados de acuerdo con su tipo, y siempre que esta actividad no cause pérdida, daño, alteración o contaminación de los indicios o elementos materiales probatorios.

- **Sellado:** utilizar cintas de seguridad, medios térmicos o cualquier otro con el fin de reconocer accesos no autorizados. Cuando se empleen cintas de seguridad deberá cruzarse la firma en la cinta y en el embalaje.

- **Etiquetado**: identificar los indicios o elementos materiales probatorios una vez que han sido embalados, por lo menos, con los siguientes datos (Anexo 5 del Acuerdo A/009/15):

- Número de folio o equivalente;
- Número de carpeta de investigación;
- Identificación del indicio;
- Fecha y hora de la recolección, y
- Tipo de indicio o elemento material probatorio.

I.3. Inventario y recomendaciones para el traslado de los indicios o elementos materiales probatorios:

- **Inventario:** contabilizar y asegurar que los indicios o elementos materiales probatorios recolectados estén documentados en el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15) y en el "Formato de entrega-recepción de indicios o elementos materiales probatorios" (Anexo 4 del Acuerdo A/

009/15).

- **Recomendaciones:** emitir indicaciones para el manejo y traslado de los indicios o elementos materiales probatorios con el fin de garantizar la integridad de los mismos (Anexo 3 del Acuerdo A/009/15), las cuales deben contemplar:

- Condiciones del traslado (origen-destino);
- Condiciones ambientales;
- Tipo de indicios o elementos materiales probatorios;
- Tiempo para iniciar el traslado (mínimo);
- Tipo de transporte para el traslado, e
- Indicaciones o etiquetas que refieran el contenido y la forma en que el paquete debe transportarse (frágil, líquido, tóxico, posición, en su caso).

- Todas las actividades del procesamiento deberán realizarse con el equipamiento (materiales y equipo de protección personal) necesario para la búsqueda; identificación; documentación; recolección; empaque y/o embalaje; sellado, y etiquetado de los indicios o elementos materiales probatorios objeto de estudio.

- El acto de entrega-recepción entre el personal especializado en el procesamiento de los indicios o elementos materiales probatorios y el encargado del traslado preferentemente deberá realizarse en el lugar de intervención al concluir el procesamiento.

- Cuando por causas de fuerza mayor, seguridad u orden público no sea posible concluir el procesamiento de los indicios o elementos materiales probatorios en el lugar de intervención, éste podrá concluirse en lugar diferente.

DOCUMENTOS:

- "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15), y

- "Formato de la entrega-recepción de los indicios o elementos materiales probatorios" (Anexo 4 del Acuerdo A/009/15).

II. TRASLADO

DEFINICIÓN: actividad que tiene como finalidad transportar los indicios o elementos materiales probatorios debidamente embalados, del lugar de intervención hacia los servicios periciales, a la

bodega de indicios o en su caso, a algún otro lugar en condiciones de preservación o conservación en cumplimiento a las recomendaciones de los especialistas.

LÍMITES: inicia cuando el Policía Federal de Investigación encargado del traslado recibe los indicios o elementos materiales probatorios y finaliza con su entrega en los servicios periciales para los estudios correspondientes, en la bodega o en su caso, a algún otro lugar en condiciones de preservación o conservación de indicios para su almacenamiento.

RESPONSABLE: Policía Federal Ministerial.

ACTIVIDADES RELEVANTES:

II.1. Entrega para almacenamiento transitorio:

- Cuando por causas de fuerza mayor o recomendaciones logísticas no puedan trasladarse los indicios o elementos materiales probatorios a la brevedad hacia los servicios periciales, estos deberán ser canalizados a las bodegas de indicios para su almacenamiento o en su caso, a algún otro lugar en condiciones de preservación o conservación.

- Tan pronto como cesen las causas que ocasionaron el impedimento de traslado y se reúnan las condiciones logísticas necesarias para realizarlo con seguridad, éste deberá efectuarse inmediatamente para practicar los análisis correspondientes en los servicios periciales.

- Todo indicio o elemento material probatorio se entregará embalado sellado, etiquetado y con el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15).

II.2. Entrega en los servicios periciales:

- La Policía Federal Ministerial entregará los indicios o elementos materiales probatorios, embalados, sellados, etiquetados y con el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15).

DOCUMENTOS:

- "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15), y

- "Formato de entrega-recepción de los indicios o elementos materiales probatorios" (Anexo 4 del Acuerdo A/009/15).

III. ANÁLISIS

DEFINICIÓN: Estudios que se realizan a los indicios o elementos materiales probatorios con el fin de determinar sus características relevantes para la investigación.

LÍMITES: Tratándose de análisis en los servicios periciales, inicia con la recepción de los indicios o elementos materiales probatorios; continúa con los estudios que se aplican a estos y termina con su entrega para el traslado a la bodega de indicios. Para el desarrollo de estas actividades el perito deberá utilizar el equipamiento correspondiente.

RESPONSABLE: Perito.

ACTIVIDADES RELEVANTES:

III.1. Recepción y análisis en el laboratorio:

- Recibir los indicios o elementos materiales probatorios únicamente cuando el embalaje cumpla con los requisitos establecidos y cuenten con el "Registro de Cadena de Custodia" debidamente requisitado (Anexo 3 del Acuerdo A/009/15).

- Abrir el embalaje cuando se esté autorizado para ello, verificar que los registros de cadena de custodia acompañen a los indicios o elementos materiales probatorios y documentar cualquier cambio o alteración en el embalaje o en su contenido.

- Requisitar las actividades relacionadas con la continuidad y trazabilidad de los indicios o elementos materiales probatorios en el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15).

- Registrar los ingresos y salidas de la bodega de indicios.

- Abrir el embalaje por lado diferente al que se encuentra sellado. Siempre que se requiera el cambio de embalaje deberá documentarse en el campo de observaciones del apartado "Continuidad y Trazabilidad" del "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15). Conservar el embalaje

siempre que sea pertinente y no se ponga en riesgo la salud de las personas que lo manipulan, en caso contrario, informarle al agente del Ministerio Público de la Federación para determinar lo conducente.

- Una vez que se concluyan los estudios solicitados deberán entregarse los indicios embalados, sellados, etiquetados y con el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15) a la autoridad responsable de su traslado a la bodega de indicios.

- Tratándose de peritajes irreproducibles se estará a lo dispuesto por el artículo 274 del Código Nacional de Procedimientos Penales y se documentará esta circunstancia en el "Registro de Cadena de Custodia" correspondiente (Anexo 3 del Acuerdo A/009/15).

- Los indicios o elementos materiales probatorios sólo permanecerán en la bodega de indicios el tiempo estrictamente necesario para su análisis.

DOCUMENTOS:

- "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15), y

- "Formato para la entrega-recepción de indicios o elementos materiales probatorios" (Anexo 4 del Acuerdo A/009/15).

IV. ALMACENAMIENTO EN BODEGA DE INDICIOS

DEFINICIÓN: es el conjunto de actividades necesarias para depositar los indicios o elementos materiales probatorios en lugares adecuados que garanticen su conservación hasta que la autoridad determine su destino.

LÍMITES: inicia cuando el responsable de la recepción de indicios en la bodega recibe estos o los elementos materiales probatorios y finaliza con la salida definitiva de la bodega de indicios.

RESPONSABLE: **el servidor público que recibe los indicios en la bodega.**

ACTIVIDADES RELEVANTES:

IV.1. Recepción y custodia en la bodega de indicios:

- Registrar el ingreso de indicios, sus salidas temporales y definitivas.

- Los indicios o elementos materiales probatorios deberán estar acompañados del "Registro de Cadena de Custodia"correspondiente (Anexo 3 del Acuerdo A/009/15).

- Observar y documentar las condiciones en que se reciben los indicios o elementos materiales probatorios en el"Registro de Cadena de Custodia".

- Colocar los indicios o elementos materiales probatorios en áreas que cumplan con especificaciones de almacenamiento de acuerdo a su tipo.

- El responsable de la bodega de indicios instruirá al personal encargado de su resguardo con el fin de que reporte cualquier anomalía o circunstancia que ponga en riesgo su integridad.

- Observar las recomendaciones de los especialistas para el manejo de los indicios o elementos materiales probatorios al momento de su almacenaje.

- La bodega de indicios debe contar con áreas específicas para el almacenaje y reconocimiento de los indicios o elementos materiales probatorios.

DOCUMENTOS

- "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15), y

- "Formato de entrega-recepción de los indicios o elementos materiales probatorios" (Anexo 4 del Acuerdo A/009/15).

V. TRASLADO A SALAS DE AUDIENCIA

DEFINICIÓN: actividad que se realiza con el fin de presentar indicios o elementos materiales probatorios ante el órgano jurisdiccional, en caso de ser procedente.

LÍMITES: inicia con la salida de los indicios o elementos materiales probatorios de la bodega de indicios, incluye el traslado, su incorporación en la audiencia, su reingreso a la bodega de indicios y finaliza con la determinación judicial.

RESPONSABLES: el servidor público que recibe los indicios en la bodega, el Ministerio Público de la Federación y la Policía Federal Ministerial.

ACTIVIDADES RELEVANTES:

- El agente del Ministerio Público de la Federación ordenará el traslado de los indicios o elementos materiales probatorios a la sede judicial.
- El responsable de la recepción de indicios en la bodega realizará el registro de la salida temporal o definitiva de los indicios o elementos materiales probatorios a la sede judicial y, en su caso, el reingreso.
- La Policía Federal Ministerial trasladará los indicios o elementos materiales probatorios a la sede judicial.
- El agente del Ministerio Público de la Federación determinará la incorporación de los indicios o elementos materiales probatorios en la audiencia.
- El órgano jurisdiccional determina el destino de los indicios o elementos materiales probatorios.

- Se incluirán en el "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15) todas las actividades anteriores.

DOCUMENTOS:

- "Registro de Cadena de Custodia" (Anexo 3 del Acuerdo A/009/15), y
- "Formato de entrega-recepción de los indicios o elementos materiales probatorios" (Anexo 4 del Acuerdo A/009/15).

Anexo 2.- Formato de Entrega-Recepción del Lugar de Intervención

PGR

FORMATO DE ENTREGA RECEPCIÓN DEL LUGAR DE INTERVENCIÓN

(ANEXO 2)

Carpeta de investigación

1. Ubicación del lugar de intervención (Anote la unidad administrativa a la que pertenece el primer respondiente, la Entidad Federativa, Delegación o Municipio en el que se encuentra el lugar de intervención, así como la fecha y hora de arribo).

Unidad Administrativa	Entidad Federativa	Delegación o Municipio	Fecha y hora

2. Servidor público encargado de la preservación que entrega el lugar de intervención (Anote nombre completo, cargo, fecha y hora de entrega, así como la firma autógrafa)

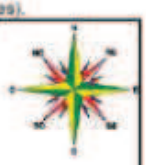
Nombre completo	Cargo	Fecha y hora	Firma

3. Servidor público recibe el lugar de intervención (Anote nombre completo, cargo, fecha y hora de quien recibe, así como la firma autógrafa)

Nombre completo	Cargo	Fecha y hora	Firma

4. Dirección o localización del lugar de intervención (Anote la dirección completa o, en su caso, la localización del lugar de intervención).

5. Croquis simple de ubicación del lugar (Incluya sitios de referencia y el sentido de circulación de vialidades).



Paginación

PGR

FORMATO DE ENTREGA RECEPCIÓN DEL LUGAR DE INTERVENCIÓN

(ANEXO 2)

Carpeta de investigación

6. Preservación del lugar de intervención (señala las medidas tomadas para preservar el lugar de intervención).

7. Documentación del lugar de intervención (Marque con "X" los métodos que adicionalmente se hayan empleado para documentar el lugar de intervención, así como el nombre completo, cargo, y firma de los elementos de la policía que realizaron estas actividades).

Fotográfico	SI		No	
Videográfico	SI		No	
Por escrito	SI		No	

Nombre completo	Cargo	firma

8. Modificación del lugar (Marque con "X" según corresponda. Si es el caso, deberá especificar las modificaciones que se hayan producido).

Modificación del lugar: SI ☐ No ☐

Tipo de modificación: Intencional ☐ Cuerpos de emergencia ☐ Fenómenos naturales ☐

Especifique:

9. Detección temprana de riesgos (Especifique aquellas circunstancias que pueden representar un riesgo para la integridad del lugar, de los indicios o de los servidores públicos que intervienen).

10. Víctimas (Anote el número de víctimas, el nombre si se conoce, si está lesionada, si se trata de un cadáver o de restos de probable origen humano. Cuando el número de víctimas sea muy grande y se encuentren en la misma condición, puede anotar por intervalos).

No.	Nombre	Condición

Paginación ☐

PGR

FORMATO DE ENTREGA RECEPCIÓN DEL LUGAR DE INTERVENCIÓN

(ANEXO 2)

Carpeta de investigación

11. Destino (señale el lugar al que fueron trasladas las víctimas)

No.	Institución que lo trasladó	Lugar al que se trasladó	Placas o número económico de la unidad

12. Personas detenidas (Señale el número y nombre completo de las personas detenidas)

No.	Nombre del detenido

13. Vehículos relacionados (Señale el número y características de los vehículos relacionados)

No.	Tipo y color	Marca	Línea o submarca	Año-modelo	Placa

14. Servidores públicos que ingresaron al lugar (En su caso, anote el nombre completo de las personas que ingresaron al lugar de intervención una vez establecido el acordonamiento y hasta antes de su entrega al personal especializado para el procesamiento)

Nombre completo	Institución y cargo	Hora de ingreso	Hora de salida

15. Servidor público que entrega el lugar después del procesamiento (Anote nombre completo, cargo, fecha y hora de entrega, así como la firma autógrafa)

Nombre completo	Cargo	Fecha y hora	Firma

16. Servidor público que recibe el lugar de intervención después de procesamiento (Anote nombre completo, cargo, fecha y hora de quien recibe, así como la firma autógrafa)

Nombre completo	Cargo	Fecha y hora	Firma

Paginación

Anexo 3.- Registro de Cadena de Custodia

PGR

PROCURADURÍA GENERAL DE LA REPÚBLICA

REGISTRO DE CADENA DE CUSTODIA

(ANEXO 3)

Carpeta de investigación

Institución o unidad administrativa	Folio o llamado	Lugar de intervención	Fecha y hora de arribo

1. Identificación (Número, letra o combinación alfanumérica asignada al indicio o elemento material probatorio, descripción general, ubicación en el lugar de intervención y hora de recolección. Relacione la identificación por secuencias cuando se trate de indicios o elementos materiales probatorios del mismo tipo o clase; en caso contrario, registre individualmente. Cancele los espacios sobrantes).

Identificación	Descripción	Ubicación en el lugar	Hora de recolección

2. Documentación (Marque con "X" los métodos empleados o especifique cualquier otro en caso necesario).

Escrito: Sí ☐ No ☐ Fotográfico: Sí ☐ No ☐ Croquis: Sí ☐ No ☐

Otro: Sí ☐ No ☐ Especifique: _____

3. Recolección y embalaje (Coloque el número, letra o combinación de los indicios o elementos materiales probatorios que fueron levantados directamente con la mano o mediante un instrumento, así como el tipo de embalaje que se empleó, según corresponda. Puede emplear intervalos).

Manual	Instrumental

Bolsa	Caja	Recipientes

Paginación ☐

PGR

REGISTRO DE CADENA DE CUSTODIA

(ANEXO 3)

Carpeta de investigación

4. Servidores públicos (Todo servidor público que haya participado en el procesamiento de los indicios o elementos materiales probatorios en el lugar de intervención deberá escribir su nombre completo, la institución a la que pertenece, su cargo, la etapa del procesamiento en la que intervino y su firma autógrafa. Se deberán cancelar los espacios sobrantes).

Nombre completo	Institución y cargo	Etapa	Firma

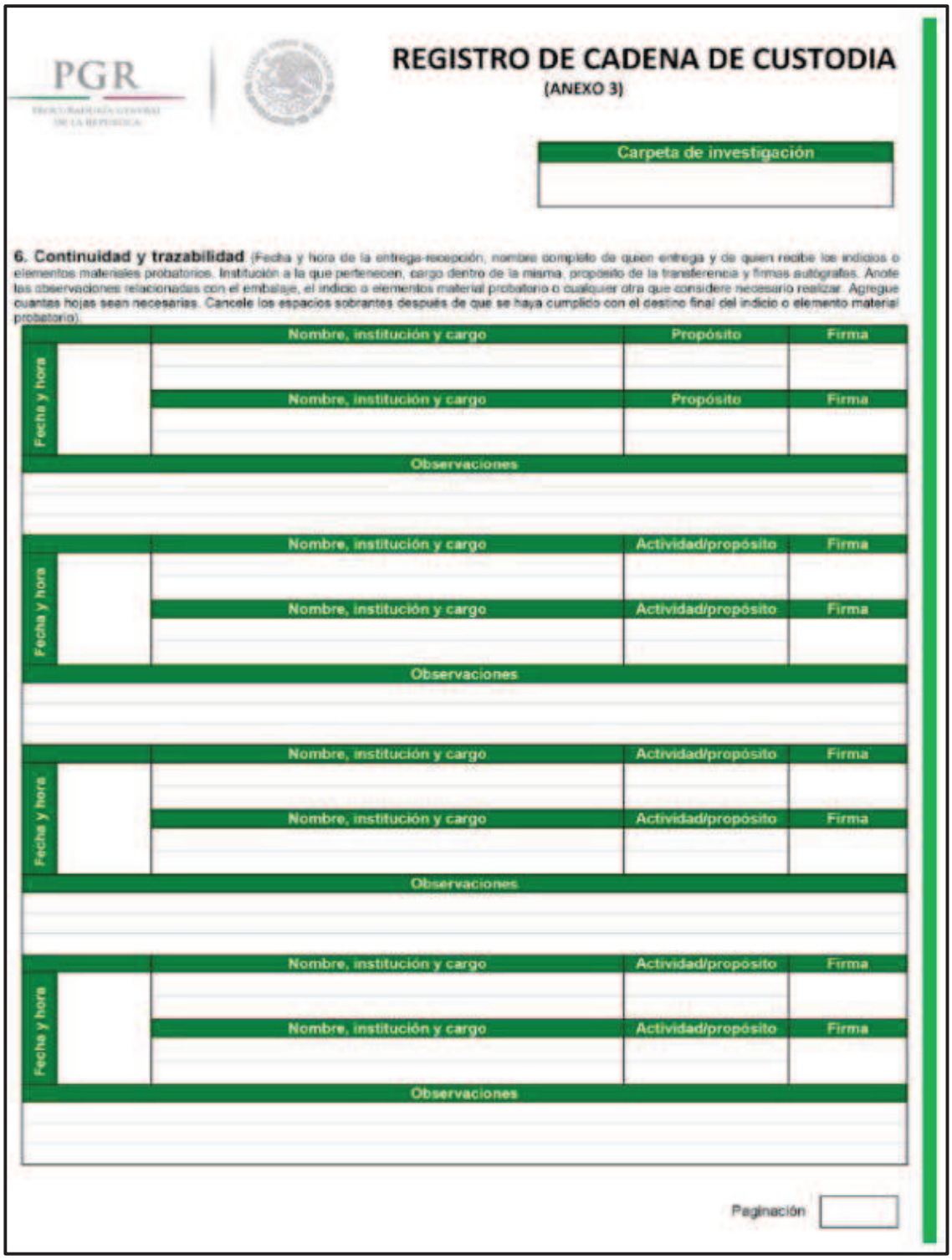
5. Traslado (Marque con "X" la vía empleada. En caso de ser necesaria alguna condición especial para el traslado de un indicio o elemento material probatorio en particular, el personal pericial o policial con capacidades para el procesamiento, según sea el caso, deberá recomendarla).

a) Vía: Terrestre ☐ Aérea ☐ Marítima ☐

b) Se requieren condiciones especiales para su traslado: No ☐ Sí ☐

Recomendaciones:

Paginación ☐



PGR

REGISTRO DE CADENA DE CUSTODIA

(ANEXO 3)

Carpeta de investigación

6. Continuidad y trazabilidad (Fecha y hora de la entrega-recepción, nombre completo de quien entrega y de quien recibe los indicios o elementos materiales probatorios. Institución a la que pertenecen, cargo dentro de la misma, propósito de la transferencia y firmas autógrafas. Anote las observaciones relacionadas con el embalaje, el indicio o elementos material probatorio o cualquier otra que considere necesario realizar. Agregue cuantas hojas sean necesarias. Cancele los espacios sobrantes después de que se haya cumplido con el destino final del indicio o elemento material probatorio).

	Nombre, institución y cargo	Propósito	Firma
Fecha y hora			
	Nombre, institución y cargo	Propósito	Firma
Observaciones			

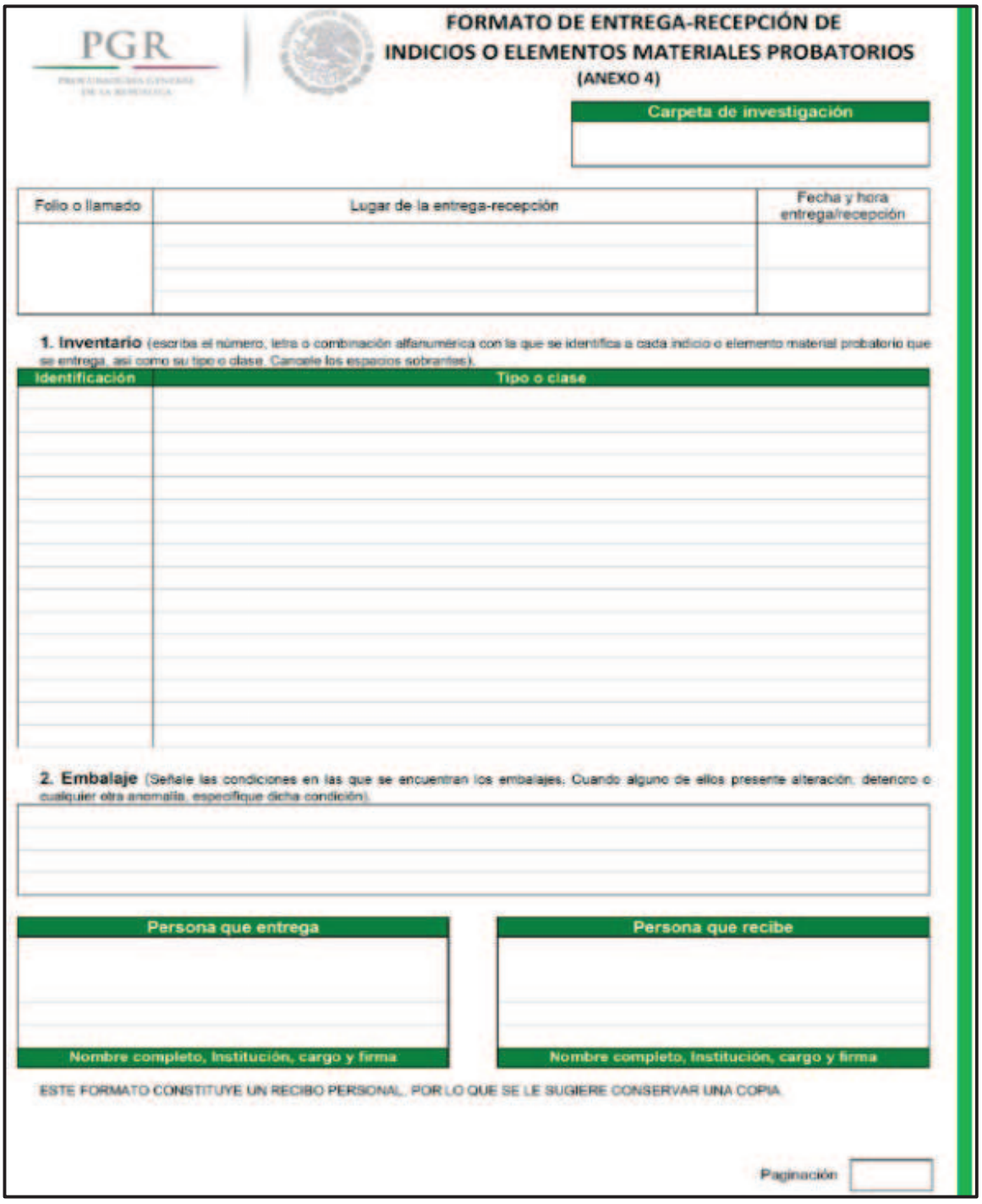
	Nombre, institución y cargo	Actividad/propósito	Firma
Fecha y hora			
	Nombre, institución y cargo	Actividad/propósito	Firma
Observaciones			

	Nombre, institución y cargo	Actividad/propósito	Firma
Fecha y hora			
	Nombre, institución y cargo	Actividad/propósito	Firma
Observaciones			

	Nombre, institución y cargo	Actividad/propósito	Firma
Fecha y hora			
	Nombre, institución y cargo	Actividad/propósito	Firma
Observaciones			

Paginación

Anexo 4.- Formato de Entrega-Recepción de Indicios o Elementos Materiales Probatorios



PGR

FORMATO DE ENTREGA-RECEPCIÓN DE INDICIOS O ELEMENTOS MATERIALES PROBATORIOS

(ANEXO 4)

Carpeta de investigación

Folio o llamado	Lugar de la entrega-recepción	Fecha y hora entrega/recepción

1. Inventario (escriba el número, letra o combinación alfanumérica con la que se identifica a cada indicio o elemento material probatorio que se entrega, así como su tipo o clase. Cancele los espacios sobrantes).

Identificación	Tipo o clase

2. Embalaje (Señale las condiciones en las que se encuentran los embalajes. Cuando alguno de ellos presente alteración, deterioro o cualquier otra anomalía, especifique dicha condición).

Persona que entrega	Persona que recibe
Nombre completo, Institución, cargo y firma	Nombre completo, Institución, cargo y firma

ESTE FORMATO CONSTITUYE UN RECIBO PERSONAL, POR LO QUE SE LE SUGIERE CONSERVAR UNA COPIA

Paginación

Anexo 5.- Formato de Etiqueta para Embalaje

ANEXO 5.

INDICIO/ELEMENTO MATERIAL PROBATORIO

Carpeta de Investigación: _____

Folio: _____

Fecha: _____ Hora: _____

Tipo de indicio/elemento material probatorio/

_____

_____

Identificación (Número, letra o combinación)