ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS.

ÍNDICE DE ANEXOS.

1. CAPÍTULO I

1.1. INTRODUCCIÓN

1.1.1. Antecedentes

Las infracciones realizadas a través de medios informáticos se han diversificado, esto es inevitable con los constantes avances tecnológicos del presente siglo.

Según un estudio realizado por **Google**, los rogues[1] son el 15% de las infecciones detectadas en la web, el 60% de los dominios seleccionados contienen palabras claves que se han ido obteniendo mediante ingeniería social relacionada con las búsquedas de interés de la actualidad, los rogues o falsos anti virus representan el 50% de las infecciones mediante anuncios (Provos N. 2010).

Una prestigiosa firma de anti virus **ESET** Latinoamérica, (Bortnik S. 2010). Presentó el siguiente informe respecto al robo de información:

- El caso de **monster.com** sufrió un robo de 1.6 millones de datos de personas en busca de trabajo.
- **HSBC**[2] reportó un robo de 15.000 clientes de su banco en Suiza.

En donde se evidencia la realidad y el costo para una empresa de la fuga de información, no se diga a un Estado en donde si sucede un evento como el mencionado por ESET en su estudio sería catastrófico por la naturaleza de la información que pueda fugarse.

---

[1] Programa que simula ser un anti virus y sus objetivos varían desde instalar malware hasta robar datos del usuario cuando compra la aplicación para "desinfectar" la máquina.

[2] La matriz se encuentra en Londres, HSBC es una de las más grandes organizaciones bancarias y financieras del mundo. (http://www.hsbc.com/1/2//about)

Ecuador dio el primer paso con la creación de la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos (en adelante LCE) que fue promulgada el 17 de abril del 2002. Con esta ley se pretendía normalizar un vacío legal, que consistía en la falta de una normalización para medios electrónicos/digitales y los delitos que pudieran ser cometidos por estos medios.

Pese a la creación de esta ley, se hace necesario ir más allá y regular correctamente por medio de reformas al Código Penal. Actualmente se encuentran casos muy comunes de clonación de tarjetas, sin que exista una unidad especializada que trate estos "nuevos" casos de infracciones y delitos.

Tomando en cuenta estos inconvenientes es indispensable que se creen departamentos capaces de procesar y presentar pruebas fiables, con alto valor probatorio y elaborar un sistema de justicia con jueces y fiscales capacitados y entrenados para entender este tipo de pruebas.

Los Rogues por ejemplo, son conocidos por ser unos falsos anti virus que alertan de infecciones o amenazas inexistentes en el ordenador, esto explota el miedo de vulnerabilidad del usuario frente a las amenazas que existen.

Esto se debe a que los usuarios no toman las debidas protecciones; no es suficiente tener un AV (anti virus) si no tener el conocimiento e "instinto" de desconfiar de los enlaces que se reciban.

En el presente cuadro se detallan las estadísticas obtenidas en la Fiscalía relacionadas con los delitos a través de medios informáticos/electrónicos que han sido reportados en los últimos cinco años (2005-2010).

Delito	Perjuicio	Artículo de referencia	Estadísticas en Ecuador (2005-2010)
Clonación de tarjetas	Estafa, falsificación electrónica	Código Penal: Capítulo V, de la Estafa y otras defraudaciones Artículos: 560-575. L.C.E.F.D.ME.D: título V, capítulo I, Artículo: 60	Denuncias: 4941.
Fraudes en la información (usando medios informáticos o afines)	Violación de la intimidad, abuso de confianza	LCE: Artículo: 60. Código Penal: Capítulo V, de la estafa y otras defraudaciones, art.: 560-575	Denuncias: 1
Pornografía infantil.	Violación a la intimidad, atentado contra el pudor	Código Penal: Capítulo III de los delitos de proxenetismo y corrupción de menores, Artículo: 528.1	Denuncias: 23

Tabla 1.1.1.1: Estadísticas de delitos informáticos en Ecuador

Fuente: Datos estadísticos del Consejo de la Judicatura, Dirección Provincial de Pichincha, Centro de computo.

1.1.2. Definición del problema.

El siglo XXI con todos sus avances tecnológicos ha traído muchas mejoras y gran comodidad a un buen porcentaje de la población actual, junto a ello se han agregado una serie de delitos e infracciones que se pueden realizar a través de los medios informáticos.

El Ecuador ha empezado a dar sus primeros pasos respecto a estos tipos de infracciones diseñando la LCE (Ley de Comercio Electrónico, Firmas digitales y Mensajes de Datos), esto no será suficiente si no se cuenta con el personal adecuado y un sistema de justicia que sepa enfrentar certeramente estas infracciones.

La LCE provee una normativa antes inexistente, que entre sus partes fundamentales requiere enmiendas al Código Penal para poder sancionar infracciones realizadas por medios informáticos. Se necesita una unidad especializada en delitos informáticos/ electrónicos, para poder enfrentar los casos como los de suplantación de identidad, clonación de tarjetas, entre otros.

1.1.3. Alcance

En el presente estudio titulado: *"Análisis jurídico-técnico de la informática forense en el Ecuador y estudio del procedimiento forense aplicado a casos reales"* se analizó la informática forense, su importancia en la actualidad, las etapas de un análisis técnico de peritaje en informática forense, la recolección y preservación de evidencia; su importancia judicial, para el efecto se detalló y explicó detenidamente cada fase.

Después se investigó dos casos nacionales y dos extranjeros cometidos mediante medios informáticos y sus clasificaciones contenidas en las categorías dadas en la ONU, que han ocurrido, junto con una entrevista a la Dra. Nancy Armendáriz Espinosa que trabaja en la **Corte Suprema de Justicia** con el cargo de Asistente ADMINISTRATIVO III en la Sala de Sorteos y Casilleros.

Después de analizar la información se explica los delitos estipulados y sancionados en el Código Penal y en lo referente a la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos.

Al final se evidencia los cambios y/o posibles implementaciones que se deben realizar.

1.1.4. Objetivos

1.1.4.1. Objetivo general

Realizar un análisis jurídico-técnico de la informática forense en el Ecuador y estudio del procedimiento forense aplicado en casos reales.

1.1.4.2. Objetivos específicos.

- Evidenciar la importancia del peritaje informático en el sistema judicial mediante un análisis jurídico y técnico.
- Identificar procesos para un análisis forense (peritaje informático).
- Establecer los procedimientos para obtener la evidencia digital.
- Identificar procesos para preservar la evidencia digital.
- Analizar avances realizados en el Ecuador frente al peritaje informático.
- Estudiar cuatro casos prácticos aplicando procedimientos descritos.
- Analizar la Interjudicialidad de la normatividad ecuatoriana frente a las demás legislaciones sudamericanas.

1.1.5. Justificación del trabajo

El trabajo es de alta importancia tanto nacional como institucional para la Universidad Internacional SEK.

Respecto a lo institucional, la Universidad Internacional SEK tendrá un análisis sobre la informática forense que es un tema de actualidad, bastante complejo, con escaso entendimiento en el Ecuador; así como también una fuente de consulta sobre la informática forense aplicada en el país como herramienta de soporte en el área judicial, tendiente a esclarecer infracciones cometidas mediante herramientas informáticas.

En el plano de aporte a la comunidad, se ayudará con un análisis capaz de explicar la relación entre la informática forense y el ámbito judicial; su aporte en el esclarecimiento de actos delictivos y promover una conciencia colectiva sobre la vulnerabilidad frente a los ataques informáticos más frecuentes.

Es así, que Latinoamérica ni siquiera cuenta con una normativa legal y reglamentación respecto al uso de la informática. Por ejemplo una noticia de Silicon News:

> La falta de una legislación apropiada en Asia y América Latina ha tenido como consecuencia que estas regiones sean las que crean mayor spam a nivel mundial. Concretamente, más de la mitad de estos envíos en todo el mundo, vienen de estos lugares. (Bárbara B. 2010)

1.1.6. Marco Metodológico

El presente trabajo inicia con un análisis descriptivo partiendo por los hábitos generales actuales respecto al uso de Internet como es el Comercio Electrónico y Negocios Electrónicos, posteriormente se explica las tendencias de las amenazas actuales.

Se realizó una encuesta en el Colegio Rousseau de la ciudad de Quito para ver la costumbre de uso de la tecnología.

Después se analizó mediante el método analítico la situación del Ecuador circunscrita a lo que la Ley de Comercio Electrónico y Firmas Digitales se refiere.

Se entrevistó a un jurista profesional para sustentar la importancia legal de la informática forense y la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos para el proceso judicial de los delitos informáticos.

En los cuatro casos ha servido de apoyo la metodología analítica y la investigación documental.

2. CAPÍTULO II

2.1. MARCO TEÓRICO CONCEPTUAL

2.1.1. Seguridad Informática

La seguridad es un conjunto de procesos y metodologías que se encargan de resguardar la información y el acceso a ella.

La seguridad informática se sustenta en varios pilares, que son:

- **Confidencialidad**: La información es solamente accesible a quien esté autorizado.
- **Integridad**: Característica que hace que su contenido permanezca inalterado, salvo si fue modificado por personal autorizado.
- **Disponibilidad**: La información permanece accesible para ser procesada por personas autorizadas.
- **Autenticación**: El usuario deberá probar su identidad en cualquier parte del sistema.
- **No repudio**: Ni el origen, tampoco el destino debe negar haber recibido o enviado la información.

La seguridad se puede dividir en dos grandes espectros:

La seguridad física.- Es la que se encuentra orientada a defender el perímetro de acceso a los Centros de Datos, daños por sabotaje, desastres naturales o provocados; entre otros.

Este tipo de seguridad generalmente es la que menos se toma en cuenta, ya que cuando se habla de seguridad de la información o sobre seguridad informática, inmediatamente viene a la mente firewalls, anti virus, sistemas de detección y prevención de intrusos; pero

ocasionalmente se toma en consideración este tipo de seguridad que siempre es útil como por ejemplo en caso de un robo el anti virus no sirve de nada.

La seguridad lógica en contra parte, es la que se encarga de poner murallas virtuales que permitan proteger el acceso a los datos y garantizar de igual manera la seguridad física, los pilares en donde se sustenta la seguridad informática.

Entre sus principales funciones de la seguridad lógica se puede encontrar:

- Restringir el acceso a información no autorizada.
- Que la información transmitida sea sólo recibida por el destinatario a quien va dirigida.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

2.1.2. Estándares

Al igual que en todo proceso empresarial existen buenas prácticas que ayudan a conseguir procesos de calidad.

Mediante las certificaciones las empresas presentan sus procesos de calidad.

Existen varios estándares y buenas prácticas de seguridad, empezando con ISO 27000, SGSI, RFC 2196, COBIT.

- **ISO 27000**

Es la norma que engloba todas las prácticas de seguridad.

Existen dos versiones principales del ISO 27000. El estándar ISO 27001 es el que las organizaciones se deben certificar y el 27002 que reúne las mejores prácticas.

Existen varias versiones dentro de la familia ISO 27000.

- ISO 27003 (diciembre de 2010) es un soporte para la ISO 27001 y ésta se basa en directivas para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).
- ISO 27004 (diciembre de 2009) contiene métricas para la gestión de SGSI.
- ISO 27005 (junio de 2008) dedicada exclusivamente a la gestión de riesgos respecto a la seguridad de la información.

El implementar una certificación como ISO 27001 permite contar con un conjunto estructurado de prácticas para proteger el activo más valioso de una empresa como lo es la información, así minimizando a un nivel aceptable las pérdidas de la misma ya que reducir a cero el riesgo es imposible y contar con prácticas adecuadas dentro de la organización ayudara a manejar mejor el margen de costo y riesgo dentro de la organización.

Al saber que la empresa cuenta con buenas prácticas de seguridad, genera confianza por parte de los clientes.

La disponibilidad y continuidad de un negocio es importante porque el tiempo que esté suspendido por un error del programa o una intrusión por falla de seguridad, no sólo generará pérdidas económicas, sino también daño a la imagen y confianza por parte de clientes internos y externos.

Este estándar está diseñado para todo tipo de organizaciones desde instituciones gubernamentales hasta organizaciones sin fines de lucro.

Tomando en cuenta esto, se evidencia que no todas las medidas o controles que pide implementar el estándar ISO 27001 son aplicables para todos, por lo cual si no se aplica, se debe presentar la debida justificación al momento de sacar la certificación de calidad ISO.

Todo el análisis debe estar de acuerdo con los objetivos del negocio, para así tener el apoyo de la gerencia, tomando en cuenta que la inversión en la seguridad de la información, es un pilar fundamental para el éxito de la empresa.

Se debe considerar que el costo de la implementación es alto, por lo tanto es importante dar prioridad a las áreas en donde es necesario realmente un nivel de protección elevado.

Esto va de la mano siempre con los objetivos de la empresa; por ejemplo si la empresa es un cine y tiene servicio para compra de boletos en Internet, uno de los objetivos sería seguir prestando este servicio, por lo cual se debe implementar seguridad a los centros de datos para dar un nivel de confianza a los clientes. La necesidad de implementar los controles del estándar de seguridad ISO 27001 se convierte en prioridad.

Entre varias de las medidas de seguridad se encuentran los Memorandos de acuerdo (MOU) o también los Acuerdos de nivel de servicio (SLA).

Siempre es importante responder las preguntas relacionadas a las normas de seguridad: ¿Qué será protegido? ¿Quién es responsable? ¿Cómo se gestionará? ¿Cuándo entra en vigor? ¿Por qué se creó?

- **SGSI (Sistema de Gestión de Seguridad de Información)**

El **SGSI** es el resultado de haber aplicado el estándar de ISO 27001 junto con las mejores prácticas del ISO 27002.

Este es un conjunto de normas para resguardar la información y garantizar la disponibilidad, integridad y confidencialidad de la misma.

Para garantizar su eficiencia ésta se sujeta a un ciclo de proceso llamado PDCA acrónimo de Plan-Do-Check-Act.

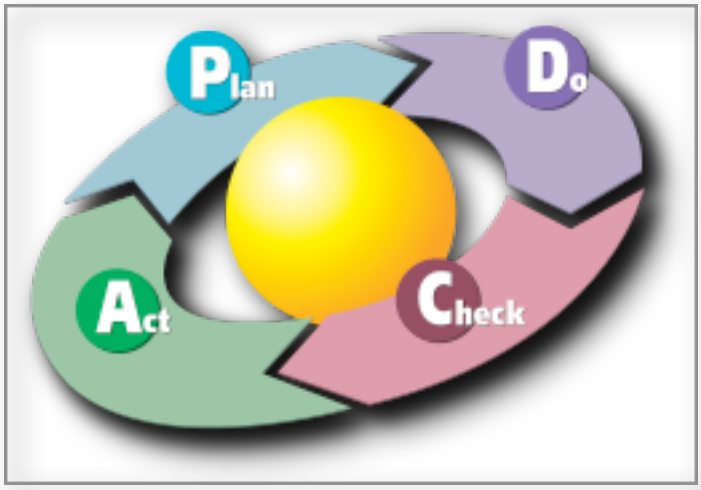


Figura 2.1.2.1 Ciclo de Deming
Fuente: Wikipedia

El principal objetivo del SGSI es el proteger el activo más importante de una empresa sin importar su tamaño; este activo es la información y todo proceso relacionado a éste.

- **Planear (Plan):** En esta fase se realiza el estudio de la organización, aquí se identifica las áreas críticas y se realiza un análisis de riesgos. Esto se debe a que no toda la información disponible en la organización corre el mismo riesgo, pero esto no significa que sea menos trascendente. La información se puede clasificar según la incidencia que tiene para la organización; ésta puede ser: clasificada, importante y pública.

Esta clasificación depende de cada organización y el impacto que pueda tener en caso de que ésta sea comprometida.

Aquí también se debe definir el nivel de riesgo aceptable; esto quiere decir no sólo el nivel de impacto, sino también el nivel monetario.

De igual forma, debe existir un plan de recuperación, como servidores secundarios, procesos que se pueden realizar manualmente y procesos que se deben realizar para recuperar el funcionamiento al cien por ciento.

- **Hacer (Do):** En esta fase se implementan los controles físicos y lógicos anteriormente planificados en las áreas específicas de la organización o empresa. De igual forma la educación a los clientes internos (usuarios) mediante charlas, juegos, carteles y otros tipos de metodologías que puedan motivar a la integración de las metodologías de seguridad implementada.
- **Revisar (Check):** Mediante indicadores métricos se revisará el desempeño de los controles implementados en el SGSI y se identificará los procesos de control que no trabajan correctamente.
- **Actuar (Act):** En esta etapa se despliega las correcciones necesarias a los puntos que se identificaron en la fase anterior del PDCA y el ciclo continúa para seguir mejorando la eficiencia de **SGSI**.

- **RFC 2196**

Llamado en español “El libro de mano de la seguridad”.

Como dice el documento, se basa en el sustento de la seguridad como cualquier estándar o buena práctica de seguridad.

Al igual que el SGSI se tiene pilares que ayudan a alcanzar el objetivo de proteger la información junto con el que pueda tener el negocio:

- Identificar qué se necesita proteger.
- Identificar los riesgos.
- Identificar la frecuencia de los riesgos.
- Implementar controles de protección.
- Mejorar continuamente las medidas de protección.

Al igual que en los otros estándares y buenas prácticas anteriormente mencionadas, se recalca la importancia de una correcta implementación de un gobierno de seguridad.

Primero identificando los archivos, programas y/o documentos de valor a proteger, considerando los riesgos.

Se enlistará lo que se va a proteger:

- **Soporte físico:** Discos Duros, computadoras personales, routers, dispositivos de almacenamiento, etc.
- **Soporte lógico:** Código fuente, bases de datos, Sistemas Operativos.
- **Datos:** Datos en ejecución, datos almacenados en bases de datos, datos en el canal de transferencia.
- Documentación impresa, digital.
- Personal Administrativo, operativo.
- Suplementos de almacenamiento, etc.

También se puede identificar las amenazas como:

- Acceso no autorizado.
- Fuga de información intencionada o no.
- Denegación de servicio (DoS).

Como se puede ver tiene mucha relación con lo anteriormente tratado en ISO 27000 y el SGSI.

El objetivo de toda buena práctica o estándar de seguridad, debe ser costumbre de todo gerente de tecnología en una empresa; independientemente de su tamaño o al mercado que satisface. Es indispensable que se disponga de una política de seguridad elemental y básica por lo menos.

Esta necesidad marca un camino o guía para resguardar la información y los recursos necesarios para un normal funcionamiento de la organización.

El propósito de toda política de seguridad siempre debe ser el cumplimiento del objetivo de la empresa de una forma segura, de igual manera derriba en objetivos propios de todo gobierno empresarial, el avisar a los usuarios de su obligación de proteger la información, independientemente de como se encuentra presentada (física o digital); identificar los mecanismos para proteger la información, dar una línea base para las auditorías, etc.

Algo que debe ser parte de toda política de seguridad es el Uso Apropiado de las Políticas (AUP) por sus siglas en inglés; en donde se debe poner de manera clara para evitar las ambigüedades que se puede o no hacer en los sistemas y sus componentes (si se tiene acceso a componentes claves del sistema, cambiar el soporte físico, actualizaciones del Sistema Operativo), incluyendo el tipo de tráfico que se va a generar en el sistema.

Lo anterior es importante, porque ayuda a detectar rápidamente brechas de seguridad por un tráfico poco habitual, algunos errores en el sistema por una actualización del Sistema Operativo que causó una falla de comunicación con la red debido a que el programa no podía correr en la nueva versión.

Para terminar se enumerará las personas que debieran estar involucradas en el proyecto de gobierno de seguridad:

- Administrador de seguridad.
- Técnicos de la empresa.
- Encargados de grupo de usuarios grandes, por ejemplo jefe de ventas, mercadotecnia, etc.
- Grupo de respuesta de incidentes.
- Representantes de los grupos afectados por las políticas de seguridad de la empresa.
- Responsable de la directiva de la empresa.

- Grupo legal.

- **COBIT.**

COBIT da soporte al gobierno de TI para alinear el departamento con los objetivos de negocio, maximiza el beneficio porque capacita al negocio, se usa los recursos de TI de manera responsable y los riesgos de TI son manejados de forma responsable y eficiente. COBIT es un marco de trabajo desarrollado por ISACA su primera publicación fue en el año 1996, su más reciente versión es la 4.1 publicada en el año 2007 y se planea su actualización a la versión 5.0.

En el siguiente gráfico se explica las áreas en que se enfoca COBIT, donde se puede observar como COBIT asegura que las Tecnologías de Información se alinean con el negocio, maximiza beneficios, uso responsable de recursos y administración adecuada de los mismos.

Figura 2.1.2.2 Áreas de enfoque de TI
Fuente: COBIT 4.1 en español

- **Alineación Estratégica.-** Se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.
- **Entrega de Valor.-** Se refiere a ejecutar la propuesta de valor a todo el ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de TI.
- **Administración de Recursos.-** Se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.
- **Administración de Riesgos.-** Requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.
- **Medición del Desempeño.-** Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards[3] que traduce la estrategia en acción para lograr las metas que se puedan medir más allá del registro convencional.

La orientación al negocio, es el objetivo de COBIT que la tecnología tiene que ser el soporte que ayude a cumplir los objetivos de la organización de una manera fácil.

[3] Una herramienta de gestión que traduce la estrategia de la empresa en un conjunto coherente de indicadores.

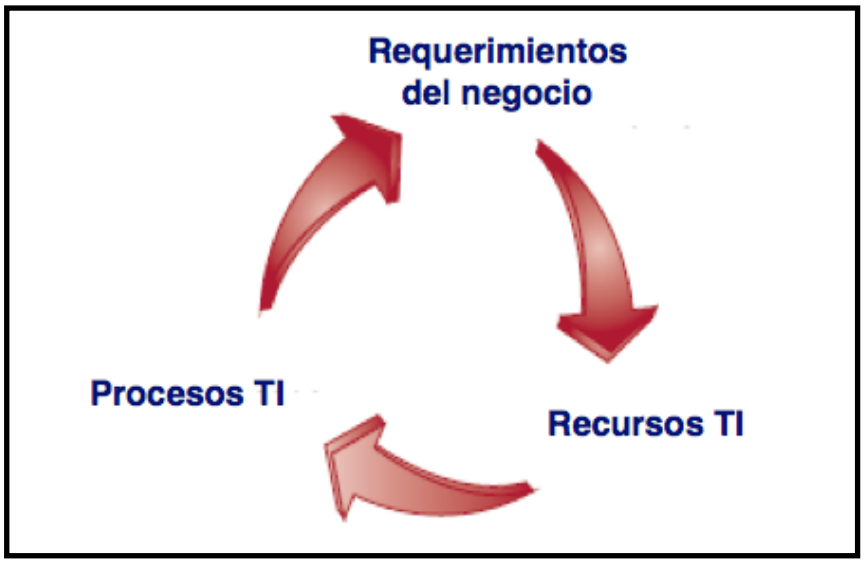


Figura 2.1.2.3 Marco de trabajo de COBIT
Fuente: COBIT 4.1 en español

En el gráfico se puede ver que la organización administra los recursos de TI mediante procesos estructurados para satisfacer los requerimientos del negocio.

A nivel de seguridad en COBIT se tiene los controles de entregar y dar soporte que se centran entre algunos puntos como: niveles de servicio, continuidad del servicio, seguridad de sistemas, administración de la configuración, los problemas, entre otros temas.

- **Acuerdo de nivel de servicio.**

El Acuerdo de Nivel de Servicio (SLA) se logra al establecer, por medio del contrato escrito entre proveedor y cliente, con objeto de disponer garantías de niveles de calidad, de servicio y multas por incumplimiento de términos del contrato.

Este proceso requiere de monitoreo y oportuna notificación a los clientes sobre los cumplimientos de los SLA y retro alimentación entre TI y clientes.

Entre los objetivos que se tiene en este control constan los siguientes:

- Marco de trabajo de la administración de los niveles de servicio.

- Definición de los servicios.
- Acuerdo de niveles de servicio.
- Acuerdo de niveles de operación.
- Monitoreo y reporte de cumplimiento de niveles de servicio.
- Continuidad de servicio, entre otros.

Hace unos meses cuando un grupo de hackers de nombre Anonymus penetraron la seguridad de la PSN[4], se robaron datos de los usuarios, llevando al servicio de la PlayStation 3 a varios meses fuera de servicio.

Por lo tanto, tener un plan de contingencia es importante para evitar o mitigar el daño causado por una eventual penetración a los sistemas; esto lleva a planificar respaldos fuera de la instalación de la información crítica, que permita el menor tiempo de restauración, identificando procesos que puedan hacerse manualmente, ensayando sucesos para probar vías de comunicación (conexión) alternas. Todo esto con el objetivo de mitigar el impacto de las interrupciones en los servicios de TI y servicios claves para el negocio.

Dentro de los objetivos en este punto de control se puede encontrar algunos como:

- Marco de trabajo de seguimiento para soportar la continuidad del negocio de manera consistente a lo largo de la empresa.
- Planes de continuidad basados en el marco de trabajo para reducir a niveles aceptables el impacto de una interrupción en el negocio.
- Identificar los puntos críticos de TI para medir la resistencia y planificar los pasos de recuperación, no distraerse con los puntos no críticos.
- Pruebas de planes de recuperación para identificar errores y asegurar el estado de recuperación, que las deficiencias sean atendidas y el plan continúe aplicable.
- Entrenamiento del plan de recuperación para reducir tiempos de respuesta.

[4] PlayStation Network

Se tiene también casos ecuatorianos como el reciente (10 de agosto del 2011) que bloqueó a la página del Gobierno y del Ministerio de Telecomunicaciones. Esto se relaciona con un anuncio del grupo Anonymous ante los sucesos del Gobierno y su operación llamada Condor Libre que empezó el 10 de agosto del 2011.

En resumen, se enumeró algunos controles de los estándares y prácticas de la seguridad en información.

2.1.3. Tendencias de los delitos.

El año 2011 tuvo muchas novedades como el *boom* de las redes sociales Facebook y Twitter, entonces las empresas comenzaron a preocuparse por su intimidad y así evitar la fuga de información y el uso de los abreviadores de direcciones de Internet para ocultar programas maliciosos.

En el ámbito de fuga de información recuerden el caso citado de Sony:

> En abril, Sony anunciaba una intrusión en los sistemas de PlayStation Network donde se puso en riesgo a 77 millones de clientes. Los atacantes lograron datos del historial de compras y los datos de las tarjetas de créditos (Cid C. 2011).

El otro caso que se va a citar a continuación es para ejemplificar el uso de las redes sociales y el abreviador de direcciones de Internet:

> Dicha amenaza, la cual utilizaba una de las diversas técnicas de Ingeniería Social, empleaba el llamativo mensaje indicando saber quién visitó nuestro perfil de Twitter: "I just viewed my TOP20 Profile STALKERS. I can't believe my EX is still checking me every day", el cual llegó a generar 159 tweets por minuto de usuarios infectados.
>
> Una vez que la víctima realiza clic sobre el enlace malicioso, el cual utilizaba el acortador de direcciones URL Bit.ly[5], se le pide a la víctima autorización para realizar la instalación de una aplicación de terceros en Twitter. Luego, la misma comienza a enviar mensajes automáticamente a todos los seguidores de la víctima, repitiéndose el texto antes mencionado sobre "quién visitó nuestro

[5] Servicio para acortar direcciones web (URL)

perfil", para continuar así con el engaño a fin de comprometer cuentas de los usuarios afectados (Cid C. 2011).

Como se puede observar mediante algunas técnicas de los ejemplos anteriormente citados la intimidad se vio amenazada al igual que información personal.

Se observa que en el 2011 los ataques con fines políticos continúan, según una encuesta realizada por la firma de seguridad Symantec (http://www.symantec.com/es/mx/resources/articles/article.jsp?aid=principales-tendencias-2011), más del 50% de las empresas encuestadas sospechan ser un blanco o tienen la certeza de ser un blanco de ataques motivados por la política; un ejemplo fue el gusano Stuxnet en las plantas nucleares en Irán en el 2010.

Respecto a los dispositivos Apple que han aumentado considerablemente su popularidad están los iPhone e iPads en empresas. Los cyber criminales seguramente añadirán a su lista de objetivos a dichos dispositivos. El caso más reciente el troyano Macdefender.

Seguramente crecerá el hacktivismo[6] con el impulso de Wikileaks, se prevé el hacktivismo en forma de ataque de denegación de servicio distribuido (DDoS).

Un ejemplo es la operación #AntiSec, una alianza entre Anonymus y LulzSec, que mediante un DDoS, atacaron a la página web del gobierno y la presidencia de Brasil.

"Tango abajo, gobierno y presidencia de Brasil… nuestra unidad en Brasil está haciendo progresos"[7]

[6] Por hacktivismo (un acrónimo de hacker y activismo) se entiende normalmente "la utilización no violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos". (Wikipedia)

[7] Mensaje de rama de LulzSec en Brasil (noticia completa en http://alt1040.com/2011/06/comienza-la-operacion-antisec-lulzsec-ataca-al-gobierno-de-brasil-y-anonymous-envia-un-mensaje)

Con estos ejemplos de tendencias se debe tomar en cuenta que el delito por medios informáticos seguirá creciendo y como administradores, estado, usuarios, etc. Se debe tomar precauciones y saber que ninguna tecnología es 100% segura.

2.1.4. Amenazas y delitos.

Las amenazas informáticas se pueden englobar en varias clasificaciones, se sitúa en la primera categoría las amenazas lógicas que es el malware.

El malware viene de las palabras en inglés que significa programa malicioso.

El malware engloba todas las amenazas por programas no deseados o maliciosos tales como:

- **Virus informático**.- Se considera actualmente a un archivo o porción de código que es: auto ejecutable, capaz de ser Dañino, Auto-replicante, Subrepticio[8] (DAS).
- **Gusanos**.- Programas que se reproducían hasta colapsar los recursos del huésped, actualmente cumplen una función distinta como propagarse a través de correos electrónicos, redes P2P, servicios de mensajería instantánea para llegar a la mayor cantidad de víctimas y posteriormente implantar otro tipo de malware que es el que hará realmente el daño.
- **Troyano**.- Es un código malicioso que se oculta dentro de una aplicación o archivo "normal" que aparenta hacer algo beneficioso, pero al mismo tiempo ejecuta acciones dañinas sin que el usuario se percate.
- **Ransomware**.- Es un tipo de amenaza en donde el atacante secuestra los archivos de la máquina generalmente cifrándolos con una clave y dejando instrucciones para el rescate de los mismos.

[8] Que se hace ocultamente o a escondidas. (fuente: RAE)

- **Scam o engaño.-** Es una técnica en donde se busca robar datos confidenciales y para incentivar esta práctica se usa estímulos como el traspaso de cantidades enormes de dinero respecto a comisiones de negocios.
- **Spyware o programa espía**.- Es un programa que se ejecuta en la máquina recogiendo información sobre los hábitos de navegación, este tipo de información es valiosa para empresas dedicadas a la publicidad porque permite tener avisos de publicidad mucho más relevantes para el usuario.

Respecto a otro tipo de amenazas, existen las físicas como robos, incendios, sabotaje físico, erupciones, terremotos, etc.

Dentro de los delitos están:

- **Robo**: Artículo 58 de la LCE[9] "El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica".
- **Sabotaje**: Artículo 59 de la LCE "Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su Calidad de tales, o que les hubieren sido encomendados en razón de su cargo".
- **Falsificación**: Artículo 60 de la LCE "Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemática ..."

[9] Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos

- **Daños a la propiedad privada**: Artículo 61 de la LCE Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.
- **Violación a la intimidad**: Artículo 64 de la LCE.- Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Estos son los delitos contemplados en la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos que se sugiere añadir al Código Penal.

2.1.5. Informática Forense

La informática forense es una ciencia que sirve de soporte al sistema judicial para el esclarecimiento de delitos perpetrados por medios tecnológicos y presentar pruebas con carácter probatorio y válido jurídicamente según la legislación del país y es completamente determinante en cada fase.

La informática forense junta herramientas de soporte físico y lógico para develar pruebas y esclarecer los hechos en la comisión de un delito.

2.1.5.1. Concepto.

Existen varias definiciones relacionadas con la informática forense[10]

[10] Forense: Perteneciente al foro (tribunales y audiencia), a la justicia.(Diccionario Jurídico)

El sitio de Venezuela relacionado a peritaje informático (informática forense) (Administrador 2008) define: "La Informática Forense es el proceso de investigar dispositivos electrónicos o computadoras con el fin de descubrir y de analizar información disponible, suprimida, u ocultada que puede servir como evidencia en un asunto legal. Es igualmente provechosa cuando se han perdido accidentalmente datos debido a fallas."

Se entiende que es una disciplina orientada a descubrir evidencias de los delitos[11] sobre la base de conocer el programa o el Sistema Operativo violentado. La informática forense se basa en un conjunto de técnicas asistidas por el soporte lógico especializado en informática forense.

También se puede ayudar con otra definición de informática forense por parte de Microsoft: "La Informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos".(Gómez E. 2011). La informática forense también puede ser usada y de hecho lo es, como herramienta preventiva ante ataques, intrusiones, fuga de información ya sea por atacantes internos o externos junto con el Hacking Ético.

Se usa para diseñar políticas de seguridad, acoso sexual, robo o apropiación de información confidencial y espionaje industrial.

La necesidad de esta herramienta radica en que actualmente los datos son digitales y mucha información sensible se encuentra en discos duros de servidores, gerentes y otros responsables de áreas.

[11]Es una conducta, acto u omisión en contra de la ley, derecho culpable al que corresponde sanción o pena. (Wikipedia)

2.1.5.2. Clasificación de la informática forense

La informática forense se puede clasificar en dos grandes grupos dependiendo de su escenario de análisis.

- El análisis en vivo se procederá a suspender o terminar todo proceso sospechoso, se desconectará de la red para evitar envío de información o manipulación de la evidencia por parte del atacante y al equipo se le conectará a un switch vacío (sin otras conexiones a más del equipo que se va a realizar en análisis) para evitar mensajes de error de conexión en los registros.
- Para un análisis en cadáver se terminará todo proceso desconectando el equipo, no se seguirá el proceso "normal" de apagado ya que puede llevar a sobre escritura de evidencias que resultarán útiles para la investigación.

Según su especialidad se tiene:

- Forense en redes: Esta disciplina se basa en analizar el tráfico de redes y de los paquetes de transmisión en base del análisis de las cabeceras de cada protocolo.
- Forense digital: Es similar a la informática forense, al aplicar conceptos tecnológicos y criminalista para capturar a los ciberdelincuentes[12].

2.1.6. Aplicación

La informática forense es actualmente una ciencia, que toma valor por la cultura tecnológica que se vive en la actualidad.

Como se describió anteriormente, la información es algo indispensable para la continuidad de la organización o empresa.

[12] Persona que comete actos ilegales por medios informáticos y/o electrónicos

> Esta ciencia da la capacidad de descubrir alguna filtración o actividad anormal, como lo dicen en el sitio de Microsoft: “Cuando una empresa contrata servicios de Informática forense puede perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se han producido” (Gómez E. 2011).

En un escenario constantemente cambiante ya sea por razones políticas, empresariales o el simple hecho del enriquecimiento, la ciencia forense en especial la de la informática, da soporte a la justicia ayudando a solucionar delitos, prevenirlos o esclarecer alguna otra acción delictiva.

La tendencia de las amenazas en el presente año, el campo de batalla es el mundo virtual (Internet), porque se encuentra ahí la información.

También toma bastante importancia en el mundo empresarial, como herramienta de auditoría para hacer cumplir las reglas en caso de acoso sexual, robo de información, de propiedad intelectual o secretos empresariales; incluso sirve para develar casos de espionaje empresarial.

Como se puede divisar es una herramienta tanto preventiva como reactiva que claramente cumple esa función en los casos de investigación de delitos.

3. CAPÍTULO III

3.1. ANÁLISIS JURÍDICO Y TÉCNICO DE LA INFORMÁTICA FORENSE

3.1.1. Código Penal y delitos contemplados.

Código Penal (C.P) es un conjunto de normas jurídicas, punitivas emanadas del Estado que son el resultado de un pacto social que contempla toda conducta atípica que genera un daño a la sociedad; usualmente deriva de los derechos contemplados en la Constitución, por ejemplo: el derecho a la vida, propiedad, derecho a la identidad, derecho al buen vivir entre otros.

Las sanciones o penas establecidas en este cuerpo legal están orientadas a corregir una conducta humana que violentan los derechos enunciados. Esta conducta debe estar claramente establecida dentro del código en términos legales; tipificada en el mismo. La sanción usualmente o en su generalidad contempla la privación de la libertad como característica general.

El Código Penal contempla todos los delitos punibles en el Estado.

El Libro Segundo del Código Penal tipifica los delitos en general, así inicia con aquellos que comprometen la seguridad del Estado. En este título, se comienza tratando los delitos que comprometen la seguridad exterior, como lo dice el Artículo 115: “Todo el que dentro del territorio de la República conspire contra su seguridad exterior, induciendo a una potencia extranjera a declarar la guerra al Ecuador, será reprimido con reclusión mayor Extraordinaria, de doce a dieciséis años, sometido a la vigilancia especial de la autoridad, por diez años, e inhabilitado por el mismo tiempo para ejercer los derechos de ciudadanía”.

El contexto del párrafo anterior tiene que ver mucho con la actualidad, en tal sentido se revela esa necesidad de protección al Estado dentro de la noticia, publicada el 24 de agosto del 2010 en donde Estados Unidos alista "cyber defensas" ante un posible ataque de hackers extranjeros con el afán de proteger la seguridad externa del referido Estado.

Actualmente, el Ecuador no posee la capacidad de reaccionar ante una situación de ataque de naturaleza tecnológica, esto se evidenció el 10 de agosto de 2011, cuando el grupo hacktivista Anonymous realizó un ataque dirigido a las páginas gubernamentales como el caso de la Súper Intendencia de Telecomunicaciones entre otros.[13]

En el Artículo 58 de la LCE "...Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica".

En el Capítulo tercero del Código Penal se habla de la seguridad interior del Estado.

En el 59 de la LCE se habla algo relacionado a este capítulo: "Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo".

Este Artículo reformatorio al Código Penal se relaciona no solo con la seguridad interna por dañar fuentes de información muchas que pueden ser estratégicas y de vital importancia, sino que también se centra en proteger la información de las personas naturales que hayan encargado su información a entidades financieras, empresas que por negligencia pongan en riesgo la información confiada a ellos. También es aplicable a

[13] Noticia completa en: http://alt1040.com/2010/08/estados-unidos-alista-las-defensas-para-la-ciberguerra

empresas que encargan el manejo de la información al director de tecnología o a la persona encargada del centro de datos que por venganza o malicia borre o dañe la información.

Un caso relacionado a esto, es el de las centrales nucleares de Irán con el gusano Stuxnet, que se cree que es un ataque de algún gobierno a Irán por la complejidad del gusano.

También lo anterior es considerado en delitos contemplados en el capítulo cuarto del Código Penal “Sabotaje y terrorismo”.

En el capítulo quinto relacionado a la inviolabilidad del secreto, es algo que siempre se debe tener presente en la vida diaria e inclusive en la digital.

La intimidad se encuentra protegida en la Constitución en el numeral veinte del Artículo sesenta y seis en el Capítulo VI.

También se encuentra mencionado en la LCE en el Artículo noveno, que se refiere a la protección de los datos.

Un caso reciente es el de Scarlett Johansson, quien sufrió una intrusión en su celular y se publicó en Internet fotos íntimas.

En el capítulo segundo, se habla de la falsificación de marcas algo muy común en el ámbito de la estafa y robo de información.

Entre los casos más comunes se encuentran la suplantación de entidades financieras en donde se engaña al cliente bancario y también suelen abusarse de la popularidad de algún servicio.

Otro ejemplo es la copia de la página del servicio más popular de comunicación, Skype; el sitio falso de Skype está diseñado para robar las credenciales de autenticación de los usuarios engañados, tarjetas de crédito y dirección de facturación.

En el capítulo tercero, se habla de la falsificación de documentos como se explica claramente en el Artículo 337:

> Serán reprimidos con reclusión menor extraordinaria de nueve a doce años, los funcionarios públicos que, en el ejercicio de sus funciones, hubieren cometido una falsedad que consista en:
> - Firmas falsas;
> - Alteración de actas, escrituras o firmas;
> - Suposición de personas;
> - Escrituras hechas o intercaladas en registros u otros documentos públicos, en escritos u otras actuaciones judiciales, después de su formación o clausura.

Es cierto que no dice expresamente sobre falsificaciones digitales pero es extensible a ese ámbito; tales como alterar una sentencia o introducir una (caso Chucky Seven[14]), correos electrónicos que sean orientados a obtener información sensible (correos que simulen ser de Blizzard) para robar información bancaria, credenciales de ingreso del popular juego World of Warcraft o cualquier otro de esta empresa, los clientes de esta empresa son blancos de preferencia de los estafadores por la gran popularidad de los juegos y el dinero que invierten en éstos.

También se tiene un título que habla sobre la seguridad pública, éste tiene una relación estrecha con los delitos informáticos, electrónicos.

A continuación cito al capítulo primero que habla sobre las asociaciones ilícitas "Art. 369.- Toda asociación formada con el fin de atentar contra las personas o las propiedades, es un delito que existe por el solo hecho de la organización de la partida".

Cómo dice el Artículo que es un delito el formar una asociación con el fin de atentar contra persona o propiedades, éste Artículo es extensible a organizaciones de hackers que residan en Ecuador porque encajan con este Artículo; permanentemente se apresan a personas

[14] Se refiere al caso de la redacción de la sentencia del periódico El Universo (más detalles en: http://rafaelcorreacontraeluniverso.eluniverso.com/2011/12/16/juez-paredes-se-contradice-en-audiencia-por-caso-chucky-seven/)

involucradas en grupos de hackers, por ejemplo el 22 de septiembre se apresaron a dos hackers, uno en San Francisco, otro en Phoenix.

Con este ejemplo se concluye que es necesaria una ley, que regule las asociaciones de esta naturaleza ya que según un estudio el 50% de las transacciones que se realizan en Ecuador son realizadas en Internet (Andes. 2011). Tomando en cuenta estos precedentes, se hace necesario un conjunto de normas jurídicas que regularicen estas actividades, caso contrario estos delitos crecerán exponencialmente sin sanción alguna.

En el capítulo tercero, se habla de la intimidación y lo podemos ver el Artículo 377:

> El que por escrito, anónimo o firmado, amenazare a otro con cualquier atentado contra las personas o las propiedades, que merezca pena de reclusión menor, será reprimido con prisión de seis meses a tres años y multa de ocho a dieciséis dólares de los Estados Unidos de Norte América, si la amenaza ha sido acompañada de orden o condición.
>
> En caso contrario la pena será de tres meses a un año y multa de seis a nueve dólares de los Estados Unidos de Norte América.

El delito de intimidación se lo encuentra frecuentemente en el ámbito informático para muestra se citará una amenaza ya tratada en este texto y es el "Ransomware" que es el "secuestro de la información", al igual que amenazas de intrusión a gobiernos (caso Anonymous), que al final se terminaron cumpliendo, entre otras que fueron en su momento noticia.

En el capítulo décimo, contiene todo lo relacionado con los delitos contra la propiedad como son el hurto y el robo.

Respecto al hurto en el capítulo primero especifica que:

> "Art. 547.- Son reos de hurto los que, sin violencias ni amenazas contra las personas, ni fuerza en las cosas, sustrajeren fraudulentamente una cosa ajena, con ánimo de apropiarse".
>
> Además, son considerados como reos de hurto los individuos de reconocida conducta delictuosa, que habitualmente se dedicaren a la comisión de delitos contra la propiedad y que se hallaren registrados como tales en las Oficinas de Seguridad

del Estado. La pena para esta clase de delincuentes será de uno a tres años de prisión.

El hurto de información es algo que sucede seguido con los engaños de Ingeniería Social.

Está técnica usa la ingenuidad de los usuarios para que ellos mismos les proporcionen esa información; los casos más comunes son los que se hacen pasar por entidades bancarias o explotando la popularidad de un juego como World of Warcraft.

En cualquier caso el fin es el apropiarse de la información personal.

A diferencia del hurto el robo se realiza mediante fuerza como se cita en el capítulo segundo.

- "Art. 550.- El que, mediante violencias o amenazas contra las personas o fuerza en las cosas, sustrajere fraudulentamente una cosa ajena, con ánimo de apropiarse, es culpado de robo, sea que la violencia tenga lugar antes del acto para facilitarlo, en el momento de cometerlo, o después de cometido para procurar su impunidad".

Esto trasladado al campo de la tecnología, es utilizar técnicas de intrusión mediante fuerza bruta, instalar puertas traseras, malware, otras tecnologías que a diferencia de la ingeniería social en donde no se utiliza la "fuerza" para realizar la intrusión sino la astucia del atacante.

En el capítulo cuarto, se explica sobre la extorsión, que en muchos casos como es el ransomware, se extorsiona al individuo para realizar un pago.

Un caso reciente es el del malware de nombre Ransom.AN, lo que hace es cifrar todos los archivos importantes y bloquear al equipo; pide una cantidad de dinero a cambio de la clave para poder descifrar los archivos y poder acceder al equipo.

En el capítulo quinto, se explica todo lo relacionado a la estafa y otras defraudaciones.

> El que fraudulentamente hubiere distraído o disipado en perjuicio de otro, efectos, dinero, mercancías, billetes, finiquitos, escritos de cualquier especie, que contengan obligación o descargo, y que le hubieren sido entregados con la condición de restituirlos, o hacer de ellos un uso o empleo determinado, será reprimido con prisión de uno a cinco años y multa de ocho a dieciséis dólares de los Estados Unidos de Norte América.

Con todo esto se advierte que las reformas que plantea la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, cubren una parte de este espectro que se está volviendo cada vez más común por la cantidad de información personal que se registra en Internet (redes sociales) y financiera (banca en línea).

En las encuestas realizadas al colegio Rousseau (ver Anexo 1) se puede contemplar la necesidad de la reforma al Código Penal, las cuales podrían ser:

- Acoso: En la pregunta 7 (ver Anexo 2) se aprecia claramente que los jóvenes entre once y diecisiete años, un equivalente al 50,85% alguna persona desconocida se ha contactado con ellos, la causa ponen datos privados de manera pública, esto evidencia una falta de protección hacia menores; en el Anexo 2 pregunta 5 se refleja que un 12,82% ponen datos privados en las redes sociales, todo ello demuestra una falta de protección respecto al uso de la información almacenada en los servidores que puede ser vendida o usada por personas con falta de escrúpulos como pedófilos o traficante de menores.
- También existe la responsabilidad por parte del Estado de proteger y garantizar la intimidad de los habitantes.

3.1.2. Código Civil y Cuasidelitos contemplados.

El Código Civil es un conjunto de normas que regulan el intercambio comercial entre personas naturales y jurídicas; públicas y privadas siempre y cuando las públicas actúen como particulares.

En el título treinta y tres se habla de los delitos y cuasidelitos.

En el Código Penal se habla de delitos, estos se castigan generalmente con privación de la libertad, a diferencia del Civil se habla de indemnizaciones de daños o perjuicios como lo dice el Artículo 2214:

"El que ha cometido un delito o cuasidelito que ha inferido daño a otro, está obligado a la indemnización; sin perjuicio de la pena que le impongan las leyes por el delito o cuasidelito".

El cuasidelito es derivado de un delito que está tipificado en el Código Penal.

En el Artículo 2215 se habla de las indemnizaciones y de las penas que respaldan el Código Penal.

> Puede pedir esta indemnización, no sólo el que es dueño o poseedor de la cosa que ha sufrido el daño, o su heredero, sino el usufructuario, el habitador o el usuario, si el daño irroga perjuicio a su derecho de usufructo, de habitación o uso. Puede también pedirla, en otros casos, el que tiene la responsabilidad con obligación de responder de ella; pero sólo en ausencia del dueño.

Este caso es aplicable al daño de la propiedad digital, como puede ser la información encargada a una institución y que haya vulnerado.

3.1.3. Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos

La Ley fue promulgada en el año 2002 tiene como objetivo regular los mensajes de datos, contratación electrónica, la prestación de servicios, entre otras.

A lo largo de este capítulo se habla de la interrelación entre el Código Civil, Penal con la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos; al igual que las fortalezas y debilidades de la ley ecuatoriana y otras de países de Sur América.

3.1.4. Interjudicialidad

La Ley de Comercio Electrónico ecuatoriano busca regular un aspecto "nuevo" que va cada vez más tomando fuerza conforme avanza el tiempo. En este cuerpo legal se habla de certificados, delitos informáticos, firmas electrónicas y al momento de tratar los delitos informáticos. Este ordenamiento jurídico busca actualizar al Código Penal pidiendo reformas para poder castigar estos medios delictivos, de acuerdo a un nuevo espectro que se abre mediante el avance de la tecnología, considerando que estos delitos son cada vez más comunes, pues la información y los movimientos económicos se encuentran más ligados al Internet.

El Código Civil, entendido como la norma jurídica encargada de regular las transacciones mercantiles que involucran bienes muebles, inmuebles e intangibles; está encargado de cuantificar o valorar los mismos. Dentro de este cuerpo legal tenemos también un capítulo dedicado a reconocer los cuasi delitos que son los daños en el ámbito Civil, que dependiendo de la intensión de causar daño de una de las partes en litigio; podría convertirse o configurar un delito en el área penal.

La interrelación de estos cuerpos jurídicos de naturaleza diversa se da y evidencia porque el hecho ilegal se encuentra tipificado en el Código Penal como tal y reconocido como medio delictivo en la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, dando paso al reconocimiento económico del bien vulnerado que procede en el campo del Código Civil. Estos cuerpos legales se encuentran mutuamente apoyados y la supletoriedad entre éstos provoca una interrelación entre los mismos.

Con lo descrito se advierte que las leyes son convergentes, todas cumplen una función para poder regular este ambiente, como el Internet la mayoría de operaciones son transacciones económicas. Como se leyó en la definición del Código Civil esta interviene en la regulación de las actividades económicas que se efectúan en Internet, la LCE se encarga de proporcionar el campo regulador de todas las operaciones y conceptos necesarios para poder entender este ámbito y además plantea reformas necesarias al Código Penal para

que éstas puedan accionar de manera correctiva respecto a los delitos que se realicen en este ámbito legal.

3.1.5. Análisis comparativo entre leyes de diferentes estados

- **Semejanzas.**

La ley de Comercio Electrónico venezolana promulgada el año 2001, establece:

> Artículo 1. El presente Decreto Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

Igual que la ley ecuatoriana, da fuerza legal al mensaje de datos; esto quiere decir que si tenemos la misma información en formato impreso (físico) y digital ambas tienen la misma importancia.

Argentina al igual que Venezuela y Ecuador, promulgaron la Ley de Comercio Electrónico y Firmas Digitales; en el año 2001.

Similar que las anteriores, la Ley de Argentina reconoce la eficacia jurídica de los mensajes de datos y la firma electrónica:

Artículo 1 Objeto: “Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley”.

En Colombia el decreto número 527 da fuerza legal a la ley de Comercio Electrónico, similar al del resto de países de Sur América, en su capítulo segundo en los Artículos seis y siete se habla de igual manera sobre la validez jurídica de todos los mensajes de datos y firmas digitales.

Artículo 6: Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este Artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

Artículo 7: Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación.

Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Cómo se aprecia, las intenciones de las leyes son crear un camino en donde se comience a digitalizar los documentos sin perder su validez y eficacia; al igual éstas regularizan el mensaje de datos desde su envío hasta la recepción.

En la Ley ecuatoriana en el Artículo once hace una clara diferenciación al envío y recepción de los mensajes de datos.

Art. 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

- **Momento de emisión del mensaje de datos**.- Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto;
- **Momento de recepción del mensaje de datos**.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalada por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos.
- **Lugares de envío y recepción**.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales,

el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos.

Se advierte claramente, como la ley pretende normar este proceso de comunicación.

En la ley venezolana se menciona esto, en el capítulo tercero referente al intercambio de mensajes de datos y en el Artículo noveno reglamentan el proceso para la emisión de mensajes de datos:

> Las partes podrán acordar un procedimiento para establecer cuándo el Mensaje de Datos proviene efectivamente del Emisor. A falta de acuerdo entre las partes, se entenderá que un Mensaje de Datos proviene del Emisor, cuando éste ha sido enviado por:
>
> 1. El propio Emisor.
> 2. Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje.
> 3. Por un Sistema de Información programado por el Emisor, o bajo su autorización, para que opere automáticamente.

En el capítulo tercero de la ley colombiana, se reglamenta la comunicación de los mensajes de datos y de la validez de los contratos electrónicos:

> **Artículo 14**. Formación y validez de los contratos. En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

También se menciona la presunción del origen del mensaje:

> **Artículo 17**. Presunción del origen de un mensaje de datos. Se presume que un mensaje de datos ha sido enviado por el iniciador cuando:
>
> 1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o
>
> 2. El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

A diferencia del resto de capítulos vistos hasta ahora, respecto a los mensajes de datos, el colombiano es el más completo ya que cubre los aspectos que las otras leyes ignoran, tales como la duplicidad del mensaje, tiempos de envío y recepción del mensaje, aspecto jurídico y presunción de recepción.

En la Ley argentina esto se cubre brevemente en el capítulo primero en generalidades, en tres Artículos el 6, 7, 8.

> **Artículo 6º** Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.
>
> **Artículo 7º** Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.
>
> **Artículo 8º** Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

Claramente se aprecia que esta ley contiene menos normas que sus pares.

En el tercer capítulo, Artículo 29 la entidad certificadora según la ley ecuatoriana se explica que:

> Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

En el capítulo tercero, Artículo 17 en la Ley argentina se explica sobre el certificador licenciado (entidad de certificación):

> Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

En el capítulo quinto de la ley venezolana, se define a la entidad de certificación en sus Artículos 20 y 21:

> **Artículo 20** Se crea la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.
> **Artículo 21**. La Superintendencia de Servicios de Certificación Electrónica tiene por objeto acreditar, supervisar y controlar, en los términos previstos en este Decreto Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados.

En la Ley ecuatoriana definen a los certificados de firma electrónica como:

> **Artículo 20** Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

En la Ley colombiana:

> Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación

En la Ley argentina dice lo siguiente:

> Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

Por último en la venezolana:

> La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:
> 1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
> 2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
> 3. No alterar la integridad del Mensaje de Datos.
> A los efectos de este Artículo, la Firma Electrónica podrá formar parte integrante

del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

Como se observa las leyes regulan la validez de los certificados y/o las firmas sean éstas digitales o electrónicas. La diferencia entre la una y la otra, es el valor probatorio, en un documento que esté firmado digitalmente, automáticamente es atribuido de genuino, al menos que se pruebe lo contrario, en el caso de la firma electrónica la situación es la siguiente: a la persona que alega que la firma es genuina, ésta debe probar el hecho.

Tecnológicamente las firmas digitales se basan en una infraestructura de llave pública (PKI), ésta nos da la seguridad de la autenticidad de la información y la confianza entre las partes (emisor y receptor), entre otras funciones.

Diferencias.

Las principales diferencias entre las leyes se establecen en que, la ecuatoriana no trata mucho sobre el comercio electrónico. La colombiana, enmarca el entorno de la ley en el comercio electrónico en la parte segunda, Artículo 26. La venezolana no habla sobre el comercio electrónico solo reglamenta lo referente a mensajes de datos y los certificados, la ley argentina, solo reglamenta al comercio electrónico y en este aspecto se apoya en leyes de defensa del consumidor, Código Civil y el Código de Comercio.

La ecuatoriana a diferencia de las otras, habla de los delitos informáticos/electrónicos con el espíritu de reformar el Código Penal, éste se encuentra en el título quinto de la ley.

La ley colombiana no especifica delitos informáticos.

En Colombia se habla de la modificación mediante acuerdo en lo que se refiere a los contratos, entre estos se encuentran: la formación y validez del contrato, reconocimiento de los mensajes de datos por partes, atribución del mensaje de datos entre otros.

En la Ley argentina se habla del sistema de auditoría que se aplicará a la autoridad certificante en el capítulo séptimo, Artículos treinta y tres y treinta y cuatro.

También habla de la Comisión Asesora para la Infraestructura de Firma Digital, que tiene como fin el emitir recomendaciones respecto a estándares tecnológicos, metodología y requerimiento de resguardo físico de información, entre otros. Todo esto se encuentra en el Capítulo Octavo.

La Ley venezolana habla respecto a la sana crítica si la Firma Electrónica no cumple con los requisitos. (Artículo 17)

En la Ley ecuatoriana se da importancia al tema de la propiedad intelectual en el Artículo 4 indicando que los mensajes de datos se encuentran protegidos por las leyes internacionales respecto a dicha materia.

También se aclara en la ley ecuatoriana que la extinción del certificado o de la firma digital no exime al titular de las obligaciones obtenidas anteriormente.

En el Artículo de la Ley ecuatoriana también se habla de las sanciones administrativas en el Artículo 40 del Capítulo cuarto que tiene de título: “De Los Organismos De Promoción Y Difusión De Los Servicios Electrónicos, Y De Regulación Y Control De Las Entidades De Certificación Acreditadas”.

En el Capítulo tercero de la ley ecuatoriana se habla de los derechos de los usuarios o consumidores de los servicios electrónicos, por ejemplo se menciona el consentimiento al acceso a su información, aceptar mensajes de datos como registros electrónicos; contemplado en los Artículos 49 y 50 de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Digitales.

4. CAPÍTULO IV

4.1. PASOS PARA REALIZAR UN ANÁLISIS FORENSE Y ANÁLISIS DE CUATRO CASOS REALES

En este capítulo se van a explicar los pasos para realizar un análisis forense informático e identificarlos en cuatro casos reales.

4.1.1. Fases de un Análisis Forense

La informática forense es una ciencia que consta de procesos estructurados claramente.

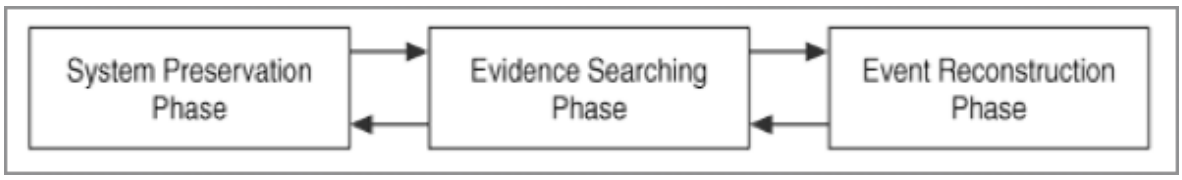


Figura 4.1.1.1: Fases del análisis forense
Fuente: File System Forensic, Wesley

En la figura 4.1.1.1 se puede observar las tres fases mayores de un análisis forense.

Cada fase tiene sus características.

4.1.1.1. Fase de preservación de la evidencia

Es la primera fase del análisis forense, aquí se intenta preservar la escena de crimen, para poder realizar un análisis más real.

Cada acción se debe hacer considerando el contexto y el ambiente legal; habrá casos en donde se necesite desconectar el equipo para evitar alteraciones por parte del atacante o

por procesos maliciosos y sea necesario hacer una copia de seguridad completa del sistema; otro caso por ejemplo, no se podría apagar al equipo porque se investiga algún programa espía o es un señuelo (honeypot[15]) en estos casos no sería posible realizar respaldos. El fin de toda esta fase es evitar viciar la evidencia que se obtendrá.

Entre las técnicas de preservación de la evidencia se procede a desconectar la computadora evitando la secuencia normal de apagado, así evitar rutinas del sistema operativo que puedan inferir en la preservación de la evidencia y proceder a desmontar la unidad de disco duro para realizar un duplicado mediante imagen e incluir bloqueadores de escritura.

Existen dos tipos de bloqueadores de escritura, en soporte físico y en lógico.

- **El físico** se coloca entre el equipo y el dispositivo de almacenamiento, analizando cada comando enviado.

Estos protectores de escritura soportan las interfaces más comunes tales como USB, SATA, SCSI entre otros.

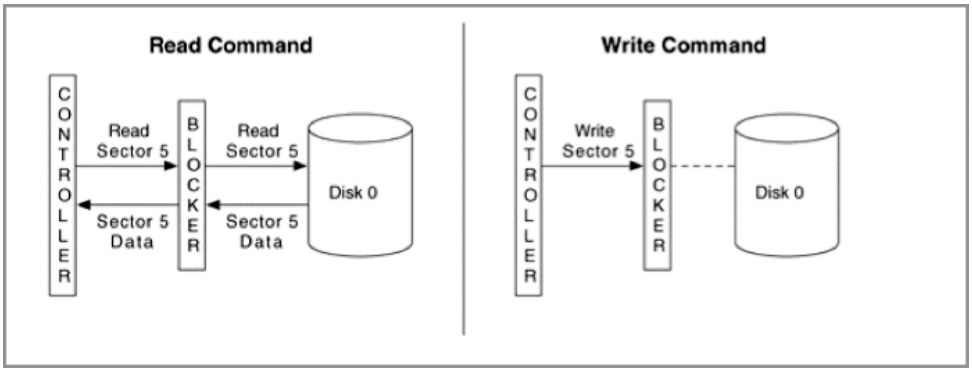


Figura 4.1.1.1.1: Bloqueo de escritura en soporte físico
Fuente: File System Forensic, Wesley

[15] Se denomina honeypot a un programa informático que simula ser un sistema vulnerable para atraer atacantes.

- **Bloqueo de escritura mediante soporte lógico**

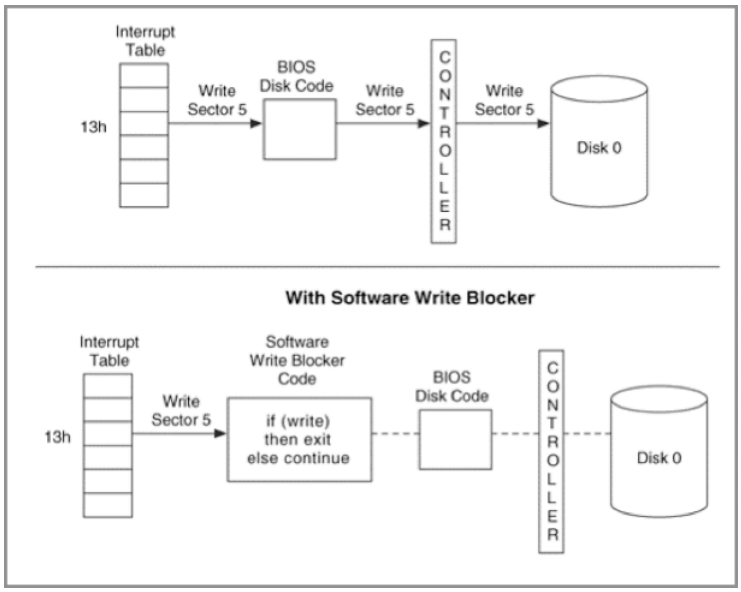


Figura 4.1.1.1.2: Bloqueo de escritura mediante soporte lógico
Fuente: File System Forensic, Wesley

Las herramientas de informáticos forenses corrían en DOS, donde se hacía uso de una de las interrupciones del sistema operativo, la Int 13 h; interrupción que supervisa las funciones de lectura/escritura para el disco duro. Actualmente, los sistemas operativos Linux (GNU/Linux) y los derivados de NT (Windows XP, Server 2.003) entre otros, interceptan la interrupción Int 13 h y en lugar de apuntar al código de servicio de BIOS, pasan al mecanismo nativo del sistema operativo; lo que hace un bloqueador de escritura mediante soporte lógico mediante la alteración de las tablas de interrupción que son dirigidas hacia éste.

La principal diferencia entre los bloqueadores de escritura basados en soporte lógico y los de soporte físico es en la eficacia. Los bloqueadores basados en soporte físico son más eficaces ya que se ponen entre el dispositivo de almacenamiento y el equipo, rastreando, toda la comunicación a diferencia del segundo bloqueador de escritura que al ser un programa este puede ser vulnerado o evadido las restricciones sin cometer su objetivo.

Lo anterior es aplicable a un análisis en cadáver[16], sin embargo, si no se tiene la posibilidad o la situación no permite el referido análisis, se deberá suspender toda conexión a red y conectar al equipo a un dispositivo de red vacío, así se evitará todo mensaje de error de conexión o en su defecto utilizar filtros de red; en cualquiera de los dos casos el objetivo es evitar que el atacante altere la evidencia. Otra medida a realizar sería el sacar respaldo de toda la evidencia para así en caso de una sobre escritura tener donde investigar.

Como lo que se busca es probar el suceso, sea que se realice una investigación en cadáver o no; siempre se debe demostrar que la evidencia no ha sido viciada, esto se puede realizar mediante sumatoria de hash que evidencian de manera irrefutable la autenticidad de las pruebas a presentar (documentos, etc).

4.1.1.2. Fase de búsqueda de evidencia

Ya se aseguró la "escena del crimen", lo siguiente es investigar; se busca evidencia que soporte o refute la hipótesis.

Al igual que en una investigación de un crimen "normal", en la investigación de informática forense, se empieza por los lugares más comunes de acuerdo con el incidente, por ejemplo si se está investigando un caso de pornografía infantil se investiga los hábitos de navegación del sospechoso.

Al buscar indicios de una intrusión a un sistema operativo, se comienza buscando signos de rootkits, usuarios no autorizados, etc. La búsqueda es relativamente "sencilla", se debe idear qué se va a buscar y sus características; por ejemplo si interesa documentos *pdf*, se revisa todo archivo que tenga extensión *pdf* (nombre.pdf). Es así como el investigador debe visualizar lo que busca y así poder obtener características claves para poder encontrar.

[16] Se refiere al tipo de análisis forense que se realiza en una imagen del disco más no en el equipo comprometido. (Ver Clasificación de la informática forense)

En la mayoría de casos se investigará el computador sospechoso realizando búsquedas en sistemas de archivos o en los archivos de acuerdo con el nombre, patrones, palabras clave o incluso con archivos ocultos y línea de tiempo. Para todo esto el investigador se ayuda con herramientas desde forenses a "comunes", entre estas se tiene al *Google Desktop Search,* una herramienta para búsqueda en el sistema operativo de información tales como archivos, directorios, música e imágenes.

En el sitio web *Security by default,* muestra como se puede dar un uso forense gracias a las características de la herramienta. Esta herramienta crea un pequeño servidor dentro del equipo que indexa todo a nivel de archivo, permitiendo mostrar como evidencia los archivos contenidos; tiene sus limitaciones pero no deja de ser una ayuda, mediante añadidos se puede ampliar su catálogo de búsqueda e incluso que muestre la fecha de modificación en lugar de la de indexación.

Dentro de la Fiscalía General del Estado se tiene una guía relacionada a la evidencia digital y otro manual respecto a los delitos informáticos.

Referente a las evidencias, éstas deben cumplir las siguientes características:

- **Objetividad**: El investigador debe cumplir los principios de ética profesional.
- **Autenticidad y conservación**: Durante la investigación se debe mantener la integridad de los medios probatorios.
- **Legalidad**: El perito debe conocer la ley respecto a su actividad y cumplir los requerimientos en la ley respecto a la designación como perito.
- **Idoneidad**: Las herramientas probatorias deben ser auténticas, relevantes y suficientes para el caso.
- **Inalterabilidad**: Se debe respetar la cadena de custodia.
- **Documentación**: Se debe documentar todo el proceso pericial.

Todos estos principios garantizarán la legalidad de las pruebas.

Legislación ecuatoriana en comercio electrónico en el capítulo primero del título primero, Artículo segundo dice: “Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento”.

En lo concerniente a las evidencias se tiene el soporte físico y el lógico, para que tenga valor probatorio se debe distinguir lo siguiente:

Evidencia	**Explicación**
Soporte físico como fruto del delito o mercancía ilegal.	Cuando su tenencia está prohibida por la ley.
Soporte físico como herramienta.	Cuando cumple un papel importante en el delito.
Soporte físico como evidencia.	Cuando no es ni herramienta para un delito o es mercancía ilegal o fruto de un delito.

Evidencia	Explicación
Mensajes como medios de prueba.	Artículo 53 LCE: Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.
Información como fruto del delito o tenencia ilegal.	Cuando su tenencia está prohibida por la ley.
Información como instrumento.	Cuando es instrumento para cometer una infracción.

Tabla 4.1.1.2.1: Explicación te tipos de evidencias con valor probatorio.
Fuente: Manual de manejo de evidencia de la Fiscalía General del Estado

Otros aspectos aparte de los tecnológicos al momento de recuperar la evidencia, también se debe cumplir con responsabilidades en la escena del crimen cómo:

- En caso de ser necesaria una incautación de equipos, tener lista una orden judicial para la incautación y el acceso a la información almacenada.
- Saber a qué hora se debe realizar la incautación para minimizar riesgos para el personal y a la evidencia.
- Entrar sin previo aviso.
- Preparar previamente los materiales.

- Realizar simultáneamente las incautaciones en diferentes lugares.
- Crear respaldos en el lugar.
- Grabar, fotografiar la evidencia y el sitio del crimen.
- Etiquetar la evidencia.
- Obtener códigos, contraseñas de acceso.
- Obtener documentos que contengan información de acceso, redes.
- Cualquier otra evidencia necesaria.

En el informe ejecutivo consta de:

- Motivos de la intrusión.
- Desarrollo de la intrusión
- Resultados del análisis.
- Recomendaciones.

La diferencia entre el uno y el otro es grande como se puede observar, el técnico justamente es eso, se dirige hacia personas con conocimiento amplio de la materia y engloba toda la parte operativa y "por menores" de la investigación.

El ejecutivo va dirigido hacia personas "comunes", en donde se explica a grandes rasgos toda la intrusión en términos sencillos.

4.1.1.3. Fase de reconstrucción del evento.

Esta es la última fase del proceso de investigación forense.

Con la evidencia se debe revelar los hechos ocurridos; habrá evidencia que se recupera que sea relevante. Para tal efecto, es importante tener claro para los hechos que se investigan. Se necesita además, conocimiento respecto al sistema operativo que se analiza, pues no se

tiene los mismos eventos entre versiones de sistemas operativos e incluso entre diferentes versiones del mismo navegador o sistema operativo.

La reconstrucción del evento se debe comparar con la evidencia física. Se tiene tres clases de reconstrucciones:

- **Relacional**: Se basa en la evidencia obtenida que muestran la relación del objeto con la escena del delito y su interacción con el resto de objetos.
- **Funcional**: En donde se indica la función de cada objeto que se encuentra en la escena del delito y cómo son usados.
- **Temporal**: Ubica en la línea temporal de los hechos en la escena del delito y muestra la relación de los hechos con la evidencia.

A esto se suma que debe ir acompañado con el informe ejecutivo y el técnico.

El informe técnico consta de:

- Antecedentes del hecho.
- Recolección de los datos.
- Descripción de la evidencia.
- Entorno del análisis.
- Descripción de las herramientas.
- Análisis de la evidencia.
- Información del sistema analizado.
- Características del Sistema Operativo.
- Aplicaciones.
- Servicios.
- Vulnerabilidades.
- Metodología.
- Descripción de los hallazgos.

- Huellas de la intrusión.
- Herramientas usadas por el atacante.
- Alcance de la intrusión.
- El origen del ataque
- Cronología de la intrusión.
- Conclusiones.
- Recomendaciones específicas.
- Referencias.

4.1.2. Análisis de casos

A continuación se presentarán cuatro casos de delitos informáticos: dos nacionales y dos extranjeros de delitos informáticos, en donde se identificará el delito, sustento legal para que sea delito, clasificación nacional e internacional, fases del análisis en el caso, sanción nacional que se le imputaría.

Los casos internacionales a ser revisados son: el primero correspondiente a “phishing” que es un delito de suplantación de identidad, junto con extorsión y estafa; luego, se presentará el caso español de pornografía infantil, en la cual se evidencia en forma mucho más clara el procedimiento pericial que se siguió para determinar los culpables y responsabilidades en el mismo.

Con relación a los procesos judiciales locales cometidos a través de medios informáticos, se revisa un juicio de injurias, así como también, el conocido caso “Raúl Reyes”. De estos dos procesos se revelará claramente que se cuenta con muy pocos avances en materia pericial informática.

4.1.2.1. Caso recargasmasmovil.net

El caso en estudio es de marco internacional, ocurrió el 29 de septiembre de 2009, en España. Se refiere a un usuario que utilizó un chip de una operadora prepago, pues el banco no realizaba los abonos a esa operadora. El usuario al buscar en Google "recargas más móvil" y de entre los resultados escoger uno de publicidad "Google Ad Sense"[17], le llevó al sitio falso de una empresa recargasmasmóvil.

De requerir ampliar esta información, se la puede encontrar en el sitio web: http:// www.securitybydefault.com/2009/09/el-extrano-caso-de-recargamasmovilnet.html

- **Fase de preservación de evidencia.**

Al ser el usuario una persona entendida en el entorno informático, se dio cuenta inmediatamente que no es un sitio de la empresa "recargas más móvil" sino uno ficticio, siendo éste una concurrencia de varios delitos entre los que se puede nombrar a la estafa, conocido internacionalmente como "phishing".

Todo este caso transcurre en el sitio web falso de "Recargas más móvil", hospedado en España, con el fin de obtener información financiera como es el número de tarjeta, nombre, dirección, correo electrónico entre otros para poder lucrar con la venta de esta información.

- **Fase de búsqueda de evidencia.**

En esta pantalla (figura 4.1.2.1.1) se puede ver el sitio que simula ser de "*Recargas más móvil"*, en donde se debe ingresar el número de teléfono al que se le va a realizar la recarga.

[17] Es un programa de publicidad gratuita de Google.

Figura 4.1.2.1.1: Sitio web falso Recarga más móvil

Fuente: Security by default (http://www.securitybydefault.com/2009/09/el-extrano-caso-de-recargamasmovilnet.html)

Al ingresar el número de teléfono, redirecciona a un programa para recargar, en donde no usa cifrado (HTTPS), se encuentra ausente esta seguridad, al igual que clave de internet.

Figura 4.1.2.1.2: Pantalla de ingresos de datos.

Fuente: Security by default (http://www.securitybydefault.com/2009/09/el-extrano-caso-de-recargamasmovilnet.html)

El protocolo HTTPS, que es el mismo HTTP con una capa de seguridad adicional que justamente se la utiliza para estos tipos de transacciones que protegen datos sensibles como números de tarjetas bancarias, nombres de usuarios, contraseñas, etc. Es obvio e

imprescindible para empresas o corporaciones serias, implementar un sistema de seguridad adecuado en sitios que realicen operaciones con datos en el Internet ya que cada vez es más común este tipo de operaciones.

Un sitio falso (de suplantación de identidad), lo que busca es obtener los datos de la víctima, como datos de tarjetas de crédito, nombre y apellido, teléfono, dirección.

Al observar el código fuente se puede ver un procedimiento que llama a un formulario de correo electrónico (*emailmeform*) a través de un *CGI*[18] que es un programa que se ejecuta en un servidor que es llamado por el sitio para realizar una cierta función, como es en este caso de un servicio que se llena y envía un correo electrónico con los datos llenados, como es común cuando se da de alta en el sitio.

Figura 4.1.2.1.3: Llamada al CGI.
Fuente: Security by default(http://www.securitybydefault.com/2009/09/el-extrano-caso-de-recargamasmovilnet.html)

Como se puede leer en la línea uno de la imagen 4.1.2.1.3 se puede ver la llamada después de la etiqueta *action*.

Si se ejecuta una consulta al dominio con el comando *Who Is,* se puede observar la fecha de creación del dominio, a nombre de quien se encuentra registrado, nombre del servidor en donde se encuentra el sitio, fecha de expiración del dominio, y estado.

[18] Common Gateway Interface (español: Interface de Acceso Común)

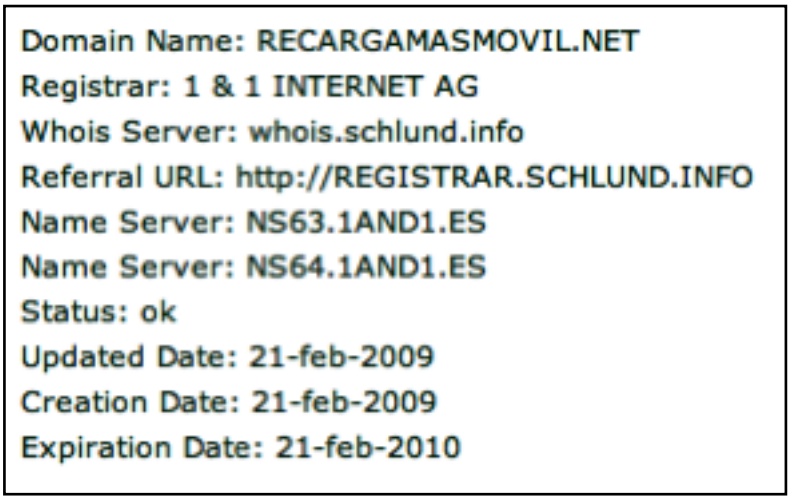


Figura 4.1.2.1.4: Resultado del comando Who Is.
Fuente: Security by default (http://www.securitybydefault.com/2009/09/el-extrano-caso-de-recargamasmovilnet.html)

De esta información se puede deducir que la estafa estaba operando desde el año 2009 y si se usa un programa de rastreo se puede ver por la IP que el servidor se encuentra en España.

- **Fase de reconstrucción de eventos**

Con la evidencia recolectada se realizó la reconstrucción funcional del evento, como se aprecia en el párrafo anterior, en este caso se revela la importancia del proceso forense para analizar su sitio fraudulento. Para determinar el sustento legal y la sanción nacional que se le imputaría si fuese cometido en el territorio nacional, se debe remitir al Capítulo IV numeral 4.3 sobre la "CLASIFICACIÓN DE LOS DELITOS".

4.1.2.2. Caso de pornografía infantil

Este caso es mucho más grave ya que involucra a menores de edad, aquí se usa la tecnología para atentar contra la dignidad y el pudor de otra persona. También, se encuentra revelado el hecho que la pornografía infantil abunda en el Internet; como se observará más adelante. En el caso se encuentra involucrada una menor de edad que es

filmada en una situación comprometedora y el vídeo es publicado por un conocido de la víctima que también es un menor de edad.

Este hecho ocurrió en España, el 13 de abril del 2010, y si se quiere mayor información se puede consultar al sitio web: http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1

Cuentan que una chica llamada Silvia fue grabada desde un teléfono móvil en actitudes indecentes. En el colegio todo el mundo habla de que existe un enlace de acceso a una descarga del vídeo desde Rapidshare.

Se inicia el rumor por el colegio donde Silvia y Mirian estudian. Los profesores alertados por el problema deciden hablar con la chica y con sus padres. El caso se denuncia en la comisaría más próxima. Los padres acusan a dos compañeros de abusar de su hija (en el juicio quedó patente que fue consentido) y quieren que se requise todas las pruebas posibles que incriminen a los chicos. Curiosamente el iPhone ha desaparecido.

Proceso forense

Durante el proceso de análisis de los equipos informáticos se encuentra que tiene iTunes, éste es un reproductor de música y sirve para la sincronización entre dispositivos de Apple tales como iPod, iPhone o iPad con el equipo sea Mac o PC; para esto, iTunes dispone de un controlador específico para cada Sistema Operativo, estos sirven para que haya comunicación segura entre el dispositivo y el equipo, cuando se hace una copia de seguridad.

La copia de seguridad se almacenan en dos archivos cuando el ordenador es Windows: mddata y mddinfo. Entre los datos que se obtienen respaldo se encuentran:

- Marcadores, historial de navegación, cookies.
- Ajustes, preferencia y datos de aplicaciones.

- Agenda.
- Fondos de pantalla.
- Cuentas de calendario.
- Cuentas de Mail.
- Notas.
- Carrete.
- Vídeos en el carrete.
- Compras in app.

Estas copias se encuentran en los siguientes directorios dependiendo del Sistema Operativo:

- Windows XP: \Documents and Settings\(nombredeusuario)\Application Data\Apple Computer\MobileSync\Backup\
- Windows Vista / Windows 7: C:\Users\(nombredeusuario)\AppData\Roaming\Apple Computer\MobileSync\Backup\

Cuando el iPhone en este caso es conectado por primera vez, iTunes crea una carpeta con 40 caracteres alfanuméricos que es un identificador único en este caso era "0387fecb24b358ec337ab2ad3323fb8e0bbc27ca". Esta carpeta tiene los respaldos del iPhone para este caso; el contenido de esa carpeta tiene varios archivos que se irán a continuación identificando:

PLIST

Estos tipos de archivos que tienen extensión *plist* se dividen en tres que son info.plist que tienen información respecto a la fecha cuando se sacó respaldo, nombre del dispositivo asignado por el usuario, número de serie y número de teléfono.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.
<plist version="1.0">
<dict>
    <key>Build Version</key>
    <string>7E18</string>
    <key>Device Name</key>
    <string>Al3x</string>
    <key>Display Name</key>
    <string>Al3x</string>
    <key>GUID</key>
    <string>6ECF6D9297E5960C5C5FCE4A0C984060</string>
    <key>ICCID</key>
    <string>8934075100148819428</string>
    <key>IMEI</key>
    <string>011982000306700</string>
    <key>Last Backup Date</key>
    <date>2010-03-08T10:40:28Z</date>
    <key>Phone Number</key>
    <string>60          </string>
    <key>Product Type</key>
    <string>iPhone2,1</string>
    <key>Product Version</key>
    <string>3.1.3</string>
    <key>Serial Number</key>
    <string>83937BDB3NP</string>
    <key>Target Identifier</key>
    <string>0387fecb24b358ec337ab2ad3323fb8e0bbc27ca</string>
    <key>Target Type</key>
    <string>Device</string>
    <key>Unique Identifier</key>
    <string>0387FECB24B358EC337AB2AD3323FB8E0BBC27CA</string>
```

Figura 4.1.2.2.1: Archivo info.plist.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

Ahora también se tiene los otros archivos *plist* que se van a explicar a continuación.

Status.plist:

En este documento *plist* se almacena el estado de la copia de seguridad, sincronización anterior. Si se realizó correctamente la copia o el sincronizado indica que se realizó correctamente.

El tercero de los archivos *plist* es *manifest.plist* en este archivo es un binario de los archivos de la copia de seguridad con su respectiva firma digital.

Los archivos *plist* tienen información en XML.

Archivos MDINFO y MDDATA

Estos actúan como uno, cada uno tiene información que complementa al otro, en el primero tiene información en metadatos[19] respecto al archivo, por ejemplo: contactos, historial de llamadas, etc. En cambio *mddata* contiene la información real.

- **Fase de preservación.**

En este caso se confiscó los equipos informáticos para poder realizar los respectivos análisis, se sacaron imágenes del disco, para preservar la evidencia. También se tomaron fotografías de los equipos en su ubicación original.

- **Búsqueda de evidencias.**

Se tiene una carpeta que tiene de nombre *0387fecb24b358ec337ab2ad3323fb8e0bbc27ca*, como se explicó, contiene los archivos que se mencionó en la página sesenta y dos. Algunos de estos ficheros tienen estructura de SQLite.[20]

En una primera instancia se procedió a buscar indicios de que si se mandó algún mensaje de texto (SMS) desde el teléfono a alguien avisando sobre el vídeo y si proporcionó algún enlace de descarga.

Para la búsqueda de indicios se usó patrones comunes:

- **sms.db**: SMS.
- **call_history.db**: Histórico de llamadas.
- **notes.db**: Agenda y notas.

[19] Los metadatos son datos asociados a un documento digital que recogen información fundamentalmente descriptiva (autor, título, etc.). También pueden incluir información de administración (creación del recurso, derechos, control de acceso …), y preservación (tipo de formato, etc.). Fuente:e-archivo.uc3m.es/help/glosario.html

[20] Base de datos que se integra en la aplicación, el programa realiza llamadas de subrutinas y funciones.

Figura 4.1.2.2.2: Patrones de búsqueda.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

En la figura 4.1.2.2.2 se puede observar que se usó el comando *grep*[21], este comando lo que hace es listar archivos que contengan los patrones que se le proporciona en la entrada.

Es decir en este caso se usa *grep -i sms.db* al incluir "-i" no hace distinción entre mayúsculas y minúsculas y la salida del comando el archivo que como se aprecia incluyeron archivos *mdinfo* .

Si se abre desde un editor de hexadecimales se observa el formato de SQLite.

[21] grep [opciones] PATRÓN [ARCHIVO...]

Figura 4.1.2.2.3: Información de archivo mdlist.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

En la línea uno se puede apreciar que está escrito en SQLITE versión tres.

También se puede observar en la línea dieciséis que se halla un fragmento de un SMS[22].

[22] Mensaje de texto

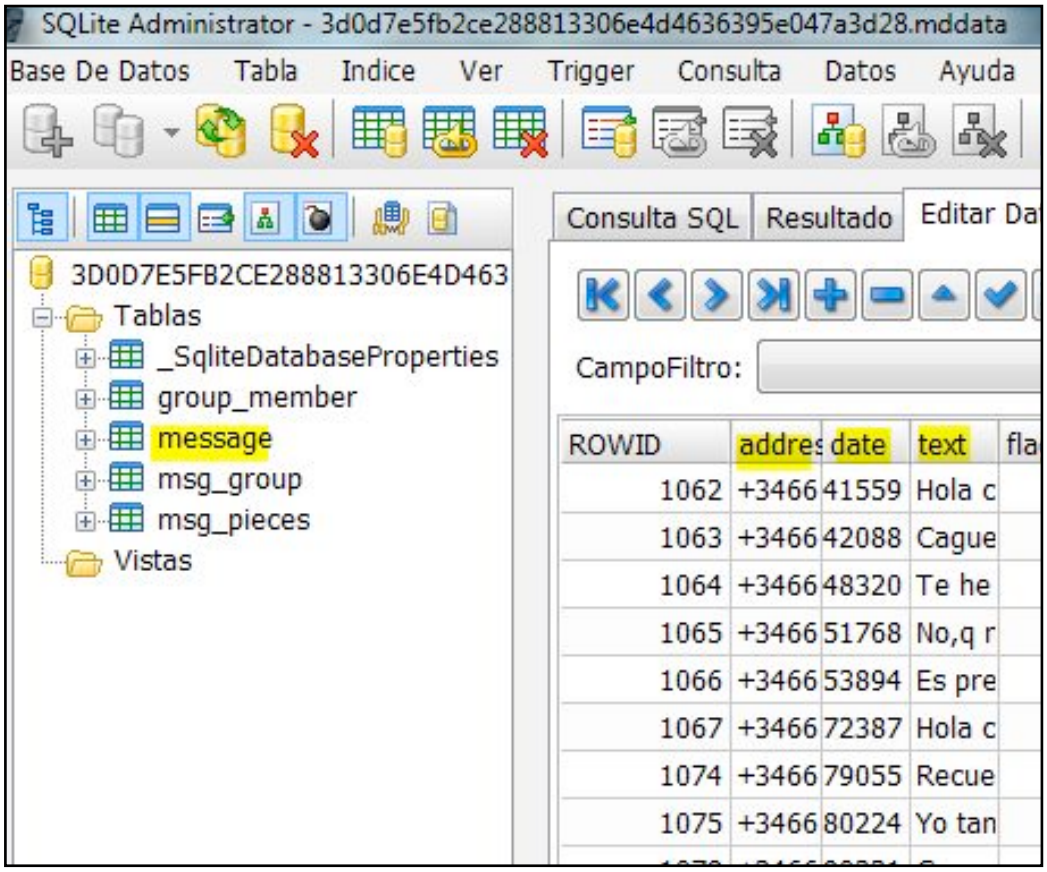


Figura 4.1.2.2.4: Información de la tabla de SMS.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

Al abrir se ve en la tabla *message* claramente los números de teléfono, fecha del envío y el texto del SMS.

Buscando un poco más, se puede encontrar un mensaje de texto revelador en donde se informa que se ha subido un vídeo a *Filestube* como se puede ver en la imagen siguiente.

Figura 4.1.2.2.5: Mensaje donde se indica la ubicación del vídeo.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

Haciendo una búsqueda usando *grep* que contenga el patrón *filestube* se obtuvo lo que se puede observar en la figura 4.1.2.2.6.

Cabe recordar que *grep* lo que hace es buscar patrones en un archivo.

Al ejecutar el comando se obtiene la siguiente salida.

Figura 4.1.2.2.6: Ubicación del vídeo.
Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

Ahora al verificar la dirección se tiene como resultado el vídeo que se encuentra todavía disponible.

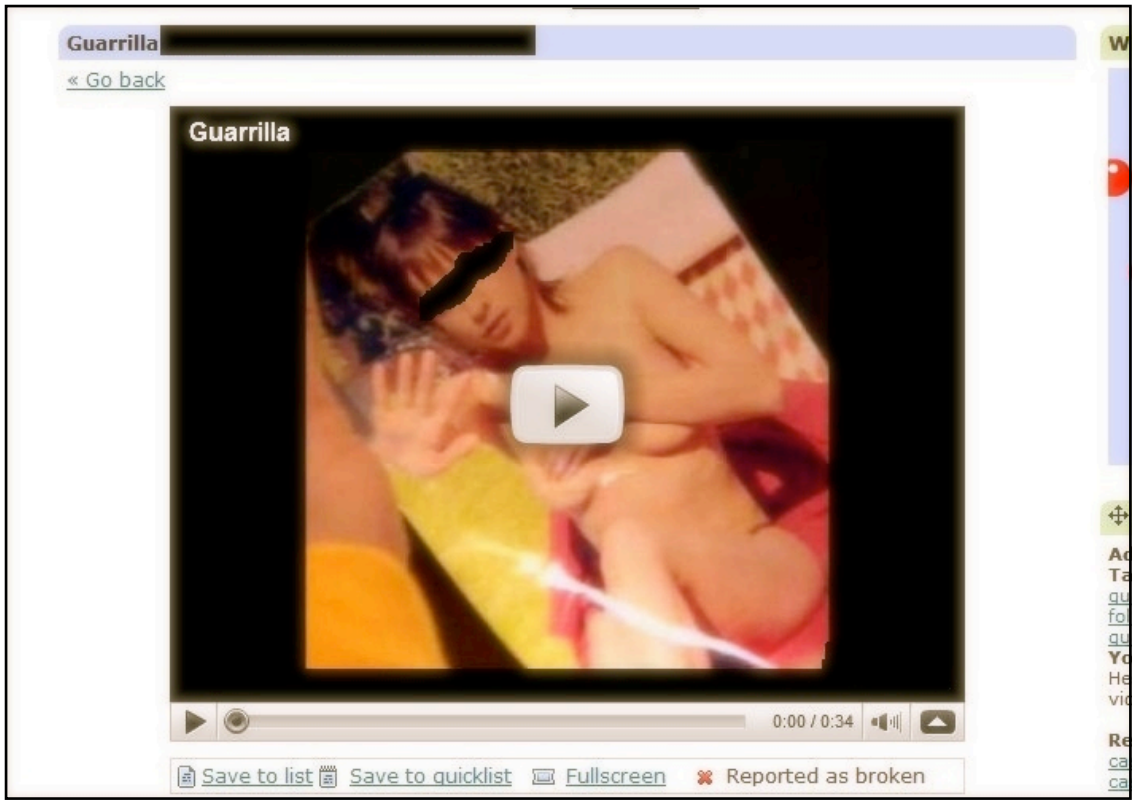


Figura 4.1.2.2.7: Vídeo.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

En el proceso de sincronización es lógico que esté en el computador algunos archivos del iPhone como imágenes, vídeos, etc.

Lo primero que se realizó es buscar algún vídeo del formato que graba el iPhone qué es MP4, MOV, entre otros.

El MP4 es un archivo de audio y vídeo popularizado por Apple y su reproductor iTunes y es un estándar de la ISO/IEC y el grupo MPEG[23].

El formato MOV (Quicktime Movie) es de Apple y es un formato de vídeo, también es capaz de transmitir vídeos de alta definición.

[23] http://es.wikipedia.org/wiki/Mp4

En la búsqueda de vídeos no se encontró ninguno que pertenezca a este caso.

Respecto a imágenes se tienen los siguientes formatos de archivos.

- Ficheros ITHMB: Contiene la galería (carrete) de imágenes.
- Ficheros BTH: Son archivos de datos BATHY Recorder.
- Ficheros THM: Es utilizado por muchas aplicaciones diferentes para almacenar miniaturas.
- Ficheros THL: Es utilizado para las imágenes de los íconos.
- Ficheros THP: Son ficheros de vídeo muy utilizados en la Gamecube de Nintendo.

En la imagen 4.2.2.6 se observa claramente los resultados que muestra el comando *dir*; este comando de MS-DOS y la consola de comandos de Windows en la actualidad que se usa para listar el directorio y su contenido. El comando *Dir* tiene varias opciones para filtrar el resultado y hacerlo más preciso. Entre sus opciones existen comodines como el asterisco (*) que reemplaza toda una cadena de caracteres (nombre), si se pone *dir *.doc* se listará todos los archivos de Word (*.doc*), como se puede ver en la sintaxis del comando[24], se puede observar *[/S]* que es la misma opción que se usa en la imagen, este parámetro sirve para listar los archivos y sus subdirectorios. Claramente se puede evidenciar en las dos ventanas que tienen un listado de directorios y archivos.

[24] DIR [unidad:][ruta][archivo] [/A[[:]atributos]] [/B] [/C] [/D] [/L] [/N] [/O[[:]Orden]] [/P] [/Q] [/S] [/T[[:]fecha]] [/W] [/X] [/4]

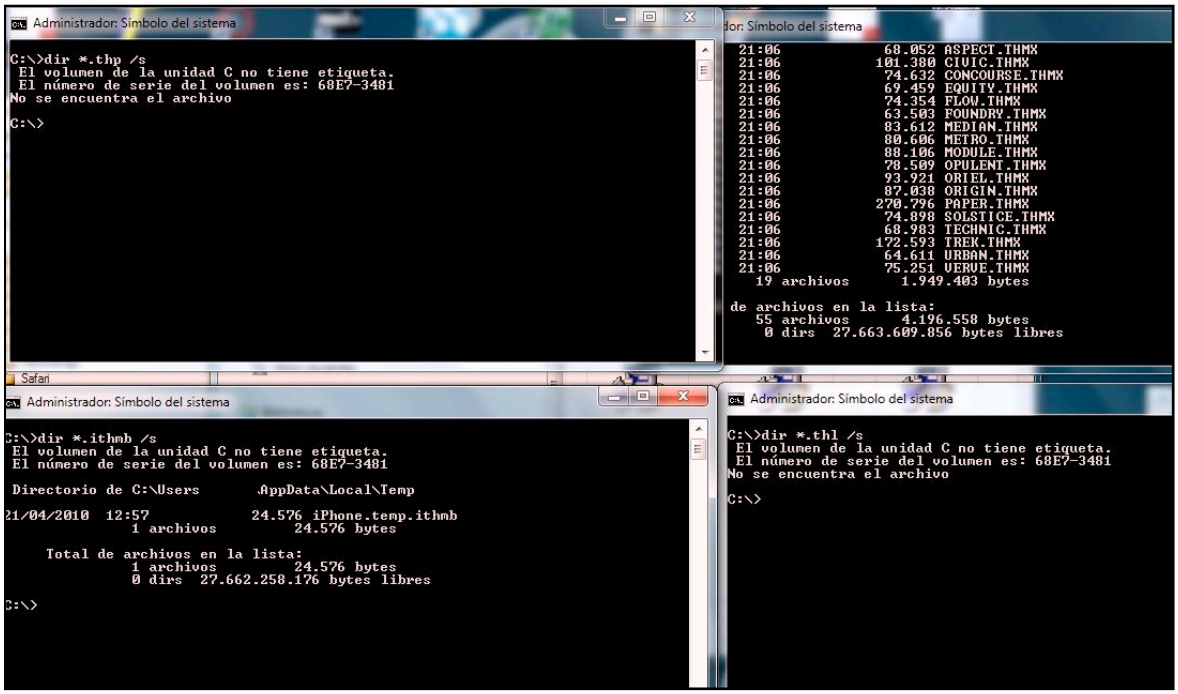


Figura 4.1.2.2.8: Búsqueda de imágenes.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

Se tiene dos ventanas que presentan espacio de investigación.

Los ficheros *ithmb* contiene el carrete (colección de imágenes) si alguna vez existió un vídeo es natural que tenga su respectivo archivo *ithmb*.

Se usó la utilidad *iThmbConv.exe* que extrae el contenido del archivo *ithmb* y sacando las miniaturas.

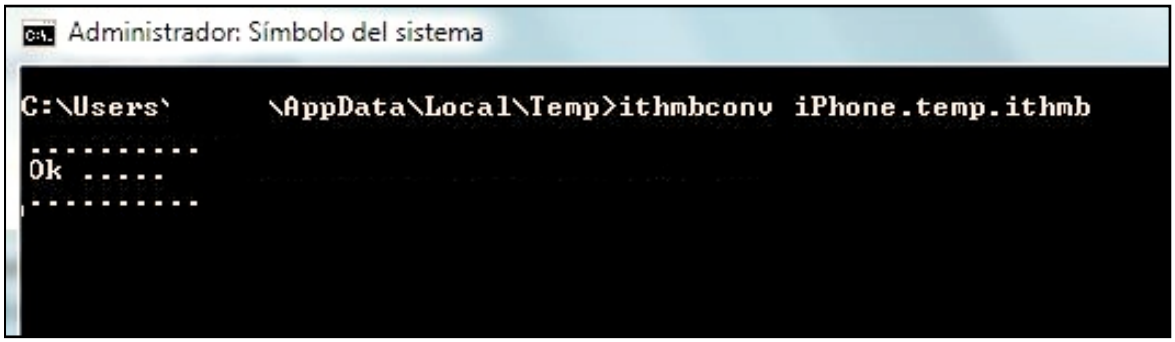


Figura 4.1.2.2.9: Extrayendo miniaturas.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

Y ahora entre las miniaturas se puede observar la miniatura del vídeo.

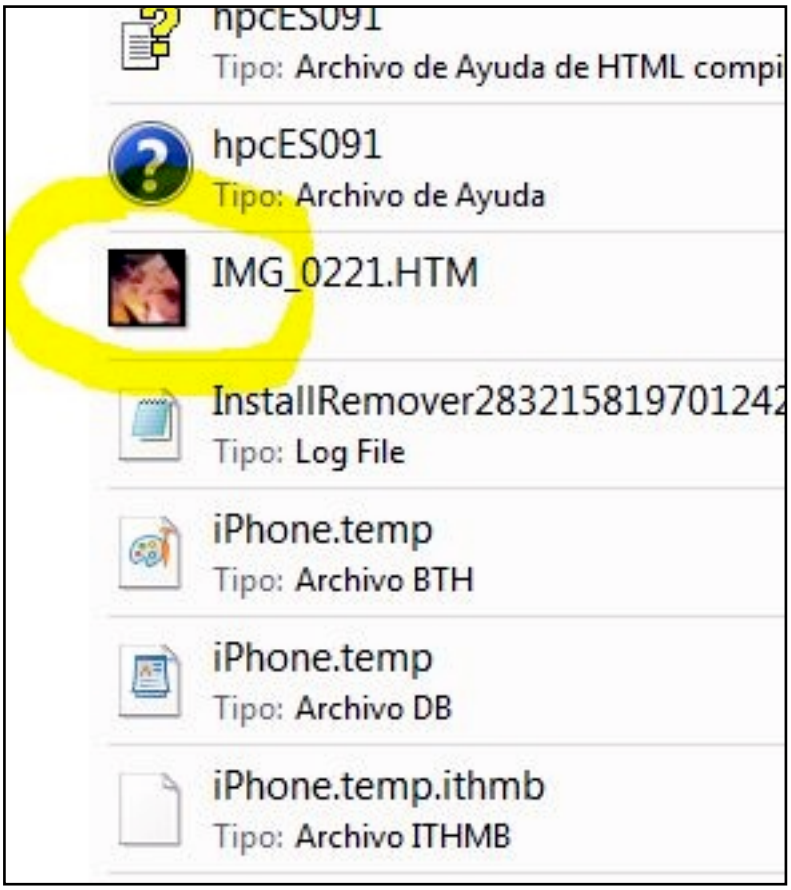


Figura 4.1.2.2.10: Miniaturas.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

Después de realizar una búsqueda en el disco duro del muchacho, se constata que borró el vídeo.

Usando una herramienta de recuperación de archivos se recupera el vídeo.

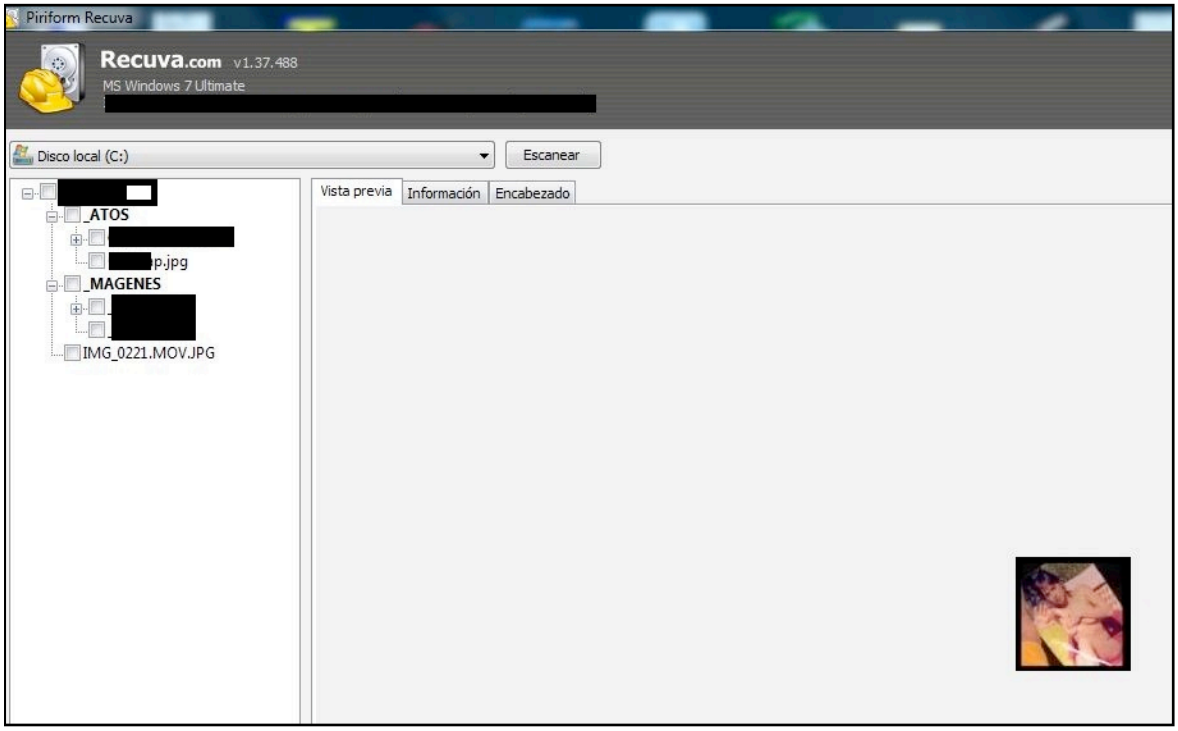


Figura 4.1.2.2.11: Recuperación del vídeo.
Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

Y probando el archivo, es completamente funcional y la prueba necesaria de vinculación del muchacho con el hecho.

Figura 4.1.2.2.12: Vídeo recuperado.

Fuente: ConexionInversa (http://conexioninversa.blogspot.com/2010/04/te-puede-pasar-tiforensics-iphone-parte.html?m=1)

- **Fase reconstrucción del evento.**

Del estudio forense se determina luego de recopilar la evidencia respectiva, que el vídeo procede de un iPhone, teléfono celular móvil, perteneciente a un joven amigo de la ofendida, junto con la fecha y hora de filmación. De estos elementos ciertos y las posteriores versiones de las partes se concluye que: la adolescente Silvia, se encontraba en una fiesta. Decide salir al jardín con dos jóvenes amigos, intercambian números de celulares como cotidiano; días después se propagan rumores respecto a un vídeo en Internet subido al sitio de vídeos Filestube, en el cual aparecía Silvia en forma muy comprometedora. Al enterarse las autoridades del suceso deciden hablar con los padres de familia. El hecho fue denunciado en una comisaría cercana, luego que el informe forense determina el medio a través del cual se cometió el delito un "iPhone" y el propietario del mismo, este dispositivo misteriosamente desaparece, sin permitir incorporar esta prueba al proceso. Ante, este hecho el juez decide que se aplace el juicio para poder analizar los demás equipos informáticos que tenía el muchacho.

En este caso la prueba del delito es el vídeo que fue recuperado del disco duro del computador del muchacho y el mensaje enviado desde su iPhone indicando la dirección de descarga del vídeo.

Al igual en esta etapa se preparará el informe técnico y el ejecutivo.

4.1.2.3. Caso de injurias.

Con fecha 13 de mayo de 2009, el señor Francisco José Enríquez Albornoz presenta en esta ciudad de Quito, ante el Juzgado Décimo de lo Penal de Pichincha una querella por injurias en contra de la Sra. Diana Karina Toscano Acosta, quien le profirió insultos y daños al buen nombre y a su honra mediante el uso del correo electrónico.

La injuria se entiende por comentarios ofensivos contra la honra de la persona. Aquí el medio informático que se utilizó para injuriar es el correo electrónico.

Se puede acceder a todo el detalle procesal de este caso en particular a través del sitio web: http://www.funcionjudicial-pichincha.gob.ec/pichincha/index.php/consulta-de-procesos, se elige la opción de la columna derecha llamada "Consulta de Procesos" bajo el cuadro de "Procesos Corporativos" y se ingresa en el campo Actor/Ofendido los apellidos completos del señor injuriado (Enríquez Albornoz), de los procesos desplegados se elige el de injuria

A continuación una revisión del procedimiento realizado por la firma de peritaje informático "Grupo Profesional Asociados PERITAJES - GPA".

- **Fase de preservación.**

Se realiza una copia de respaldo de todos los correos de la cuenta *sac@florimax.ec* para evitar sobre escrituras y garantizar la veracidad de la evidencia. Igual esta evidencia se graba en un CD en donde se realizará la investigación. Ver Anexo 3.

El equipo a investigarse es una computadora de marca HP, en ese equipo se tiene instalada la aplicación de gestión de correo electrónico *Windows Live Mail*, en donde se accedió a las bandejas de entrada y salida del correo, se sacó respaldos de los correos en formato *eml*[25], genera una carpeta en el escritorio del equipo en donde se guarda el respaldo, cabeceras de correo y una captura de pantalla del correo.

- **Fase de búsqueda de evidencia.**

Primero se establece una línea temporal para así identificar el período que se desea investigar, en este caso sería el 20 de abril del 2009 al 26 de febrero del 2010.

En ese período de tiempo se refleja la inexistencia de los correos injuriosos. Se establece el tiempo de recepción del primer correo injurioso (once meses) y el último (un mes).

Se accede con el gestor de correo electrónico al CD en donde se tiene los respaldos a la bandeja de correo de la cuenta *florimax* .

Figura 4.1.2.3.1: Cabecera de correo.
Fuente: Informe pericial

Con la cabecera de correo electrónico (ver imagen 4.1.2.3.2), se observa el origen del correo (de dónde viene), fecha de recepción y la firma digital.

[25] Formato de correo electrónico que Microsoft usa en Windows Live Mail y Outlook Express.

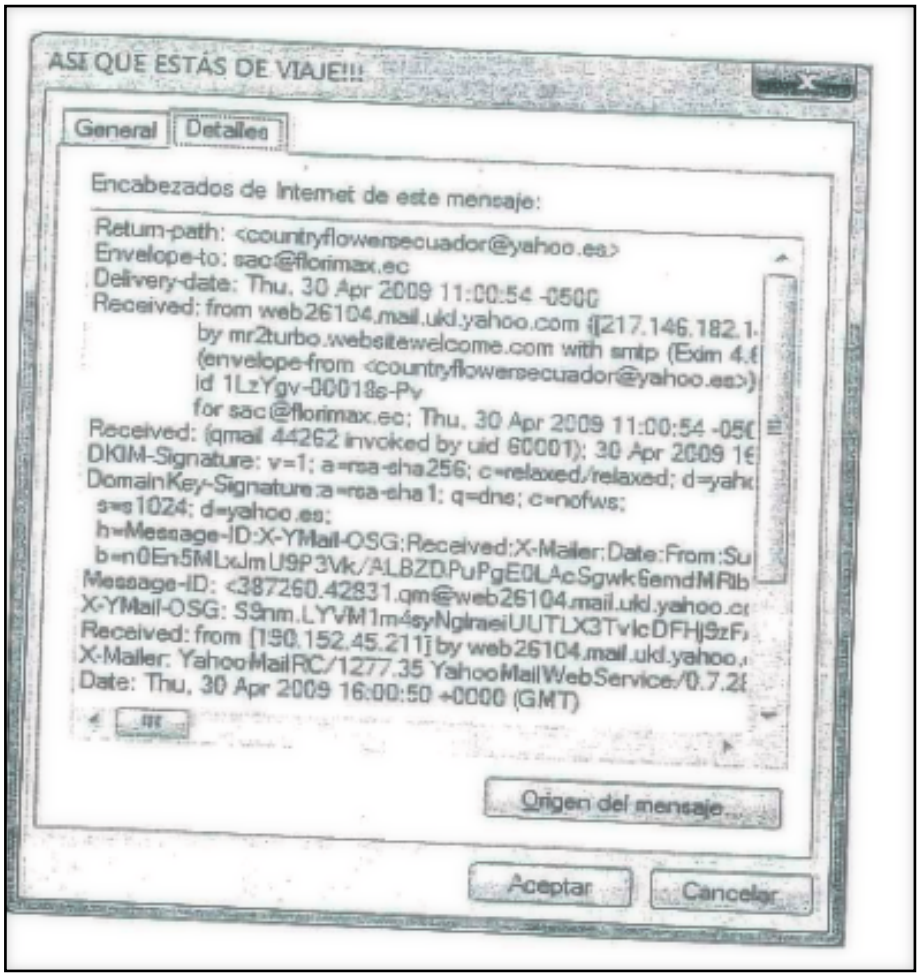


Figura 4.1.2.3.2: Información de cabecera.
Fuente: Informe pericial

- **Fase de reconstrucción del evento.**

Con la verificación de los correos recuperados se puede completar la línea temporal respecto a las fechas en que se realizó el suceso (desde 20 de abril del 2009 al 26 de febrero del 2010).

Las conclusiones y recomendaciones vertidas por parte de la empresa de Peritaje no son contundentes y se ciñen solo a investigar el computador del ofendido, que no es el dispositivo desde donde salieron los mensajes injuriosos. Siendo que una cuenta de correo electrónico público puede ser creada por cualquier persona y utilizada desde cualquier lugar; la evidencia recabada no es contundente pues no estaría determinando la

responsabilidad de la comisión del delito por parte de la señora Toscano. En tal sentido falla el juez a favor de la enjuiciada y desestima la demanda presentada.

Al momento este proceso se encuentra en segunda instancia, por apelación del supuesto agraviado.

4.1.2.4. Caso Raúl Reyes.

Este caso tiene relación con el bombardeo en Angostura, de fecha 1 de marzo de 2008, el campamento se encontraba 1.9 Km en el lado ecuatoriano, en la frontera común. El sitio de consulta es: http://es.scribd.com/doc/18717206/Forensica-Digital-Interpol-y-FARC

Después del ataque a Angostura en donde murió abatido el líder del grupo FARC Raúl Reyes.

Aquí se recuperaron discos duros, CD, computadoras portátiles, dispositivos de almacenamiento.

El grupo de peritos colombianos, llegaron al sitio y comenzaron a realizar respaldos y se llevaron para posteriores análisis, INTERPOL igual realizó un análisis independiente.

Se sacaron fotografías de los dispositivos hallados en el sitio del bombardeo.

El informe de la INTERPOL demuestra sobre escritura de la evidencia e inadecuado proceso investigativo por parte de los peritos colombianos.

En este campamento se hallaron computadoras portátiles, discos duros externos y memorias USB.

- **Fase de preservación.**

El equipo de *CompFor* fue al sitio, acompañado por dos especialistas extranjeros.

Se tomaron fotos de los equipos, discos externos y demás evidencias halladas en el campamento de Angostura.

En Bogotá se sacaron copias de respaldo de toda la información hallada en los equipos informáticos y demás medios de almacenamiento.

Figura 4.1.2.4.1: Equipo decomisado.
Fuente: Forénsica Digital, Interpol
y el caso Raúl Reyes (http://goo.gl/vFjoo)

- **Búsqueda de evidencia.**

En esta fase se comienza a obtener información de las imágenes realizadas y para garantizar la fidelidad. Igual se utilizan bloqueadores de escritura para proteger la evidencia. En el Anexo 4 puede observar el resto de evidencia obtenida.

Tras sacar la imagen del disco se comprueba por medio de una función *hash* la integridad de la misma.

En total se sacan dos imágenes del disco. Se encontraron 609.6 Gb que consta de documentos, imágenes y vídeos:

- Ciento nueve archivos de documentos.
- Cuatrocientos cincuenta y dos hojas de cálculo.
- Siete mil novecientos ochenta y nueves direcciones de correo electrónico.
- Diez mil quinientos treinta y siete archivos de audio y vídeo.
- Veintidós mil cuatrocientos ochenta y uno direcciones de páginas web.
- Treinta y siete mil ochocientos setenta y dos documentos de texto.
- Doscientos diez mil ochocientos ochenta y ocho imágenes.

Usando una herramienta especializada de informática forense cuentan con datos de tiempo llamadas *marcas de tiempo,* estas tienen información de fecha de creación, fechas de modificación y acceso.

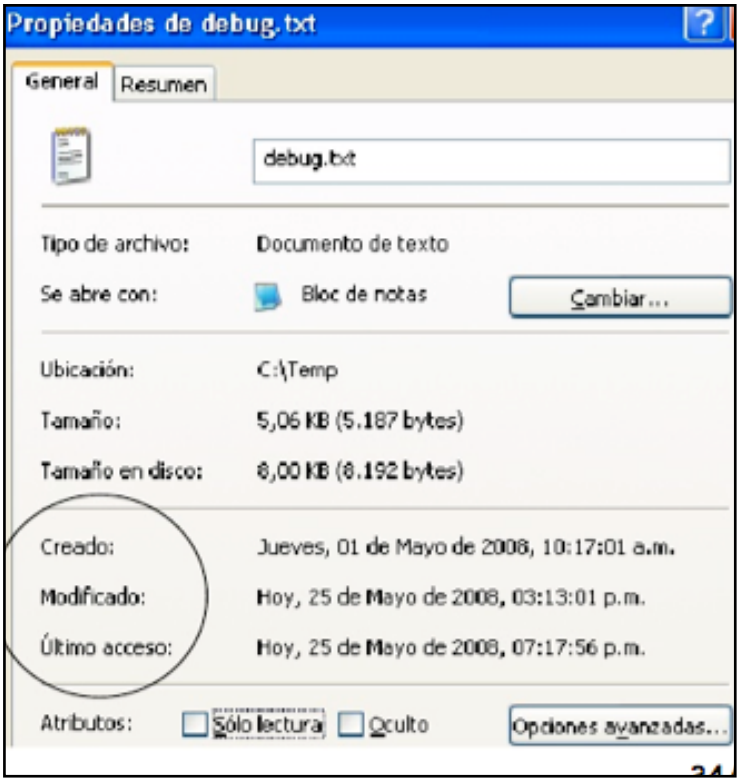


Figura 4.1.2.4.2: Marca de tiempo.
Fuente: Forénsica Digital, Interpol y el caso Raúl Reyes. (http://goo.gl/vFjoo)

Para tener unas marcas de tiempos completamente fiables se debe tener en cuenta la configuración de la zona horaria.

Existen dos formatos de tiempos el UTC (Coordinated Universal Times) basados en relojes atómicos en setenta laboratorios nacionales en diferentes lugares del mundo y éste se usa en la sincronización de los relojes de las computadoras en Internet, en los estándares de la W3C.

El otro es el GMT (Greenwich Mean Time), que se basa en zonas geográficas.

En caso de dispositivos USB la hora y fecha de la modificación de los archivos es tomada del dispositivo al que fue conectado.

- **Fase de reconstrucción del evento.**

Mediante el análisis forense se determinó que los investigadores colombianos no respetaron los principios internacionales para el análisis, ya que ingresaron sin antes haber realizado una copia de seguridad ya que las aperturas directas quedan registradas.

Los sistemas operativos de los tres computadores portátiles decomisados mostraban que los tres computadores habían sido apagados el 3 de marzo de 2008 (a diferentes horas, pero todos ellos antes de las 11:45, hora en que fueron entregados a los investigadores en informática forense de la Policía Judicial colombiana).

Los dos discos duros externos y las tres llaves USB habían sido conectados a un computador entre el 1 y el 3 de marzo de 2008, sin que se hubieran obtenido previamente copias imágenes forenses de su contenido y sin emplearse dispositivos de bloqueo de escritura.

En la investigación de un computador Toshiba Satellite se identificó que:

- Creación de 273 archivos de sistema.

- Apertura de 373 archivos de sistema y de usuario.
- Modificación de 786 archivos de sistema.
- Supresión de 488 archivos de sistema.

En el disco duro se estableció los siguientes sucesos:

- Creación de 1.632 archivos de sistema.
- Apertura de 11.579 archivos de sistema y de usuario.
- Modificación de 532 archivos de sistema.
- Supresión de 948 archivos de sistema.

Éstos se ubican entre el primero de marzo de 2008 y posteriores.

También se estableció que las computadoras y los discos externos tenían marcas de tiempo equivocados, mostraban fechas futuras.

Las pruebas en una USB se estableció que:

- Seiscientos sesenta y ocho archivos cuyas fechas de creación oscilan entre el 7 de marzo de 2009 y el 26 de agosto de 2009.
- Treinta y un archivos cuyas fechas de última modificación varían entre el 14 de junio de 2009 y el 26 de agosto de 2009.
- Estos archivos contienen música, vídeos e imágenes

En el análisis forense se estableció que 48.055 archivos que los indicadores de marca de tiempo han sido abiertos, modificados o borrados por el acceso directo a la evidencia, esto quiere decir que se perdió el valor probatorio ya que la evidencia fue viciada. Esto en las fechas de 1 y 3 de marzo. Las fotos de la evidencia se puede observar en el Anexo 4.

4.1.3. Análisis de encuesta y entrevista.

Con el afán de aclarar la situación informática/social ecuatoriana y la incidencia de los casos en dónde el medio para cometer el delito fue el medio informático, a continuación se presentará la opinión de la abogada Nancy Armendáriz, servidora pública que labora en la Corte Nacional de Justicia y los resultados de una encuesta que se aplicó a toda la secundaria del Colegio Rousseau, ubicado en Carcelén.

En lo referente a la opinión dada por la señora abogada Armendáriz al pliego de preguntas realizadas, se puede concluir que no existe el suficiente conocimiento por parte de los usuarios de las tecnologías informáticas como se conoce en el campo de la administración pública las TICs, más aún afirma que a nivel de nuestro país no tenemos leyes específicas para este tipo de delitos. Se regula algo en la ley de Comercio Electrónico y se hace más importante aún la entrevista cuando ratifica que el Internet mueve dinero, a través de diferentes dinámicas, ya sea compra/venta de productos, pago de servicios o inversiones en línea y que el país no cuenta con ninguna preparación para salvaguardar el flujo monetario y me permito citar la respuesta dada "ya que no tenemos ni la legislación ni la cultura para este tipo de situaciones".

Asombrosamente se revela que no existe dentro de la Fiscalía o la Policía Judicial una estadística sobre los delitos cometidos mediante medios informáticos. (La entrevista detallada se encuentra como Anexo 5 en este documento.)

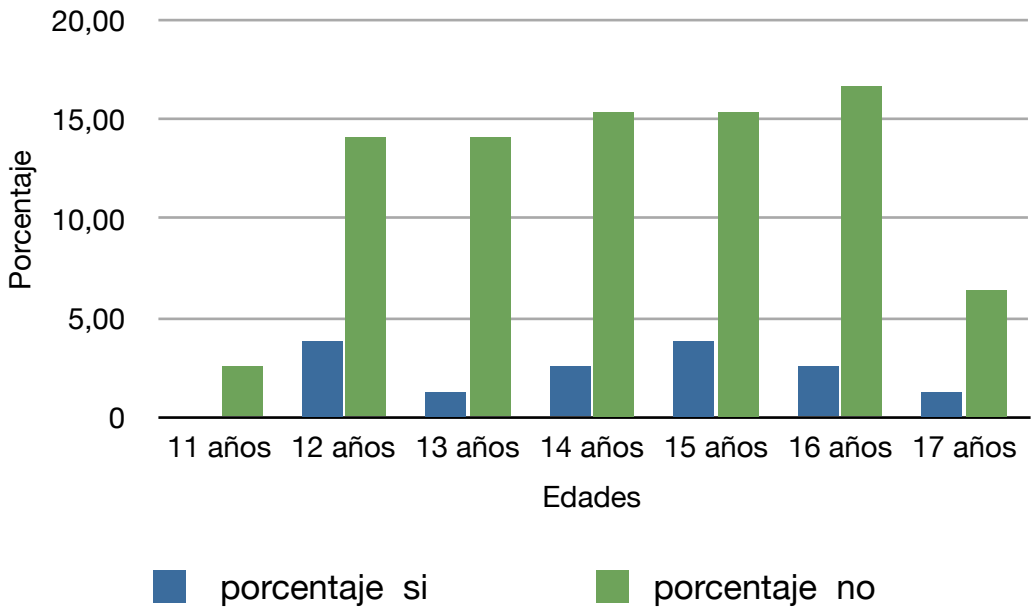
Coincidiendo con el criterio de la entrevistada, que en países desarrollados ya existen leyes que regulan este espectro (ver pregunta 3 de la entrevista) en tanto que en el Ecuador apenas se tiene un leve marco jurídico como es la Ley de Comercio Electrónico, se hace evidente la poca preparación en el tema; primero, al no tener un base legal especializada en esta materia, necesaria conforme a los continuos avances que se producen; y segundo, tal como se menciona en la pregunta 5 de la entrevista. La fiscalía tiene un cuerpo de peritos informáticos; sin embargo, el caso de injurias revisado en este documento corrobora la

respuesta de la pregunta 9 de la entrevista, no se cuentan con la preparación técnica suficiente en este campo.

Muchas empresas guardan datos personales e identificables que se les confía en buena fe como son números de teléfono, correo electrónico, número de tarjeta de crédito, dirección física, entre otra información; en la pregunta 16 de la entrevista se menciona que el Ecuador en su Constitución garantiza al inviolabilidad de la correspondencia virtual y física en el Artículo 66 numeral 21, entonces, se preguntó si el país realiza algo para garantizar este derecho constitucional, la respuesta fue que no; lo que lleva a plantear seriamente una ley que debe abarcar todos los aspectos de la vida digital cotidiana. La Informática Forense entra como una herramienta de auditoría para que se cumplan todas las medidas necesarias de respeto a la intimidad y que no se produzcan fugas de información, venta o mal uso de la misma. Este aspecto se evidencia también, en la encuesta realizada (Anexo 1) en donde se revela que todavía hay jóvenes que publican datos privados en las redes sociales. Incluso algunos tienen contactos desconocidos.

En el Colegio Rousseau, por ejemplo, 11 de un total de 84 alumnos, ponen datos de manera pública y 39 estudiantes entre el referido número de encuestados, se ha puesto en contacto con algún desconocido por redes sociales; demostrando que muchos jóvenes tienen la puerta virtual de sus vidas abierta. Más aún, analizando la encuesta realizada en el ya referido colegio, se desprende que efectivamente este grupo humano es más vulnerable a la comisión de delitos como tales, pues el riesgo no involucra la pérdida económica, sino el honor y buen nombre de la persona, la pornografía y el ciberbullying. Como en el caso internacional de "pornografía" presentado en el capitulo IV "Análisis de casos". El daño que se causa a estos jóvenes se da mediante la divulgación de fotos, vídeos o mensajes difamatorios u ofensivos a través de Internet o mensajes a celular. En el Colegio Rousseau de un grupo de alumnos de 11 a 17 años, once fueron víctimas de burlas por Internet, como lo demuestra la tabulación de la pregunta 9 de la encuesta; con lo cual se demuestra que la realidad del caso de pornografía revisado en este documento de investigación no es ajena a la realidad de nuestro medio.

Pregunta 9: Si ha sido víctima de burlas de sus compañeros en Internet



EDAD	SI	PORCENTAJE SI	NO	PORCENTAJE NO
11 años	0	0,00	2	2,56
12 años	3	3,85	11	14,10
13 años	1	1,28	11	14,10
14 años	2	2,56	12	15,38
15 años	3	3,85	12	15,38
16 años	2	2,56	13	16,67
17 años	1	1,28	5	6,41
TOTAL	12	15,38	66	84,62
UNIVERSO	78			

Figura 4.1.3.1: Tabulación y gráfica de pregunta 9

Autor: Mario de la Cruz D.

4.1.4. Guía general de análisis de casos de peritaje informática.

A lo largo de los casos expuestos se puede demostrar que en cada investigación forense se debe respetar criterios técnicos que a continuación se especifican:

- Identificar datos **esenciales** y **no esenciales**: Es importante identificar la utilidad de cada formato y/o estructura de datos en la investigación. Dentro de esto, se resalta la necesidad de poder diferenciar la relevancia de cada dato para poder dar juicios de valor imparciales y sustentados. Los datos **esenciales** son en los que se confían, el investigador sabe que son archivos o información necesaria para las operaciones de lectura y escritura, este tipo de información debe ser siempre verdadera.De otra manera los datos **no esenciales** son aquellos que están solo por "conveniencia" y no son indispensables para la lectura/escritura de los archivos.
- **Herramientas**: Existen variedad de herramientas que ayudan en cada una de las etapas de la investigación forense, una de ellas se llama The Sleuth Kit (TSK), que es un programa de código abierto y sirve para la investigación en el sistema de archivos.
- **Adquisición de datos:** El procedimiento general de copias de discos es el respaldo byte a byte para tener una copia fiel al original. Los bloques de datos que se copian son de 512 bytes. El comando que se usará para sacar una imagen del disco es el *dd*, este comando consta de parámetros que son: *if* que es la entrada de un archivo que se sacará la imagen, *of* que es la salida del archivo, *bs* es la dimensión de los bloques de muestra y por defecto es de 512 bytes debido al tamaño de los sectores del disco duro.

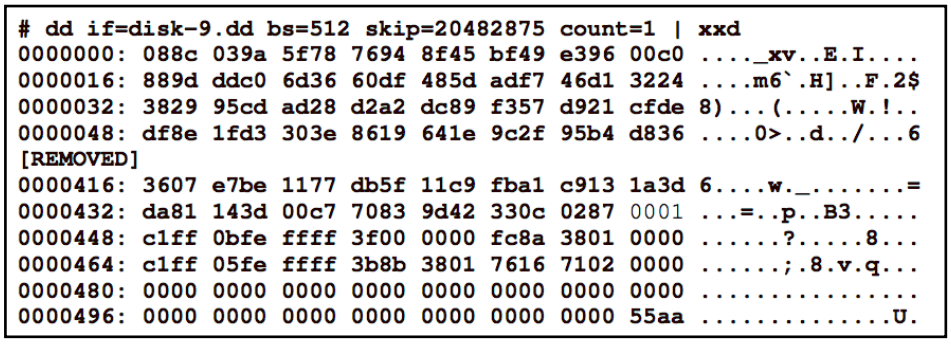


Figura 4.1.4.1: Comando dd
Fuente: File System Forensics

En la imagen 4.1.7.1 se puede ver la ejecución del comando *dd,* en este caso el archivo de entrada es *disk-9.dd* , el tamaño de bloque va a ser de 512 bytes por las razones anteriormente mencionadas, el comando *skip* lo que hace es saltarse el número de bloques designados; esto es útil para sacar imagen de una partición específica o saltarse sectores que tengan datos no esenciales y el comando *count* sirve para indicar el número de bloques que se copian del archivo de entrada al de salida; en este ejemplo no se encuentra el parámetro *of* que indica la salida del resultado de copia que puede ser un archivo o la pantalla (se omite el *of* como en la imagen) y *xxd* no es un comando propio de *dd*, este pertenece a GNU/Linux, lo que hace es transformar a hexadecimal los datos de entrada, en el caso de la imagen recibe la salida del comando *dd* (el carácter "|" concatena la salida del comando *dd* y la convierte en entrada de *xxd*) con el objetivo de tener en pantalla la información del disco para identificar el sector de arranque que comienza en la fila 423 y termina en la 496 en la figura 4.1.7.1.

- **Recuperación de archivos con los metadatos:** Esta técnica permite buscar evidencia en archivos perdidos, como fue en el caso de pornografía infantil. Son como los registros de un huésped de un hotel. Nos demuestra que ha existido un archivo algún momento. Es recuperable la información siempre y cuando exista el metadato y el archivo no haya sido movido o el metadato no haya sido destruido por una sobre escritura. Con el TSK[26] se usa el comando *istat* para ver la información del metadato que muestra si el archivo fue borrado, el nombre, tamaño y los sectores del disco en donde se encuentran los

[26] The Sleuth Kit, es una herramienta forense que se ejecuta en plataforma GNU/Linux

fragmentos del archivo. Con el comando *icat* se puede ver el archivo y recuperarlo desde el sector que nos mostró el metadato.

```
# istat -f fat fat-4.dd 4
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 8689
Name: RESUME-1.RTF

Directory Entry Times:
Written:        Wed Mar 24 06:26:20 2004
Accessed:       Thu Apr 8 00:00:00 2004
Created:        Tue Feb 10 15:49:40 2004

Sectors:
1646 1647 1648 1649 1650 1651 1652 1653
1654 1655 1656 1657 1658 1659 1660 1661
1662 1663
```

Figura 4.1.4.2: Comando istat
Fuente: File System Forensics

El comando *istat* en la imagen 4.1.7.2 se puede observar que tiene un parámetro que siempre se debe poner y es "*-f*" que lo que hace es indicar con que tipo de sistema de archivo está trabajando, en este caso es FAT, después se indica el archivo y la entrada del directorio que se analizan, el archivo es *fat-4.dd* y la entrada de directorio es *4*. El resultado que muestra *istat* son los atributos del archivo, tamaño, nombre, marcas de tiempo y sectores en donde se encuentran los fragmentos del archivo.

```
# icat -f openbsd openbsd.dd 1921 | xxd
0000000: 8107 0000 0c00 0401 2e00 0000 0200 0000 ................
0000016: 0c00 0402 2e2e 0000 8c07 0000 1400 0809 ................
0000032: 6669 6c65 312e 7478 7400 93e7 8d07 0000 file1.txt.......
0000048: 1400 0809 6669 6c65 382e 7478 7400 93e7 ....file8.txt...
0000064: 8e07 0000 2800 0809 6669 6c65 372e 7478 ....(...file7.tx
0000080: 7400 93e7 8f07 0000 1400 0809 6669 6c65 t...........file
0000096: 362e 7478 7400 93e7 9007 0000 1400 0809 6.txt...........
0000112: 6669 6c65 352e 7478 7400 93e7 9107 0000 file5.txt.......
0000128: 2800 0809 6669 6c65 342e 7478 7400 93e7 (...file4.txt...
0000144: 9207 0000 1400 0809 6669 6c65 332e 7478 ........file3.tx
[REMOVED]
```

Figura 4.1.4.3: Comando icat
Fuente: File System Forensics

El comando *icat* que se puede observar en la imagen 4.1.7.3 que tiene igual el parámetro "-*f*" sirve para indicar el sistema de archivos de la imagen del disco, también se puede poner el inodo[27] en donde se encuentran los fragmentos del archivo que se va a recuperar.

- **La búsqueda** no se debe limitar a lo que muestra el directorio de archivos, se debe recordar que en el espacio vacío del disco se puede ocultar información.

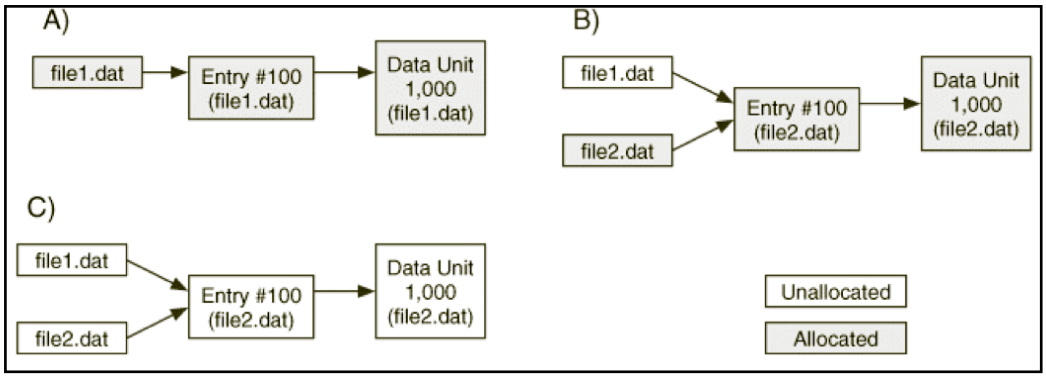


Figura 4.1.4.4: Ejemplo de espacios de disco ocupados y borrados
Fuente: File System Forensics

[27] En informática, un inodo, nodo-i o nodo índice es una estructura de datos propia de los sistemas de archivos tradicionalmente empleados en los sistemas operativos tipo UNIX como es el caso de Linux. Un inodo contiene las características (permisos, fechas, ubicación, pero NO el nombre) de un archivo regular, directorio, o cualquier otro objeto que pueda contener el sistema de ficheros. (Wikipedia)

En la imagen 4.1.4.4 se observa lo que sucede en el disco con el proceso de creación y borrado de documentos y como se va generando, borrando entradas respecto a cada archivo. En el literal (a) se crea el archivo *file1.dat* con una estructura de metadatos #100 y la unidad de datos #1000, después se borra el archivo *file1.dat* y se crea *file2.dat* (b) pero como la estructura de datos #100 se encontraba desocupada, se crean las entradas de datos igual en el número #100 y al final igual *file2.dat* es borrado y se tiene que *file1.dat* y *file2.dat* apuntan a la misma entrada #100, por lo tanto, no se sabe si el contenido de la entrada número 100, a cual de los dos archivos pertenece. Por lo que un análisis en esos sectores daría una pista importante.

- **La técnica de listado de archivos por nombre**, es espacialmente útil si se sabe específicamente que buscar. Algunos Sistemas Operativos no borran el nombre de archivos eliminados. Muchas herramientas lo que hacen es reunir toda la información del archivo e incluso mostrar si este ha sido eliminado. En TSK se hace con el comando *ffind*.

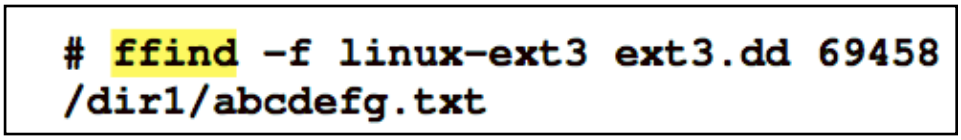


Figura 4.1.4.5: Comando ffind
Fuente: File System Forensics

El comando *ffind* encuentra archivos o directorios por su nombre y se debe especificar el tipo de sistema de archivos que se va a buscar con la opción de "*-f*" e indicar el inodo en donde se encuentra el archivo o directorio a ubicar.

- **Las marcas de tiempo** ayudan al investigador a ubicar los hechos de cada archivo.

```
Wed Aug 11 2004 19:31:58      34528 .a. /system32/ntio804.sys
                              35392 .a. /system32/ntio412.sys
[REMOVED]
Wed Aug 11 2004 19:33:27       2048 mac /bootstat.dat
                               1024 mac /system32/config/default.LOG
                               1024 mac /system32/config/software.LOG
Wed Aug 11 2004 19:33:28     262144 ma. /system32/config/SECURITY
                             262144 ma. /system32/config/default
```

Figura 4.1.4.6: MAC time
Fuente: File System Forensics

En la imagen superior se puede observar el resultado de ejecutar el comando *mactime* que muestra el día, fecha y hora en la primera columna, en la segunda el tamaño del archivo/ directorio, en la tercera columna aparecen los indicadores de que si fue modificado (m) el contenido, accedió (a) al contenido y si cambió (c) el metadato.

Con lo expuesto, se entiende que cada caso tiene sus particularidades, se debe considerar aspectos como los anteriormente mencionados, que ayudan a tener una investigación más correcta y presentan evidencia de utilidad; al final, ese es el objetivo de toda ciencia forense, independiente del campo al que pertenezca.

4.1.5. Clasificación de los delitos.

En este apartado se va a clasificar los delitos ya explicados respecto a los contemplados por las Naciones Unidas y las leyes ecuatorianas.

Delito	Clasificación de las N.U	Código Penal	LCE
	Falsificación informática como instrumento.	Falsificación Capítulo: Tercero Artículo: 337	Título: Quinto Capítulo: primero. Artículo: 60

Delito	Clasificación de las N.U	Código Penal	LCE
Caso “Recargas Más Móvil”		Estafa. Título: Décimo Capítulo: Quinto. Artículo: 560	Artículo: 58 Párrafo: quinto
		Hurto Título: décimo Capítulo: primero. Artículo: 548.	
Caso “pornografía infantil”	N/A	Atentado contra el pudor. Título: octavo Capítulo: Segundo Artículo: 506	N/A
Caso “Injurias por correo electrónico”	N/A	Delitos contra la honra. Título séptimo. Capítulo único Artículo: 491	Titulo primero. Capítulo primero. Artículo: 2.
Caso “Raul Reyes”	N/A	N/A	N/A

Tabla 4.1.5.1: Delitos según clasificación internacional y nacional

Fuente: Mario de la Cruz D.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Del presente trabajo de investigación se evidencia que en nuestro quehacer social y cotidiano, el uso de medios informáticos y electrónicos toma cada vez mayor fuerza, incluso en un contexto global se tiende a minimizar la utilización del papel o medios físicos de almacenamiento de datos. Tomando en cuenta estos aspectos, se hace necesario crear la experticia dentro del campo informático, como se revela con el caso de pornografía infantil en la cual se usa el internet para atentar contra el honor e integridad de una persona, pero esto no sucede solamente en el campo social, sino que llega incluso al manejo mismo de los datos almacenados en instituciones, entidades, empresas, etc. Cuyos datos pueden ser alterados o vulnerados por personas inescrupulosas. Esto amerita que el peritaje informático se considere como una ciencia que permita el resolver delitos y realizar auditorías de empresas de acuerdo con las leyes vigentes que garanticen la integridad de la información.

- En este trabajo se revela que cada cuerpo legal de la legislación ecuatoriana contempla lo referente a acciones o delitos a través de medios informáticos y el valor jurídico de la evidencia hallada en cualquier caso en donde haya participado la informática forense. Haciendo posible la relación entre penas, compensaciones de delitos/pseudo delitos y los actos cometidos por medio de herramientas/medios informáticos. Así se compensa la falta de unas normativas que conste en el Código Penal relacionado a los delitos informáticos y todo su campo de acción.

- El avance en materia de peritaje informático en el Ecuador es escaso, si bien ya se tiene una Ley que regula de cierta manera los delitos realizados por medios informáticos y la Fiscalía tiene una unidad especializada; aún falta implementar de manera urgente

reformas al Código Penal, que regulen el uso cotidiano de los medios informáticos porque la mayoría de la información hoy se encuentra hospedada en el Internet, sea ésta de carácter personal, empresarial o estatal; por lo que la investigación e inversión continua y pronta, debe ser tomada como política de Estado.

- El Estado debe tener o crear una estructura e institución orientada a regular todo lo que es el mundo digital e informático; en América Latina, Argentina va pasos más adelante, teniendo ya instituciones y leyes más estructuradas respecto al tema, donde el marco legal cubren cada aspecto de este entorno llegando al gobierno electrónico e instituciones estatales en donde se regula el espectro de comercio Electrónico y los mensajes de Datos. También es importante rescatar que en países desarrollados como España y Estados Unidos de Norte América tal como se dice en la entrevista (Anexo 5) se han realizado avances importantes. Básicamente en políticas de manejo de herramientas digitales tales como: defensa en caso de guerra cibernética y en España la aplicación técnica de las herramientas tecnológicas en el peritaje informático llegando a determinar el propietario del celular que grabó el vídeo del caso de pornografía incluido el contemplar nuevas figuras legales como el derecho al olvido, instituciones y leyes establecidas para dar soporte legal al proceso de peritaje como una herramienta de soporte legal, cuerpos legales completamente detallados para cada caso que se vaya presentando en España hay el decreto Real 322/2008 sobre el régimen de entidades de dinero electrónico, en EEUU hay la ley de California Anti Spam, la ley de protección de privacidad de menores y la Patriot Act 2001 que tiene que ver sobre evidencia y crímenes electrónicos.

- El Código Penal es el marco legal que regula cualquier actividad o actitud atípica y que vaya en perjuicio del Estado Ecuatoriano, pero no tiene ninguna mención o reforma hacia estos tipos de delitos, por lo que no se puede considerar a los delitos a través de medios informáticos como tales.

- El respetar los estándares internacionales y las cadenas de custodia para realizar un análisis forense permitirá presentar informes con una alta credibilidad para cualquier caso sea éste nacional o internacional y así situar al Ecuador dentro de los países que

utilizan el peritaje informático en forma certera. Así que el procedimiento aplicado tanto en el caso Reyes como en el de pornografía infantil son análogos pues obedecen a lineamientos internacionales comunes para peritaje informático. Se puede apreciar esto del uso por ejemplo de código de validación HASH utilizado en los dos procesos como medio de comprobación de la integridad de la información obtenida, respaldar la información, etiquetar la información, escritura de los informes periciales.

- Ecuador es un país en donde existe desconocimiento en temas con respecto a la seguridad informática; las encuestas reflejan que si bien los jóvenes entre 11 y 17 años, tienen conocimientos básicos del mismo, respondieron afirmativamente a la pregunta, que han sido víctimas de bullying en Internet, este porcentaje corresponde al 15,38%. (ver Anexo 2, pregunta 9). Existen múltiples casos relacionados a derecho informático e informática forense y una reforma al Código Penal se hace necesario.

5.2. RECOMENDACIONES

- De la tabulación de las encuestas realizadas que constan como anexo en este trabajo de investigación, así como lo enunciado y revisado dentro del Capítulo I; y de los casos revisados, se desprende que el instrumento legal que es el Código Penal que debe contemplar este nuevo entorno de acción delictiva, no solamente acoger lo dispuesto dentro de la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, sino además considerar ser reformado en muchos de sus Artículos. Como por ejemplo: Artículo 202 habla sobre el robo de correo, el Artículo 262 habla de la destrucción o supresión fraudulenta de información y documentos, el Artículo 353 sobre la falsificación y el uso de estos medios falsificados, entre otros; quizás sea indispensable incluso dedicar un capítulo completo de este cuerpo legal a los delitos cometidos a través de medios electrónicos y/o digitales para que se pueda sancionar correctamente los delitos por los medios referidos.

- La Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos debe ampliarse de manera tal que cubra todos los aspectos necesarios que van apareciendo en el entorno social, porque el mundo digital sigue avanzando.

- Casos presentados como el de pornografía infantil se pueden evitar educando desde la escuela y el colegio en el uso adecuado de la tecnología; el Estado debe invertir en esfuerzo para tener un marco legal adecuado, formar un equipo de peritos capaces de responder y vigilar exhaustivamente el ciberespacio y así poder enfrentar a los delitos realizados por medios informáticos.

- Se debe a la realizar ampliaciones al Código Penal, para poder regular delitos desde pornografía, violaciones a la intimidad virtual, al incumplimiento de alguna transacción en línea. El de pornografía infantil citado en este trabajo permite mirar la realidad social actual y la necesidad de un equipo de investigación competente y adecuadamente entrenado. Tal es el caso del grupo de peritos informáticos españoles que gracias a su experticia pudieron dar con el responsable del delito, aunque el iPhone se haya perdido y el vídeo haya sido borrado. Todo debidamente sustentado, técnicamente probada la culpabilidad, verificado el equipo que se utilizó, etc. Todo esto, pudo derivar en la sanción al verdadero culpable, pues existe en España el marco legal adecuado. A diferencia del caso de injurias local el peritaje como se puede observar en el Anexo 3, es básico y solo se demuestra que evidentemente recibió el correo electrónico; pero no revela la culpabilidad.

- El Estado Ecuatoriano debe proteger la intimidad y el correcto uso de la información. Como se realiza en la Unión Europea, ahí se reglamenta y protege la intimidad digital de los europeos de manera celosa, sin que se permita el uso inadecuado o peor aún la venta de la misma.

- El Estado debería implementar la tecnología de punta para proteger, rastrear y prevenir posibles ataques de fuerzas hostiles hacía la información y servicios vitales del Estado.

- Capacitar y formar a técnicos calificados en administración de sistemas informáticos, protección y rastreo de la información gubernamental y evitar posible divulgación y perdida de confidencialidad de datos reservados.

6. ANEXOS

ANEXO 1: ENCUESTA

Fecha de encuesta: 3 de noviembre de 2011

Alumnos encuestados 100

Colegio: Rousseau

Sector: Carcelén-Quito

Soy estudiante egresado de la Universidad Internacional SEK.

Estoy realizando mi tesis con el tema "Análisis jurídico-técnico de la informática forense en el Ecuador y estudio del procedimiento forense aplicado en casos reales"
Quisiera pedirle que conteste esta encuesta de forma totalmente anónima.
Gracias.

Edad:

Marque la respuesta en un círculo.

1. Cuando usted utiliza el Internet mantiene la sesión iniciada (activa)

Si **No**

2. Usted usa contraseña común (ejemplo: 1234).

Si **No**

3. Usted usa la misma contraseña para otros servicios (correos electrónicos, redes sociales, etc.)

Si **No**

4. Con que frecuencia cambia la contraseña

Cada mes **entre 3 - 6 meses** **cada año** **otro**[28] **nunca**

5. En redes sociales (Facebook, Twitter) usted pone datos personales (teléfono, dirección de domicilio/trabajo, etc.) de manera pública.

Si **No**

6. De sus contactos de redes sociales (Facebook, Twitter) a cuantos conoce.

Todos **más de la mitad** **menos de la mitad**

7. Alguna vez alguien desconocido se ha contactado con usted por Facebook o Twitter.

Si **No**

8. Si la respuesta a la pregunta anterior fue afirmativa, usted informó a:

Papá **mamá** **profesores** **ninguno**

9. Usted ha sido alguna vez víctima de burlas de sus compañeros en Facebook u otra red social a través de fotos, comentarios o cualquier otro medio ofensivo.

Si **No**

10. Si la respuesta es afirmativa, usted informó a:

Papá **mamá** **profesor** **ninguno**

11. Quien considera que debe proteger su intimidad en Internet o cualquier otro medio digital.

Estado **Padres** **usted**

Revise si puso su edad al inicio y entregue de vuelta esta encuesta.

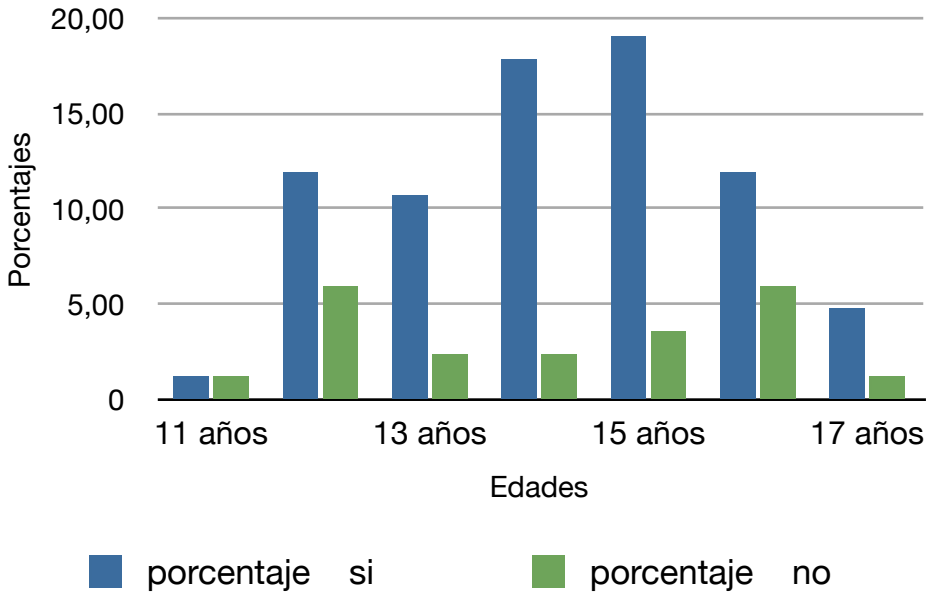
Gracias

---

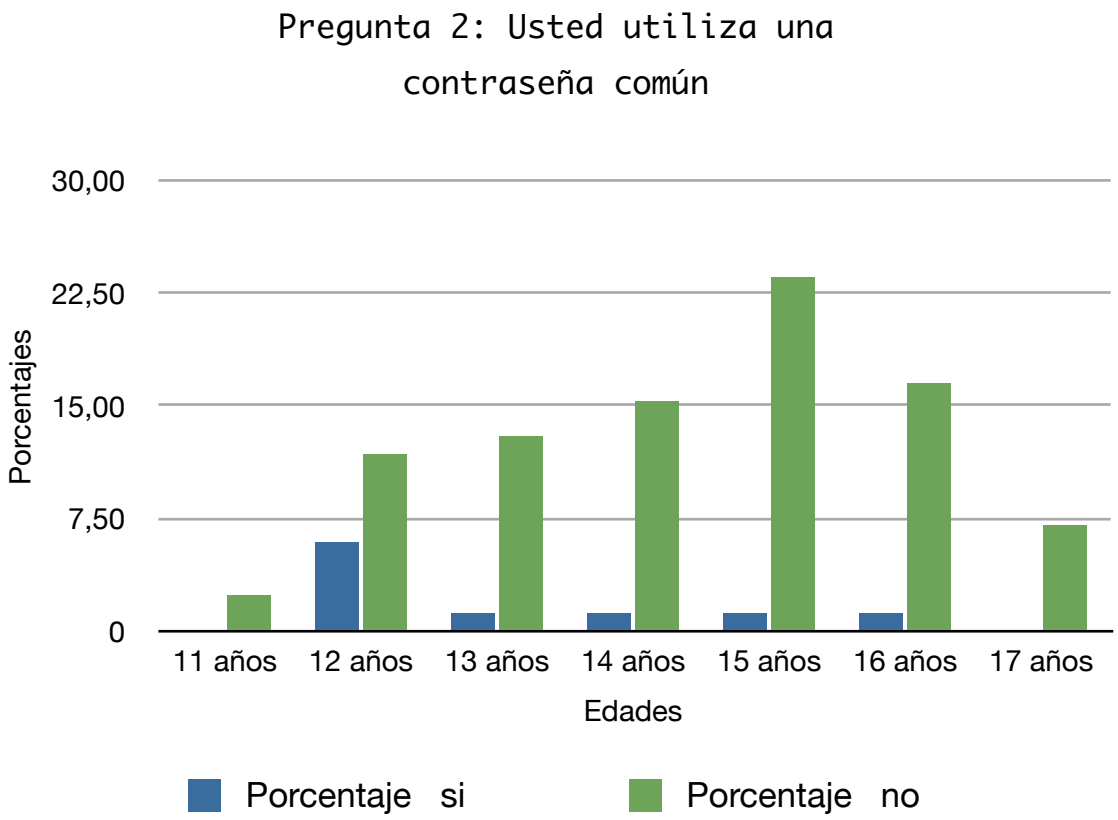
[28] A lado escriba la frecuencia

ANEXO 2: TABULACIÓN DE ENCUESTA.

Pregunta 1: ¿Cuándo usa internet mantiene la sesión iniciada? (activa)

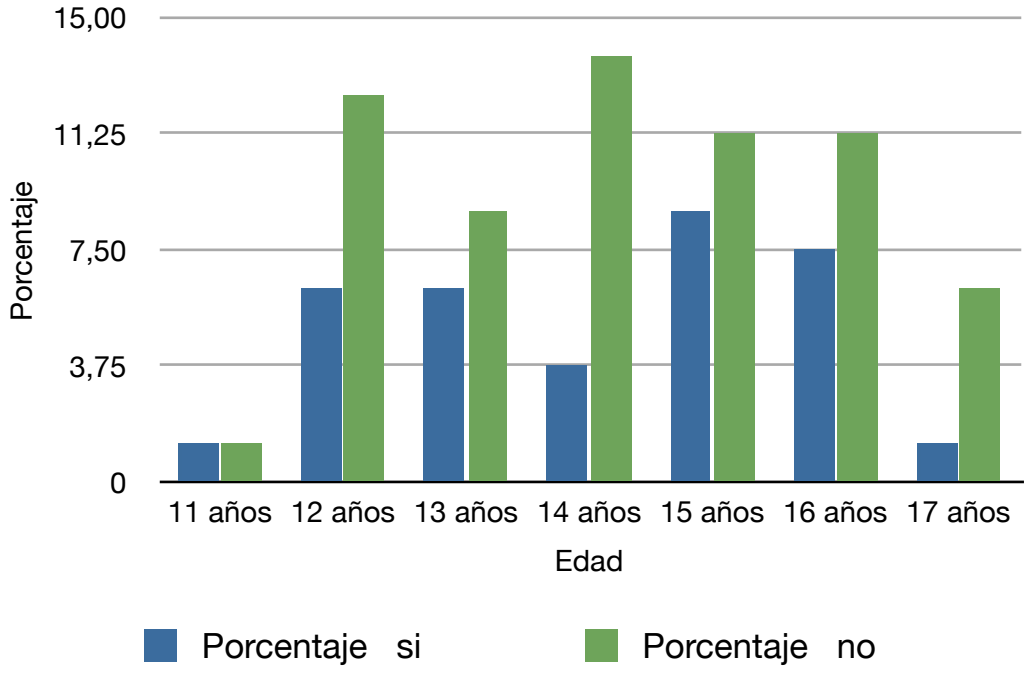


EDAD	SI	PORCENTAJE SI	NO	PORCENTAJE NO
11 años	1	1,19	1	1,19
12 años	10	11,90	5	5,95
13 años	9	10,71	2	2,38
14 años	15	17,86	2	2,38
15 años	16	19,05	3	3,57
16 años	10	11,90	5	5,95
17 años	4	4,76	1	1,19
TOTAL	65	77,38	19	22,62
UNIVERSO	84			

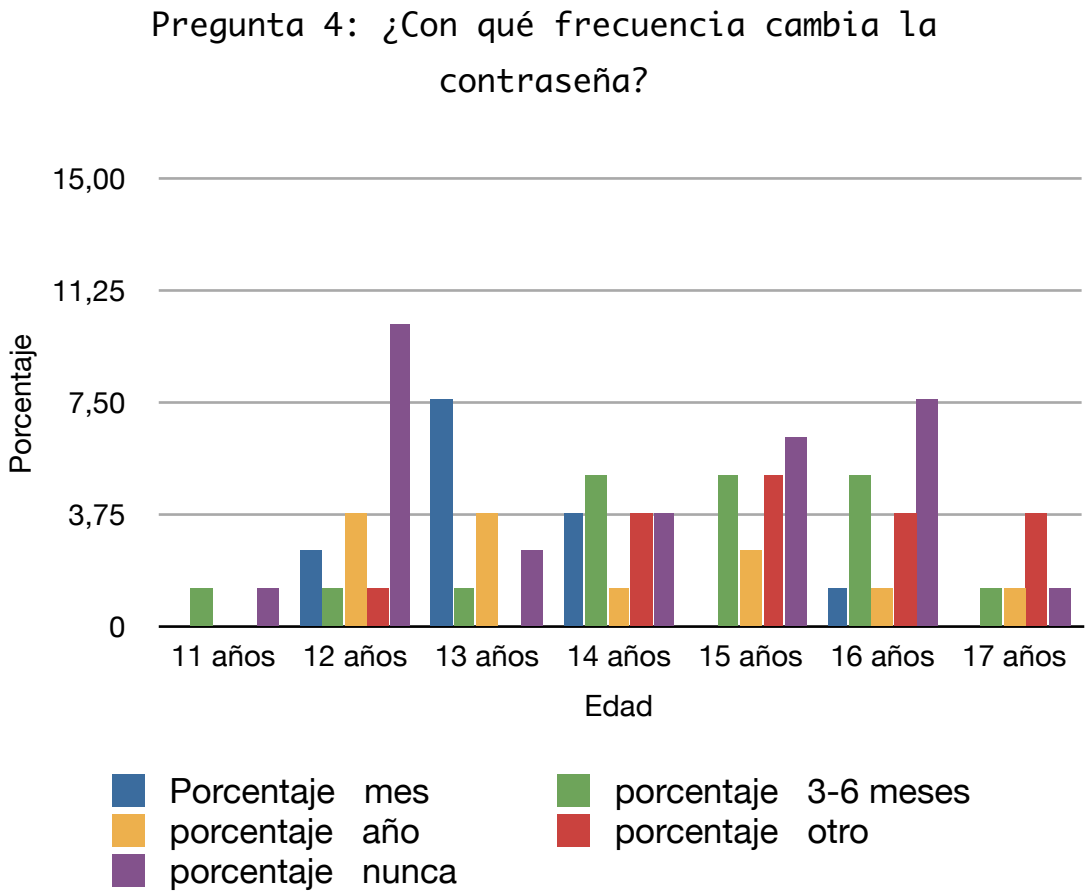


EDAD	SI	PORCENTAJE SI	NO	PORCENTAJE NO
11 años	0	0,00	2	2,35
12 años	5	5,88	10	11,76
13 años	1	1,18	11	12,94
14 años	1	1,18	13	15,29
15 años	1	1,18	20	23,53
16 años	1	1,18	14	16,47
17 años	0	0,00	6	7,06
TOTAL	9	10,59	76	89,41
UNIVERSO	85			

Pregunta 3: Usted utiliza la misma contraseña para otros servicios

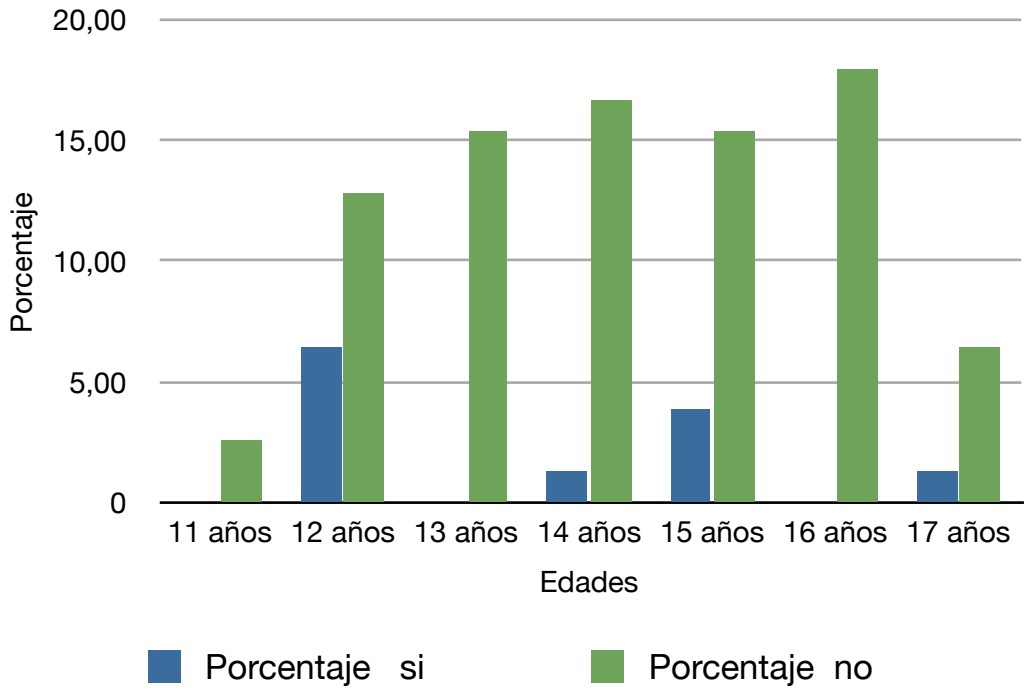


Edades	Si	Porcentaje si	No	Porcentaje no
11 años	1	1,25	1	1,25
12 años	5	6,25	10	12,5
13 años	5	6,25	7	8,75
14 años	3	3,75	11	13,75
15 años	7	8,75	9	11,25
16 años	6	7,5	9	11,25
17 años	1	1,25	5	6,25
Total	28	35	52	65
Universo	80			



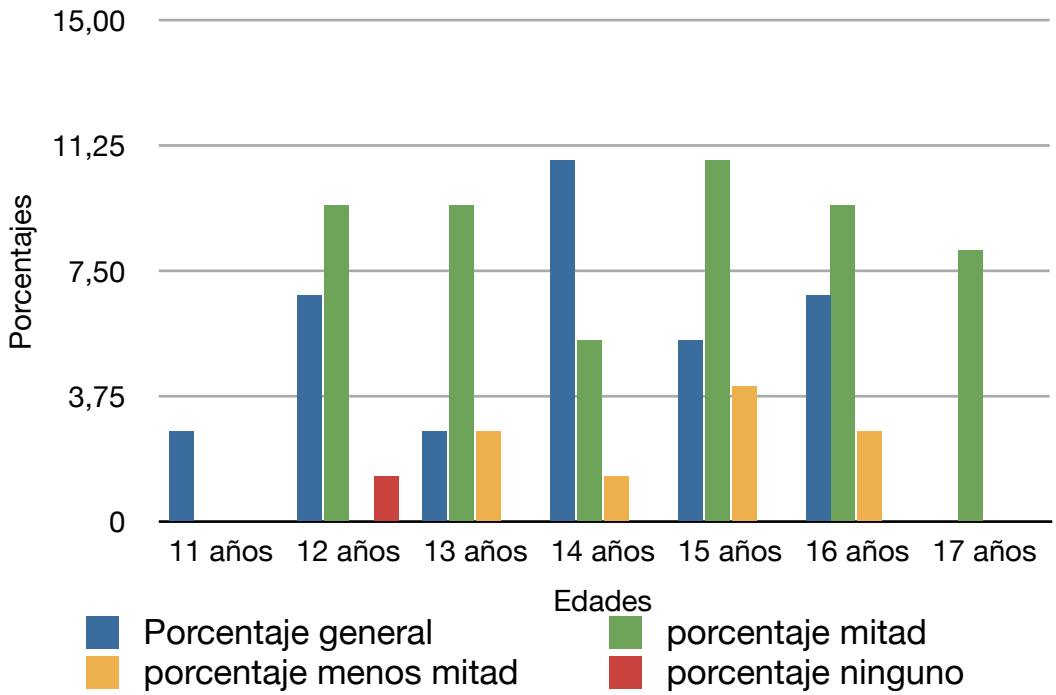
Edades	Cada mes	%mes	Entre 3-6 meses	% 3-6 meses	Cada año	%año	Otro	%otro	Nunca	% nunca
11 años	0	0,00	1	1,27	0	0,00	0	0,00	1	1,27
12 años	2	2,53	1	1,27	3	3,80	1	1,27	8	10,13
13 años	6	7,59	1	1,27	3	3,80	0	0,00	2	2,53
14 años	3	3,80	4	5,06	1	1,27	3	3,80	3	3,80
15 años	0	0,00	4	5,06	2	2,53	4	5,06	5	6,33
16 años	1	1,27	4	5,06	1	1,27	3	3,80	6	7,59
17 años	0	0,00	1	1,27	1	1,27	3	3,80	1	1,27
Total	12	15,19	16	20,25	11	13,92	14	17,72	26	32,91
Universo	79									

Pregunta 5: Pone datos personales en redes sociales de manera pública



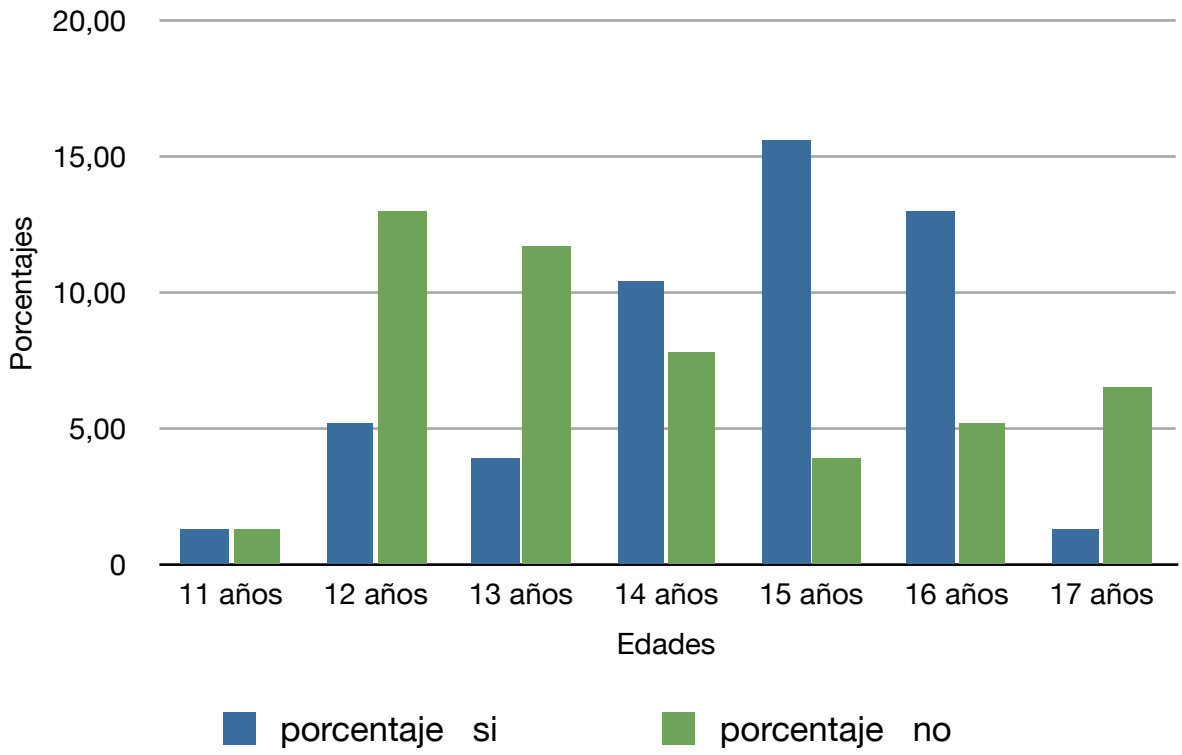
Edades	Si	Porcentaje si	No	Porcentaje no
11 años	0	0,00	2	2,56
12 años	5	6,41	10	12,82
13 años	0	0,00	12	15,38
14 años	1	1,28	13	16,67
15 años	3	3,85	12	15,38
16 años	0	0,00	14	17,95
17 años	1	1,28	5	6,41
Total	10	12,82	68	87,18
Universo	78			

Pregunta 6: ¿Cuántos contactos conoce de sus redes sociales?



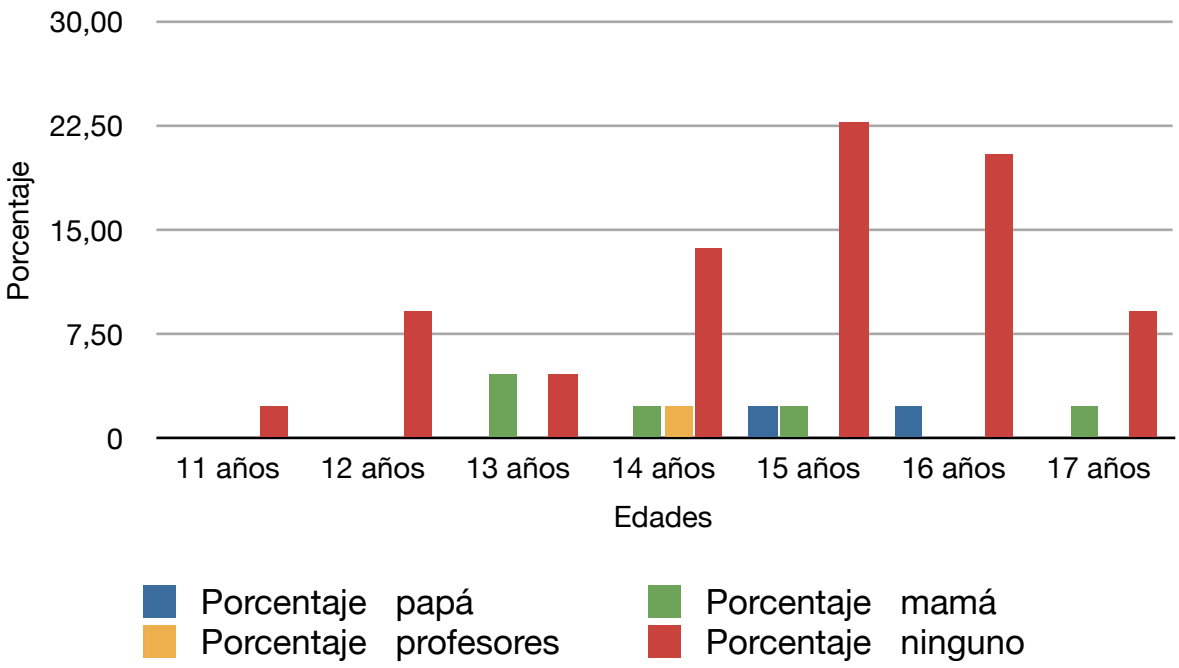
Edades	Todos	% general	Más de la mitad	%mitad	Menos de la mitad	%menos mitad	Ninguno	% ninguno
11 años	2	2,70	0	0,00	0	0,00	0	0,00
12 años	5	6,76	7	9,46	0	0,00	1	1,35
13 años	2	2,70	7	9,46	2	2,70	0	0,00
14 años	8	10,81	4	5,41	1	1,35	0	0,00
15 años	4	5,41	8	10,81	3	4,05	0	0,00
16 años	5	6,76	7	9,46	2	2,70	0	0,00
17 años	0	0,00	6	8,11	0	0,00	0	0,00
Total	26	35,14	39	52,70	8	10,81	1	1,35
Universo	74							

Pregunta 7: Alguna vez alguien desconocido se ha contactado con usted por Facebook o Twitter



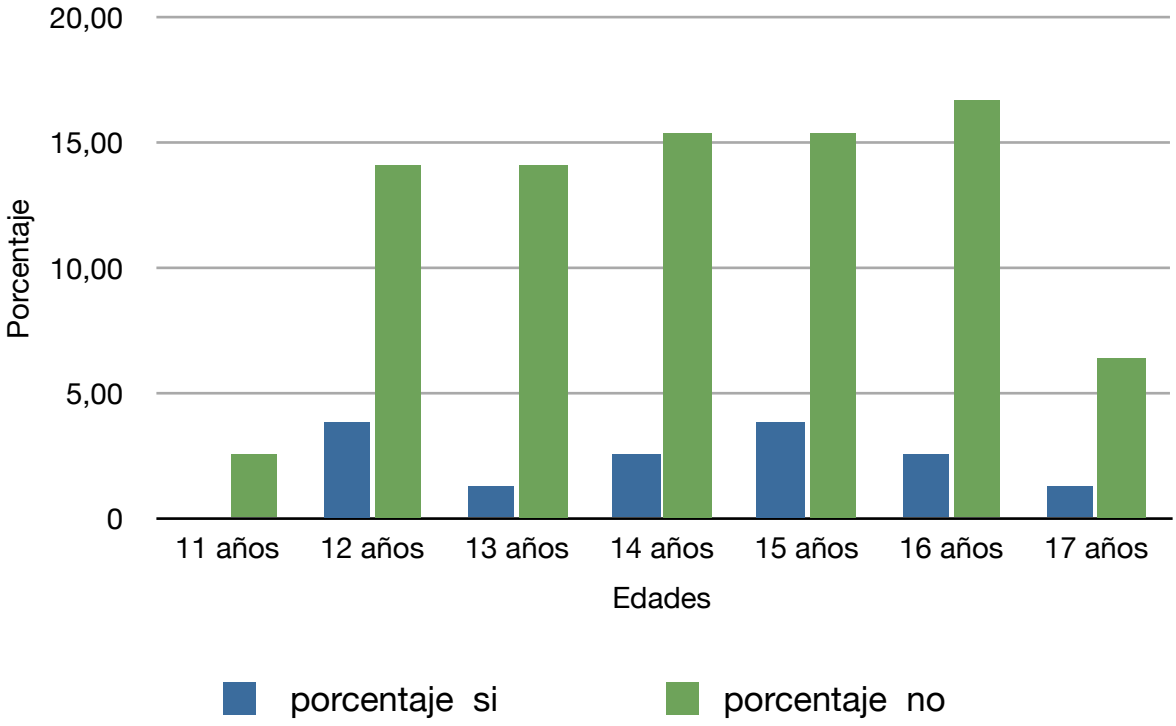
Edad	Si	Porcentaje si	no	Porcentaje no
11 años	1	1,30	1	1,30
12 años	4	5,19	10	12,99
13 años	3	3,90	9	11,69
14 años	8	10,39	6	7,79
15 años	12	15,58	3	3,90
16 años	10	12,99	4	5,19
17 años	1	1,30	5	6,49
Total	39	50,65	38	49,35
Universo	77			

Pregunta 8: Si la respuesta anterior fue afirmativa, usted informo a:



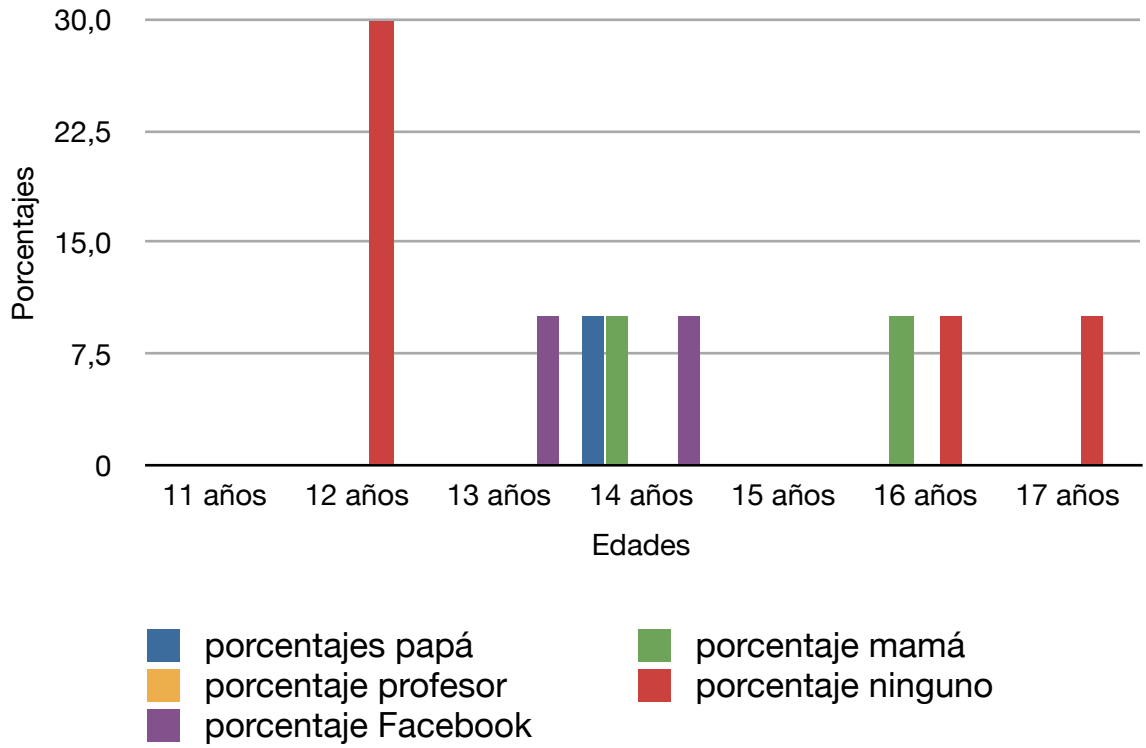
Edad	Papá	%papá	Mamá	%mamá	Profesores	% Profesores	Ninguno	%ninguno
11 años	0	0,00	0	0,00	0	0,00	1	2,27
12 años	0	0,00	0	0,00	0	0,00	4	9,09
13 años	0	0,00	2	4,55	0	0,00	2	4,55
14 años	0	0,00	1	2,27	1	2,27	6	13,64
15 años	1	2,27	1	2,27	0	0,00	10	22,73
16 años	1	2,27	0	0,00	0	0,00	9	20,45
17 años	0	0,00	1	2,27	0	0,00	4	9,09
Total	2	4,55	5	11,36	1	2,27	36	81,82
Universo	44							

Pregunta 9: Si ha sido víctima de burlas de sus compañeros en Internet



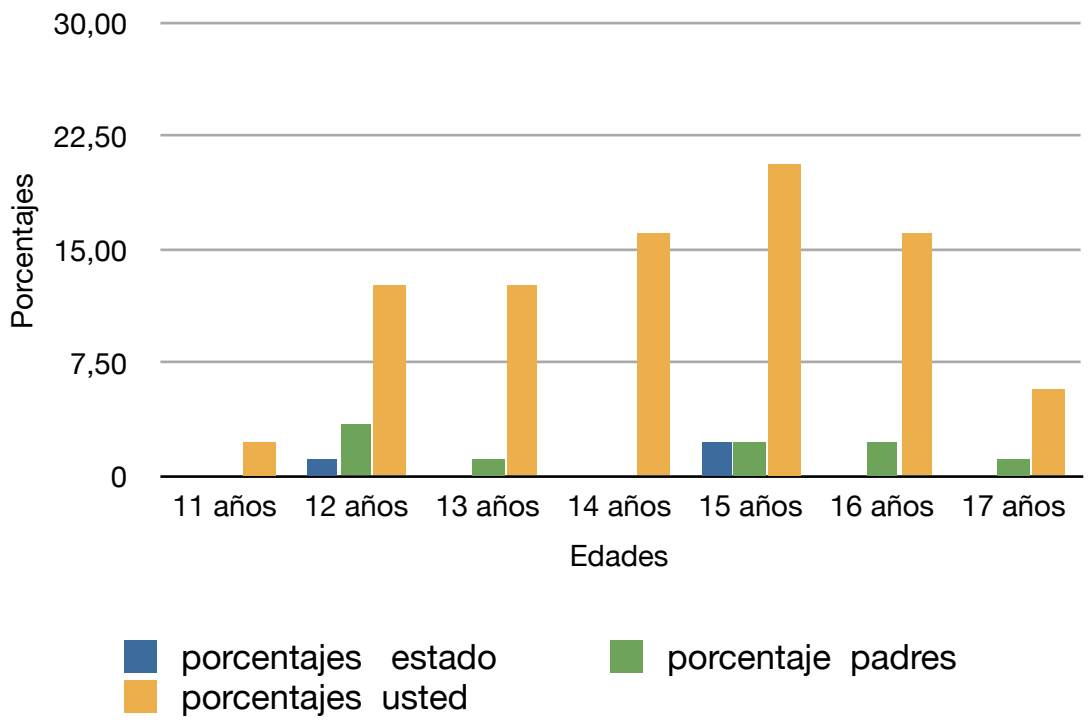
Edad	si	Porcentaje si	no	Porcentaje no
11 años	0	0,00	2	2,56
12 años	3	3,85	11	14,10
13 años	1	1,28	11	14,10
14 años	2	2,56	12	15,38
15 años	3	3,85	12	15,38
16 años	2	2,56	13	16,67
17 años	1	1,28	5	6,41
Total	12	15,38	66	84,62
Universo	78			

Pregunta 10: Si la respuesta anterior fue afirmativa, usted informó a:



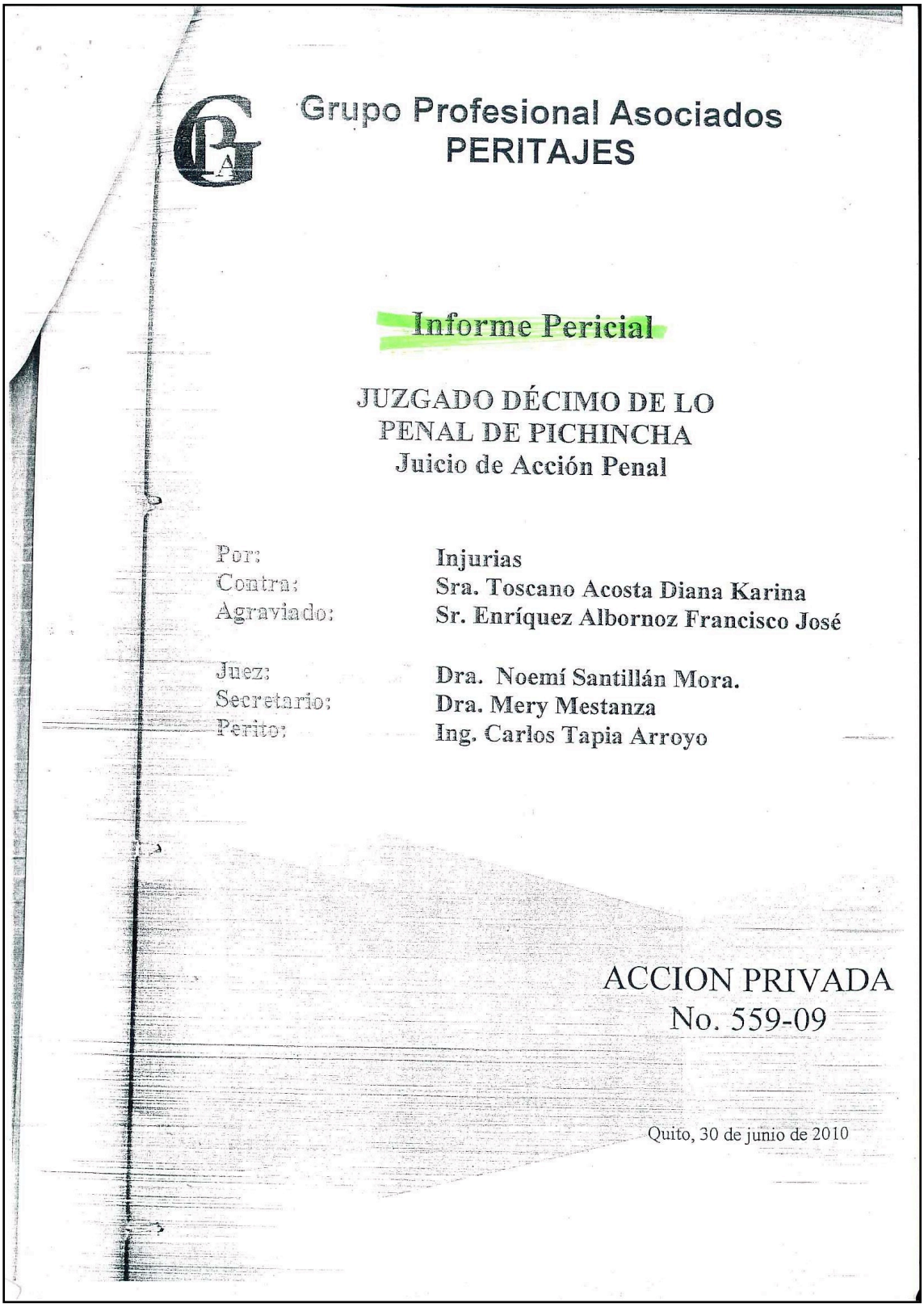
Edad	Papá	%papá	Mamá	%mamá	Profesor	% profesor	Ninguno	% ninguno	Facebook y sus autoridades	% Facebook
11 años	0	0	0	0	0	0	0	0	0	0
12 años	0	0	0	0	0	0	3	30	0	0
13 años	0	0	0	0	0	0	0	0	1	10
14 años	1	10	1	10	0	0	0	0	1	10
15 años	0	0	0	0	0	0	0	0	0	0
16 años	0	0	1	10	0	0	1	10	0	0
17 años	0	0	0	0	0	0	1	10	0	0
Total	1	10	2	20	0	0	5	50	2	20
Universo	10									

Pregunta 11: ¿Quién cree que debe proteger su privacidad?



Edad	Estado	Porcentaje Estado	Padres	Porcentajes padres	Usted	Porcentajes usted
11 años	0	0,00	0	0,00	2	2,30
12 años	1	1,15	3	3,45	11	12,64
13 años	0	0,00	1	1,15	11	12,64
14 años	0	0,00	0	0,00	14	16,09
15 años	2	2,30	2	2,30	18	20,69
16 años	0	0,00	2	2,30	14	16,09
17 años	0	0,00	1	1,15	5	5,75
Total	3	3,45	9	10,34	75	86,21
Universo	87					

ANEXO 3: CASO DE INJURIA.



Grupo Profesional Asociados
PERITAJES

Informe Pericial

JUZGADO DÉCIMO DE LO
PENAL DE PICHINCHA
Juicio de Acción Penal

Por:	Injurias
Contra:	Sra. Toscano Acosta Diana Karina
Agraviado:	Sr. Enríquez Albornoz Francisco José
Juez:	Dra. Noemí Santillán Mora.
Secretario:	Dra. Mery Mestanza
Perito:	Ing. Carlos Tapia Arroyo

ACCION PRIVADA
No. 559-09

Quito, 30 de junio de 2010

Tabla de Contenido:

Juicio Penal No. 559-2009
Av. 10 de Agosto N 13-134 y Checa
Telf. 2070623 / 099810158
@mail: carlostapia.perito@hotmail.com

4.2. Evidencia Digital, acceso a la información objeto de la pericia y toma muestra:

- Con el propósito de dar cumplimiento a lo ordenado por su Autoridad; el viernes de marzo de 2010 a partir de las 16h00, se procedió a realizar la inspección técni pericial solicitada por su Autoridad, en el domicilio del señor Francisco Jos Enríquez Albornoz, ubicado en la calle República del Salvador N34-127 y Suiz Edificio Murano Plaza, Suite 42 Con la presencia de su Abogado defensor doct Héctor Caspi y el señor perito; Ing. Carlos Tapia A.

- Para el efecto se contó con la completa colaboración por parte del denunciante, que permitió cumplir con el relevamiento, entrega de la información, constataciones y explicaciones solicitadas en el presente Análisis Pericial.

- La Evidencia Digital "es el conjunto de pruebas y constancias que quedan luego d cometimiento de un delito usando medios informático"; por lo que es necesari garantizar la integridad y la conservación de los mensajes de datos que se analiza en el presente análisis pericial. "se considera que un mensaje de datos permanec íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio d forma, propio del proceso de comunicación, archivo o presentación"; por lo que par garantizar la conservación de los mensajes de datos es necesario:

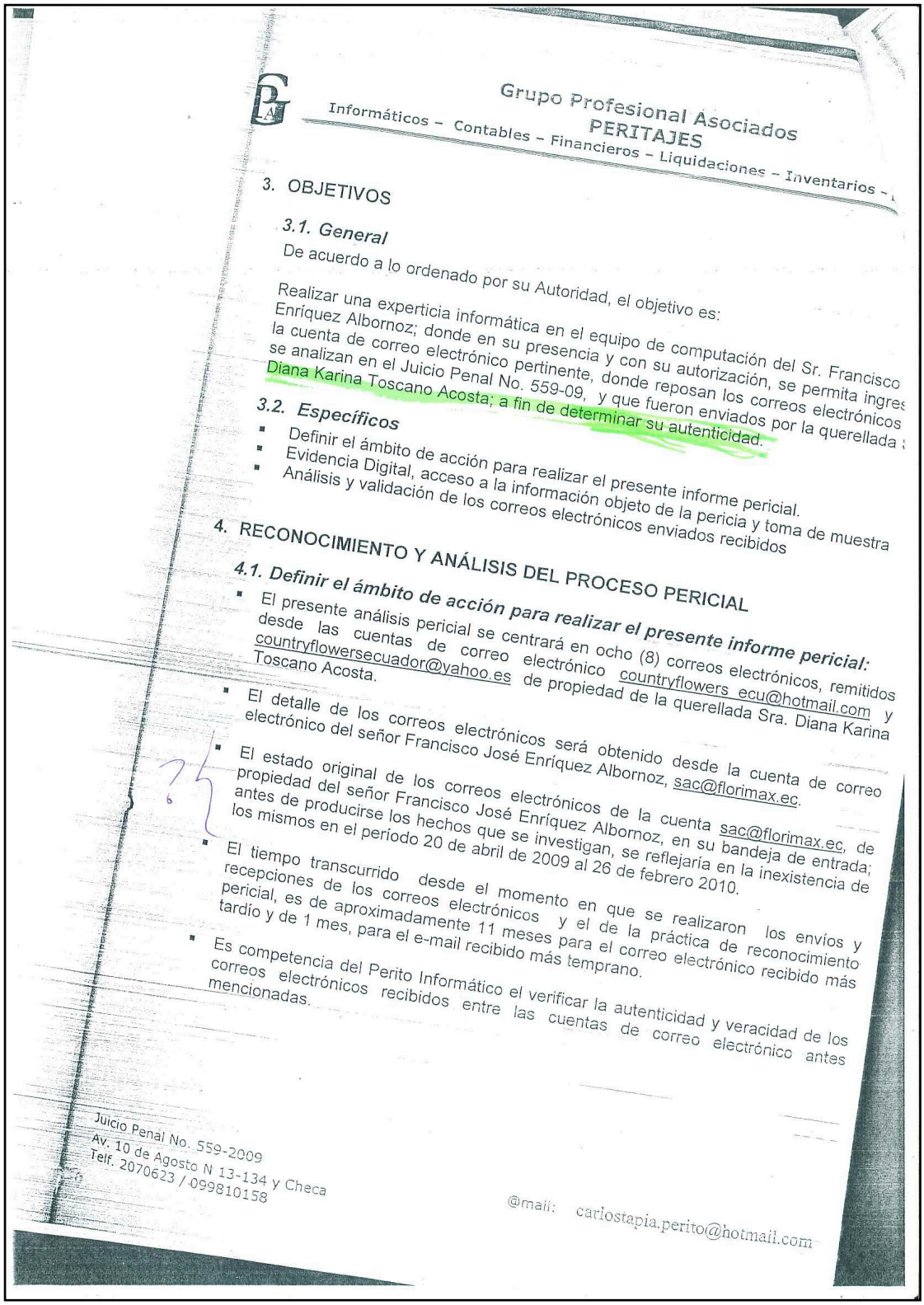
  a. Que la información que contenga sea accesible para su posterior consulta;
  b. Que sea conservado con el formato en el que se haya generado, enviado recibido, o con algún formato que sea demostrable que reproduce con exactitu la información generada, enviada o recibida;
  c. Que se conserve todo dato que permita determinar el origen, el destino de mensaje, la fecha y hora en que fue creado, generado, procesado, enviado recibido y archivado; y,
  d. Que se garantice su integridad por el tiempo que se establezca.

- Todo acceso a la información de los correos electrónicos analizados y que sor objeto del presente Informe Pericial, han sido realizados con absoluta aceptación, libre y voluntaria, del titular de la cuenta de correo electrónico sac@florimax.ec., lo que se deja constancia con la respectiva autorización escrita de que se adjunta (Anexo-1 Autorización) del presente informe.

- Con el propósito de garantizar la integridad y conservación de los mensajes de datos que puedan servir como evidencia digital en un proceso judicial, a continuación se detallan los pasos seguidos en el procedimiento pericial:

  a. Se solicita al señor Francisco José Enríquez Albornoz, acceder a los correos electrónicos que se investigan, para obtener un respaldo (Backup) de los correos que se investigan, con el objeto de no alterar la información fuente el momento del análisis de la presente pericia.

  b. El equipo que se cumplió con la diligencia:



Grupo Profesional Asociados
PERITAJES
Informáticos – Contables – Financieros – Liquidaciones – Inventarios –

3. OBJETIVOS

3.1. General

De acuerdo a lo ordenado por su Autoridad, el objetivo es:

Realizar una experticia informática en el equipo de computación del Sr. Francisco Enríquez Albornoz; donde en su presencia y con su autorización, se permita ingres la cuenta de correo electrónico pertinente, donde reposan los correos electrónicos se analizan en el Juicio Penal No. 559-09, y que fueron enviados por la querellada Diana Karina Toscano Acosta; a fin de determinar su autenticidad.

3.2. Específicos

- Definir el ámbito de acción para realizar el presente informe pericial.
- Evidencia Digital, acceso a la información objeto de la pericia y toma de muestra
- Análisis y validación de los correos electrónicos enviados recibidos

4. RECONOCIMIENTO Y ANÁLISIS DEL PROCESO PERICIAL

4.1. Definir el ámbito de acción para realizar el presente informe pericial:

- El presente análisis pericial se centrará en ocho (8) correos electrónicos, remitidos desde las cuentas de correo electrónico countryflowers_ecu@hotmail.com y countryflowersecuador@yahoo.es de propiedad de la querellada Sra. Diana Karina Toscano Acosta.
- El detalle de los correos electrónicos será obtenido desde la cuenta de correo electrónico del señor Francisco José Enríquez Albornoz, sac@florimax.ec.
- El estado original de los correos electrónicos de la cuenta sac@florimax.ec, de propiedad del señor Francisco José Enríquez Albornoz, en su bandeja de entrada; antes de producirse los hechos que se investigan, se reflejaría en la inexistencia de los mismos en el período 20 de abril de 2009 al 26 de febrero 2010.
- El tiempo transcurrido desde el momento en que se realizaron los envíos y recepciones de los correos electrónicos y el de la práctica de reconocimiento pericial, es de aproximadamente 11 meses para el correo electrónico recibido más tardío y de 1 mes, para el e-mail recibido más temprano.
- Es competencia del Perito Informático el verificar la autenticidad y veracidad de los correos electrónicos recibidos entre las cuentas de correo electrónico antes mencionadas.

Juicio Penal No. 559-2009
Av. 10 de Agosto N 13-134 y Checa
Telf. 2070623 / 099810158
@mail: carlostapia.perito@hotmail.com

4.2. Evidencia Digital, acceso a la información objeto de la pericia y toma muestra:

- Con el propósito de dar cumplimiento a lo ordenado por su Autoridad; el viernes de marzo de 2010 a partir de las 16h00, se procedió a realizar la inspección técni pericial solicitada por su Autoridad, en el domicilio del señor Francisco Jos Enríquez Albornoz, ubicado en la calle República del Salvador N34-127 y Suiz Edificio Murano Plaza, Suite 42 Con la presencia de su Abogado defensor doct Héctor Caspi y el señor perito; Ing. Carlos Tapia A.

- Para el efecto se contó con la completa colaboración por parte del denunciante, que permitió cumplir con el relevamiento, entrega de la información, constataciones y explicaciones solicitadas en el presente Análisis Pericial.

- La Evidencia Digital "es el conjunto de pruebas y constancias que quedan luego d cometimiento de un delito usando medios informático"; por lo que es necesari garantizar la integridad y la conservación de los mensajes de datos que se analiza en el presente análisis pericial. "se considera que un mensaje de datos permanec íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio d forma, propio del proceso de comunicación, archivo o presentación"; por lo que par garantizar la conservación de los mensajes de datos es necesario:

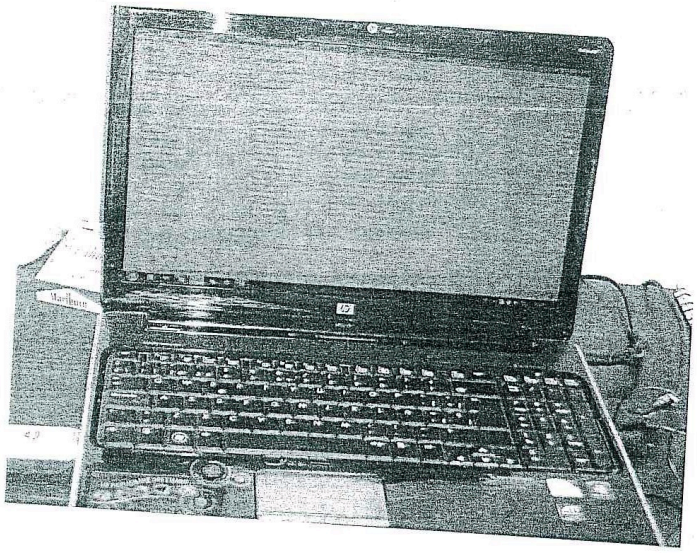
  a. Que la información que contenga sea accesible para su posterior consulta;
  b. Que sea conservado con el formato en el que se haya generado, enviado recibido, o con algún formato que sea demostrable que reproduce con exactitu la información generada, enviada o recibida;
  c. Que se conserve todo dato que permita determinar el origen, el destino de mensaje, la fecha y hora en que fue creado, generado, procesado, enviado recibido y archivado; y,
  d. Que se garantice su integridad por el tiempo que se establezca.

- Todo acceso a la información de los correos electrónicos analizados y que sor objeto del presente Informe Pericial, han sido realizados con absoluta aceptación, libre y voluntaria, del titular de la cuenta de correo electrónico sac@florimax.ec., lo que se deja constancia con la respectiva autorización escrita de que se adjunta (Anexo-1 Autorización) del presente informe.

- Con el propósito de garantizar la integridad y conservación de los mensajes de datos que puedan servir como evidencia digital en un proceso judicial, a continuación se detallan los pasos seguidos en el procedimiento pericial:

  a. Se solicita al señor Francisco José Enríquez Albornoz, acceder a los correos electrónicos que se investigan, para obtener un respaldo (Backup) de los correos que se investigan, con el objeto de no alterar la información fuente el momento del análisis de la presente pericia.

  b. El equipo que se cumplió con la diligencia:



Es una Laptop marca HP, procesador Intel Core 2 de 1.2 GHZ de velocidad y de 1,75 GB en RAM. Utiliza Windows Vista como sistema operativo, emplea como software de correo electrónico el producto Windows Live Mail, el mismo que se encuentra instalado en dicho equipo.

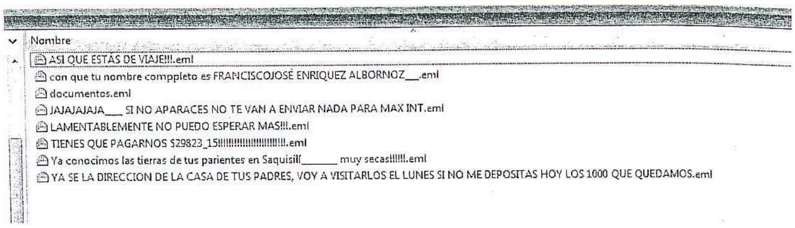
c. El Perito informa a los asistentes lo que se desea obtener; específicamente ingresar a las bandejas de entrada y salida de correo del Windows Live Mail de la cuenta del señor Francisco José Enríquez Albornoz y, ubicar los correos electrónicos requeridos (8), generar un directorio (carpeta) en el escritorio de trabajo de la Lapto utilizada, con una copia de los ocho correos electrónicos que se analizan, pero en formato *.eml, las cabeceras de cada uno de dichos correos y la captura de las pantallas de correos electrónicos (pantallazos) en un documento Word.

d. Con dicha información copiada en una carpeta se le solicita generar dos copias de la información fuente (Evidencia Digital) en medio físico CD (Compact Disk), en la que se creó la carpeta con el nombre "PERICIA 559-2009", en base a la cual el perito realizará el análisis respectivo requerido. (Adjunto Anexo-2 CD-Pericia 559-2009). La otra copia queda en custodia del doctor Héctor Caspi.

e. A continuación; utilizando el explorador de Windows, se presenta el detalle del contenido del CD generado, con la información de: nombre de los archivos, tamaño (KB) y tipo de archivos con la respectiva fecha de creación.

✓ ASI QUE ESTÁS DE VIAJE!!!.eml

- ✓ con que tu nombre compρleto es FRANCISCOJOSÉ ENRIQUEZ ALBORNOZ___.eml
- ✓ documentos.eml
- ✓ JAJAJAJAJA____ SI NO APARACES NO TE VAN A ENVIAR NADA PARA MAX INT.eml
- ✓ LAMENTABLEMENTE NO PUEDO ESPERAR MAS!!!.eml
- ✓ TIENES QUE PAGARNOS $29823_15!!!!!!!!!!!!!!!!!!!!!!!!!!.eml
- ✓ Ya conocimos las tierras de tus parientes en Saquisilí________ muy secas!!!!!!.eml
- ✓ YA SE LA DIRECCION DE LA CASA DE TUS PADRES, VOY A VISITARLOS EL LUNES SI NO ME DEPOSITAS HOY LOS 1000 QUE QUEDAMOS.eml



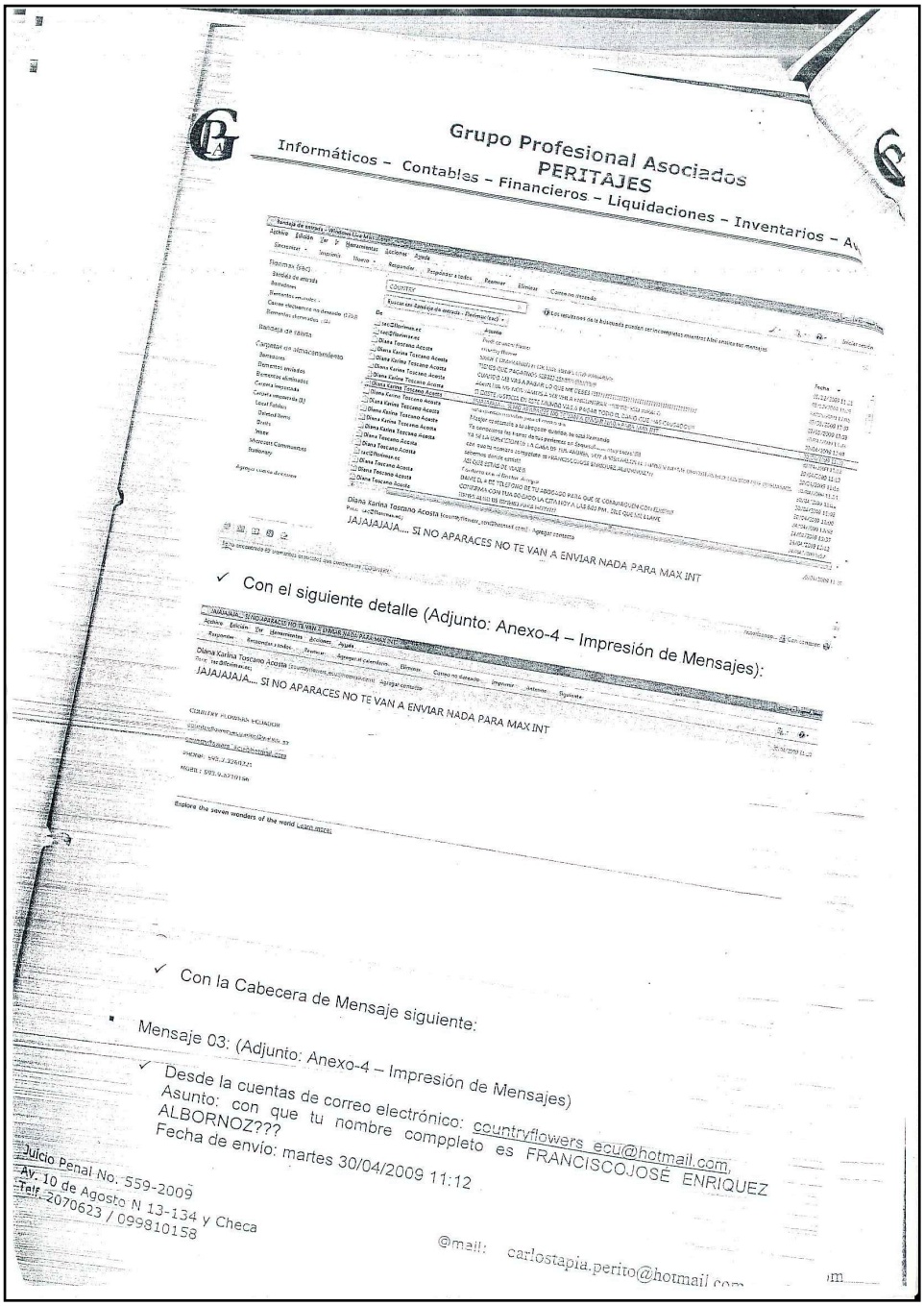
f. Se genera una Acta Entrega - Recepción con el detalle de la información ante mencionada, en la que firman el abogado defensor Dr. Héctor Caspi y el seño Perito de la Fiscalía. Constatándose la entrega de la evidencia digital (medi físico CD y la cadena de custodia de los mismos. (Adjunto Anexo-3 Act Entrega - Recepción).

4.3. Análisis y validación de la Evidencia Digital:

- Se accede al manejador de correo electrónico Windows Live Mail, donde se tiene respaldo de los mensajes recibidos objeto de la pericia; Bandeja de Entrada Usuario Florimax (SAC):

- **Mensaje 01:**

  ✓ Desde la cuenta de correo electrónico: countryflowersecuador@yahoo.es,
  Asunto: ASI QUE ESTÁS DE VIAJE!!!
  Fecha de envío: 30/04/2009 11:00



Grupo Profesional Asociados
PERITAJES
Informáticos – Contables – Financieros – Liquidaciones – Inventarios – A

JAJAJAJAJA.... SI NO APARACES NO TE VAN A ENVIAR NADA PARA MAX INT

✓ Con el siguiente detalle (Adjunto: Anexo-4 – Impresión de Mensajes):

Diana Karina Toscano Acosta
JAJAJAJAJA.... SI NO APARACES NO TE VAN A ENVIAR NADA PARA MAX INT

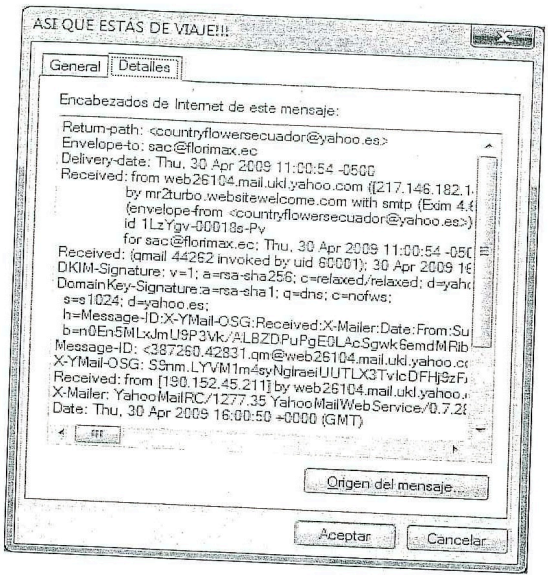
✓ Con la Cabecera de Mensaje siguiente:

▪ Mensaje 03: (Adjunto: Anexo-4 – Impresión de Mensajes)

✓ Desde la cuentas de correo electrónico: countryflowers_ecu@hotmail.com,
Asunto: con que tu nombre completo es FRANCISCOJOSÉ ENRIQUEZ ALBORNOZ???
Fecha de envío: martes 30/04/2009 11:12

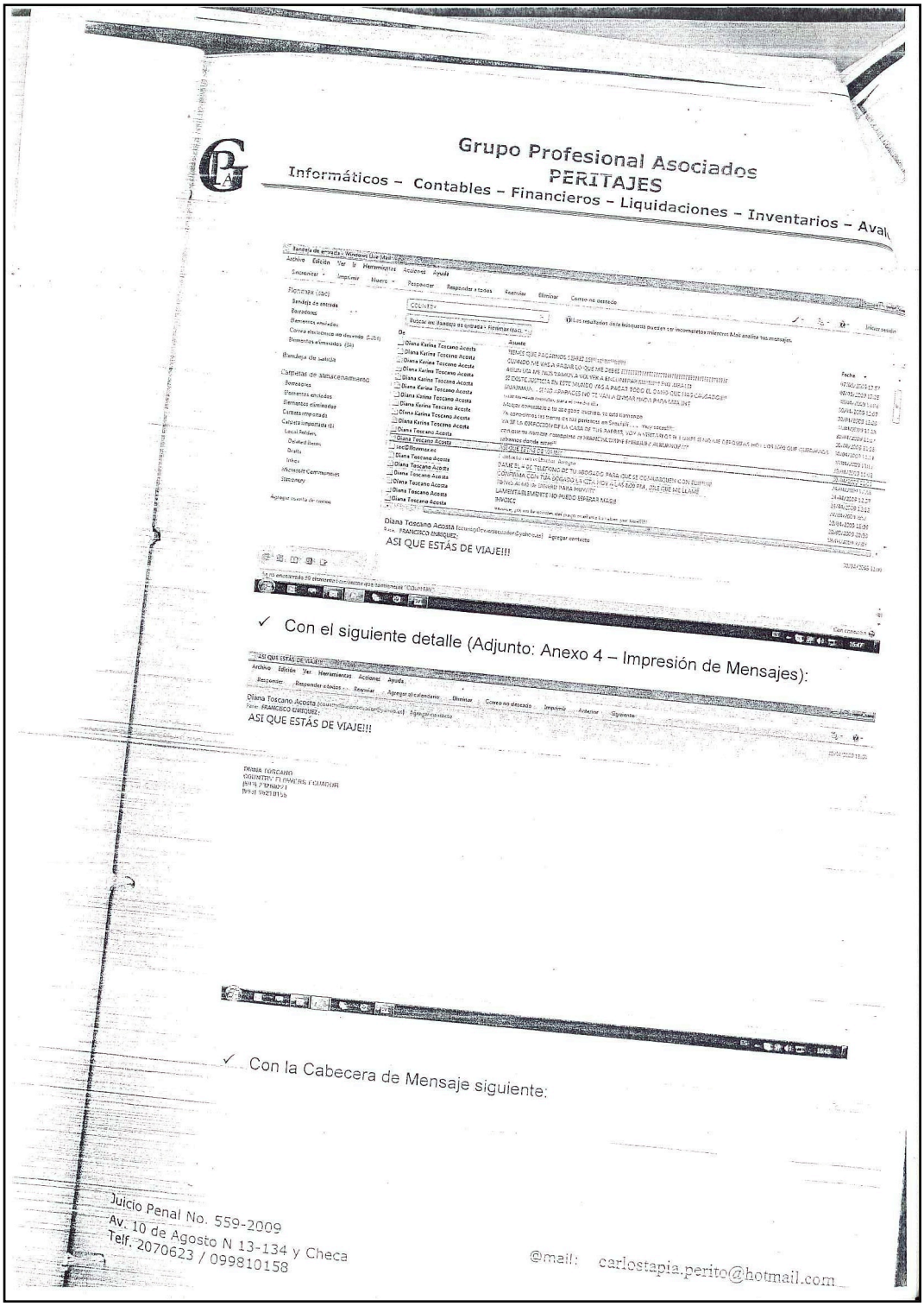
Juicio Penal No. 559-2009
Av. 10 de Agosto N 13-134 y Checa
Telf. 2070623 / 09981058

@mail: carlostapia.perito@hotmail.com



Mensaje 02:

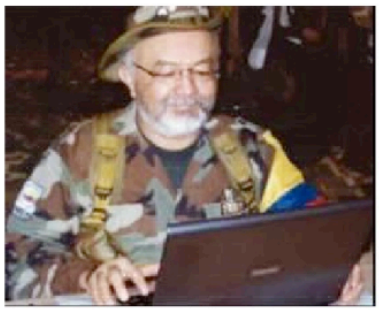
- ✓ Desde las cuentas de correo electrónico: countryflowers_ecu@hotmail.com,
  Asunto: JAJAJAJAJA____ SI NO APARACES NO TE VAN A ENVIAR NADA PARA MAX INT
  Fecha de envío: martes 30/04/2009 11:20


Grupo Profesional Asociados
PERITAJES
Informáticos – Contables – Financieros – Liquidaciones – Inventarios – Aval
Diana Toscano Acosta
ASI QUE ESTÁS DE VIAJE!!!
✓ Con el siguiente detalle (Adjunto: Anexo 4 – Impresión de Mensajes):
ASI QUE ESTÁS DE VIAJE!!!
✓ Con la Cabecera de Mensaje siguiente:
Juicio Penal No. 559-2009
Av. 10 de Agosto N 13-134 y Checa
Telf. 2070623 / 099810158
@mail: carlostapia.perito@hotmail.com

ANEXO 4: CASO RAÚL REYES.

Forénsica Digital, Interpol

y el caso Raúl Reyes (FARC)



Ing. Vincenzo Mendillo
http://vmendillo.blogspot.com

Prueba nº 30: Disco duro externo LACIE con el número de serie JJ86708J60054QR 	Prueba nº 31: Disco duro externo LACIE con el número de serie SJHHRDMH 	Prueba nº 32: Llave USB, modelo SANDISK SDCZ6-2048RB, con el número de serie BE0707AAFB 
Prueba nº 33: Llave USB, modelo Cruzer Micro 2 GB, con el número de serie 33 	Prueba nº 34: Llave USB, modelo KINGSTONCN J02907 04223-3171002F 	

13/88

Productos informáticos forenses creados a partir de las ocho pruebas instrumentales

22/88

ANEXO 5: ENTREVISTA

Entrevistada: Dra. Nancy Almendariz

Puesto: Corte Suprema de Justicia con el cargo de Asistente ADMINISTRATIVO III en la Sala de Sorteos y Casilleros.

Entrevista.

1. Dado el creciente uso de medios electrónicos de comunicación y de almacenamiento de información cotidiana, ¿Cree usted qué existe el suficiente conocimiento sobre el riesgo que los usuarios de estas tecnologías corren al utilizarlas?

No, la mayoría usa las tecnologías sin conocer los riesgos que se les pueda presentar

2. ¿Considera usted qué las personas toman las precauciones necesarias para protegerse de este tipo de actos ilegales?

No, pocas personas lo hacen.

3. Respecto a la materia de delitos cometidos a través de medios informáticos (virus, correos electrónicos, Internet, computadores, etc.), ¿Qué avances se han realizado en materia judicial?

En países desarrollados se han implementado leyes que regulan este tipo de delitos. A nivel de nuestro país no tenemos leyes específicas para este tipo de delitos. Se regula algo en la ley de comercio electrónico

4. En los delitos modernos tales como clonación de tarjetas, robo de identidad, estafas por Internet, ¿Qué procedimiento judicial se debe seguir?

El cliente afectado debe acercarse a la Fiscalía a poner la denuncia respectiva, la misma que es la encargada de hacer el seguimiento y la investigación del caso.

5. El dinero se mueve en Internet ya que permite algunas facilidades en transacciones sin necesidad de moverse del sito de trabajo u hogar, ¿En casos de delitos tecnológicos qué nivel de preparación tiene el Estado para reaccionar ante estos?

Ningún nivel, ya que no tenemos legislación ni cultura para este tipo de situaciones.

6. ¿Existe una unidad especializada en la investigación de delitos cometidos a través de medios informáticos? Si es así: ¿cómo se llama? Caso contrario:

En la Fiscalía existe la unidad de los delitos informáticos.

7. ¿Considera usted importante la creación de un departamento o unidad especializada?, ¿porqué?

Si porque cada día aumenta el riesgo por este tipo de delitos.

8. ¿Cuántos casos aproximadamente se procesan relacionados con delitos cometidos a través de medios informáticos y de qué tipo penal?

N/A

9. ¿De qué manera se recaba la evidencia material?, ¿a través de peritos externos o se cuenta con un cuerpo de peritos informáticos en la fiscalía? Si es así, considera usted ¿qué estos cuentan con la formación técnica requerida para el esclarecimiento de los hechos?

En alguna provincia sí, pero no tienen el nivel de experiencia requerida

10. ¿Conoce el procedimiento y la técnica a seguir para el análisis de la evidencia?

A nivel de la Fiscalía NO

11. ¿Esta evidencia que se recaba constituye prueba plena en proceso judicial?

No conozco.

12. ¿En que país usted cree se encuentra avanzado en el proceso de peritaje informático?, ¿porqué?

Estados Unidos e Inglaterra, tienen conocimientos en procesos y herramientas que lo soportan.

13. ¿Cree usted que se debería incluir en el código penal "el delito informático" como un tipo penal?, ¿porqué?

Sí, porque perjudica y provoca daños en las personas

14. La Informática Forense es una ciencia que sirve para dilucidar casos en donde el medio para cometer el delito fue un medio informático, ¿Ecuador hace uso de esta ciencia en casos que la necesitan?

No.

15. La intimidad y la inviolabilidad de la correspondencia virtual (y física) es algo que está protegido por la Constitución (art. 66 numeral 21), por lo cual el Estado debe velar su cumplimiento; en caso de que empresas extranjeras violen de alguna manera, ¿De qué manera el Estado protege ese derecho?

Ninguna

7. BIBLIOGRAFÍA

- Andes. (2011) 50% de transacciones electrónicas en Ecuador se realiza por internet. Consultado en septiembre del 2011 desde http://www.ecuavisa.com/noticias-nacionales/40899.html.
- Bécares, Bárbara. (2010) Asia y América Latina exportan casi la mitad del spam mundial. Consultado en septiembre de 2010, desde http://www.siliconnews.es/es/news/2010/08/09/asia-america-latina-exportan-mitad-spam-mundial.
- Cano, J (n.f) Introducción a la Informática Forense.
- Carrier, B (2005) Título del trabajo: File System Forensic Analysis. Editor:Adisson. Wesley Professional.
- Código Penal del Ecuador, Registro Oficial Nº 160 del 29 de marzo del 2010
- Consejo de la Judicatura, Dirección Provincial de Pichincha, Centro de Cómputo, (2010). Número de Causas ingresadas en las Judicaturas de Garantías Penales de Pichincha (Oficio Nº, DI-DPP-CJ-20101-MY074), Quito, Ecuador: Consejo de la Judicatura, Dirección Provincial de Pichincha, Centro de Cómputo.
- Del Pino, A (n.f) Introducción a la Informática Forense, n/a, Colombia, n/a, 10
- Gómez, E (2011) Título ¿Qué es la Informática Forense o Forensic? Consultado en febrero del 2011 desde http://www.microsoft.com/business/smb/es-es/legal/forensic.mspx
- Gutiérrez & Zuccardi Giovanni. (n.f) Informática Forense.2006, n/a, 17
- Levene R & Chariavalloti A. Delitos Informáticos. (Publicado el 05 de agosto del 2009) Consultado septiembre de 2010 desde http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3925&Itemid=426
- Ley de Comercio Electrónico, Mensajes de datos y Firmas Electrónicas del Ecuador, Registro Oficial Nº 557 del 17 de abril del 2002

- Ley de Firma Digital de Argentina, Ley 25.506 Promulgada de Hecho: diciembre 11 de 2001.
- Ley de Mensajes de Datos y Firmas Electrónicas de Venezuela, Decreto con Fuerza de Ley No 1.204 del 10 de febrero de 2001
- Ley de Comercio Electrónico de Colombia, Ley Nº 527, del 18 de agosto de 1999.
- Mendillo, V. (n/f) Forénsica Digital y el caso Raúl Reyes (FARC) Consultado en noviembre de 2011 desde http://es.scribd.com/doc/18717206/Forensica-Digital-Interpol-y-FARC
- Provos N. The Rise of Fake-Antivirus. (Publicado el 14 de abril del 2010) Consultado en octubre del 2010 desde http://googleonlinesecurity.blogspot.com/2010/04/rise-of-fake-anti-virus.html
- Rodríguez, M. Duqu, el nuevo software malicioso de la ciberguerra (Publicado el 20 de octubre del 2011) Consultado el 20 de octubre del 2011 desde http://www.bbc.co.uk/mundo/noticias/2011/10/111020_tecnologia_duqu_sotware_malicioso_mr.shtml
- SEGU-INFO. Legislación y Delitos Informáticos - Tipos de Delitos Informáticos. (n/f) Consultado en septiembre del 2010 desde http://www.segu-info.com.ar/delitos/tiposdelito.htm