FACULTAD DE INGENIERIA Y CIENCIAS AGROPECUARIAS

INFORMATICA APLICADA A LA INVESTIGACION FORENSE COMO MEDIO DE PRUEBAS – EVIDENCIA DIGITAL

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de

INGENIERA EN SISTEMAS DE COMPUTACION E INFORMATICA

Profesor Guía

ING. NELSON SALGADO

Autor

ANDREA CAROLINA MEDRANO ALARCON

Año

2012

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido este trabajo a través de reuniones periódicas con la estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación."

…….
Nelson Salgado
Ing. Informático
C.I.: 1709609588

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

"Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes"

…….

Andrea Medrano

C.I.: 171956954-1

AGRADECIMIENTO

Agradezco a Jehová DIOS, quien me ha brindado la sabiduría suficiente para desarrollar y culminar este proyecto, principalmente porque me ha permitido ver la luz de cada día.

Agradezco a mi madre, por el apoyo y paciencia brindada durante toda mi carrera Universitaria.

Y a todas las personas quienes hicieron posible que el presente proyecto haya salido adelante.

RESUMEN

El desarrollo del presente proyecto tiene como objetivo demostrar que la información que aparentemente se ha perdido, ya sea por eliminación consciente, involuntaria, daños físicos o lógicos en dispositivos de almacenamiento, se puede recuperar haciendo uso de técnicas especializadas en estos medios, en este caso técnicas que se aplican a discos duros.

Para una organización frente a un litigio legal relacionado con la pérdida de información, los datos recuperados se consideran evidencias útiles para resolver estos problemas.

La información recuperada es considerada evidencia digital, siempre y cuando los datos hayan sido tratados siguiendo las prácticas adecuadas que no alteran la información original, posteriormente estas evidencias son analizadas y relacionadas con el entorno y escenario para conocer quien fue el autor de los hechos y el momento en el que se cometió el delito.

Para el tratamiento de la información se propone procesos y técnicas para mantener los datos sin alteración alguna, este concepto se refiere a cadena de custodia de la información en el desarrollo del proyecto.

Existen herramientas que restablecen información, la que se presenta a continuación cumple con las características de recuperación intacta de datos, la misma que es usada por una organización que cuenta con valiosa información y que fue alterada por personas desconocidas que buscan intereses propios. El objetivo es averiguar quién fue el causante de este hecho y en qué momento sucedió, para que de ésta manera la empresa quede libre de culpas en cualquier caso legal en que se vea mal involucrada su información.

ABSTRACT

The development of this project is to demonstrate that the information has apparently been lost, either by removing conscious, involuntary, physical or logical storage devices can be recovered using specialized techniques in the media, in this case techniques applied to hard disks.

For an organization facing a legal dispute related to the loss of information, evidence recovered data is considered useful in solving these problems.

Information retrieved digital evidence is considered, as long as the data has been treated following the practices that do not alter the original information, then this evidence is analyzed and related to the environment and setting to know who was the perpetrator and the time when the crime was committed.

For information treatment processes and techniques is proposed to maintain the data without any alteration, this concept refers to chain of custody of information in developing the project.

There are tools that restore information, which is presented below fulfills the characteristics of data recovery intact, the same that is used by an organization with valuable information and that was altered by unknown persons seeking interests. The goal is to find out who was the cause of this fact and when it happened, that in this way the company is free of guilt in any legal case that involved look bad information.

INDICE

INDICE DE GRAFICOS

INDICE DE CUADROS

INTRODUCCION

La delincuencia actualmente hace uso de la tecnología para cometer delitos, sacando provecho de que estamos en plena era de la tecnología es necesario encontrar los métodos o mecanismos que sean de ayuda para resolver crímenes informáticos, el presente proyecto muestra una parte de lo que envuelve la informática forense, en cuanto a la información que se quiere recuperar de dispositivos de almacenamiento, para este caso discos duros, en conjunto de una metodología que no invalide las pruebas digitales.

Informática Forense

Legalmente la informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

La informática forense sirve para enfrentar desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.[1]

Evidencia Digital

Le evidencia es el aspecto más importante en cualquier disputa legal o extrajudicial, la evidencia digital son los datos que genera un equipo informático sin ser alterada ya que esto invalidará la evidencia, todo lo que se realice en estos queda registrado pudiendo ser recuperados y procesados de forma correcta para que sea presentado como evidencia dentro de un procesos legal.

Recuperación de evidencia digital

Para la recuperación de datos se debe tener en cuenta que la información perdida, eliminada o después de formateado el disco puede ser recuperada y ser prueba fundamental dentro de un proceso.

La recuperación de información como evidencia digital, debe realizarse de manera que no altere la información para evitar invalidar la evidencia, para esto

[1] INFORMÁTICA FORENSE http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

existen técnicas de recuperación, como por ejemplo el uso de herramientas que reconstruyen la información que no ha sido sobrescrita, o el uso de hardware especializado en la recuperación de discos duros, las mismas que se analizarán en el presente proyecto.

CAPITULO I

GENERALIDADES PARA EL ESTUDIO PRELIMINAR

1.1 OBJETIVOS DEL PROYECTO

1.1.1 Objetivo Principal

Analizar, investigar y evaluar sobre la investigación forense, metodología y procesos que sirvan para recuperar, recolectar, analizar y evaluar evidencias sin alterar los datos de origen de dispositivos de almacenamiento que ayuden a resolver crímenes, mediante técnicas y herramientas especializadas.

1.1.2 Objetivos Específicos

1. Desarrollar con las herramientas la solución que apoya el análisis y el estudio de informática aplicada a la investigación forense como medio de pruebas para recuperar datos de dispositivos de almacenamiento.
2. Investigar los estándares o metodologías con la finalidad de que los datos recuperados sean válidos.
3. Evaluar los resultados de evidencia digital para poder relacionarlos con el entorno y documentarlos.

1.2 PLANTEAMIENTO DEL PROBLEMA

En varios escenarios el disco duro se vuelve la única evidencia digital para resolver crímenes, este medio de almacenamiento es un dispositivo delicado ya que por su estructura y composición la información que se guarda es delicada y esta puede ser sobrescrita, lo que ocasiona que se pierda la evidencia, es por eso, que este proyecto presenta una herramienta que recupera datos sin alterarlos a pesar de que estos hayan sido eliminados o formateado el disco. En conjunto con las herramientas de análisis que presta el sistema operativo se pueden realizar estudios sobre las evidencias para que clarifiquen situaciones.

1.3 JUSTIFICACIÓN

En vista de la gran demanda de información que circula por la red permanentemente en nuestro medio y la seguridad vulnerable al momento de ser transferida y respaldada en dispositivos de almacenamiento, se ha dado origen a delitos y crímenes informáticos que tienen que ver directamente con la información.

Debido a este motivo es necesario de la computación forense como ciencia relativa que aplica procedimientos estrictos y rigurosos para ayudar a resolver problemas apoyándose en el método científico, aplicando la recolección, análisis, validación de todo tipo de pruebas digitales, para evitar en la medida de lo posible que se repita la situación, usando herramientas o técnicas que permitan recuperar datos de medios digitales, que apoyen a la aclaración de escenarios.

1.4 ALCANCE

En el medio actual la información es de vital importancia a nivel corporativo como a nivel personal, es por eso que el desarrollo del proyecto tiene como objetivo realizar la demostración de la recuperación de información del dispositivo de almacenamiento, disco duro.

Dando a conocer cuáles son las normas implantadas por el campo forense en la informática para que la información recuperada sea validada como evidencia digital, en el campo legal

El presente desarrollo analiza técnicas seguras que indican cómo recuperar datos de discos duros, sin alterar la información de origen mediante herramientas especializadas en el tema y que están ya en el mercado, siguiendo una metodología propuesta y tomando en cuenta las etapas que usa la informática forense para cumplir con la cadena de custodia.

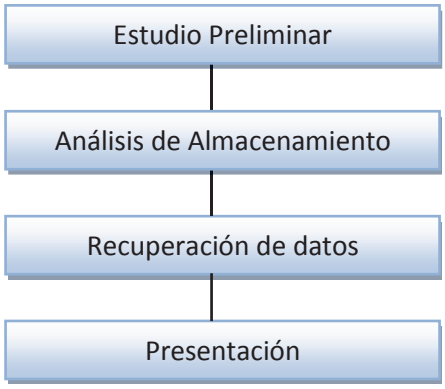
El proyecto, no incluye temas de redes forenses, ni desarrollo de herramientas para el análisis de las evidencias.

El proyecto sigue procedimientos para el análisis de los medios informáticos en conjunto con la escena para asegurar que los resultados sean válidos.

1.5 METODOLOGIA

Después de haber realizado la investigación correspondiente sobre metodologías referentes a informática forense, no existe metodología alguna que se ajuste a las necesidades específicas de este caso, pero se encontraron documentos sobre modelos de análisis forense, como por ejemplo "Fundamental Computer Investigation" de Microsoft, que indica el conjunto de procesos que se debe seguir para realizar un correcto análisis forense, en base a este documento, varios escritos y artículos, se propone las siguientes etapas, entre ellas, la etapa principal que indican cómo se debe tratar con datos que servirán de evidencia digital y las reformas legales del país sobre delitos informáticos.

Gráfico Nº 1.1 Etapas de la Metodología



Fuente: Informática Forense, Evidencia Digital
Autora: Andrea Medrano

1.5.1 Estudio preliminar

La finalidad de esta etapa es la recopilación de información suficiente y necesaria para conocer todo sobre informática forense:

- Metodología o Proceso de Análisis Forense **(1.8)**,
- Evidencia digital
- Recuperación de datos
- Tratamiento de datos

El desarrollo del proyecto se basa en análisis forense, es por eso que es indispensable que en este apartado se trate sobre políticas legales y vigentes sobre delitos informáticos en nuestro país, las mismas que se analizarán en el capítulo I.

1.5.2 Análisis de Almacenamiento

En esta fase se realiza el análisis de almacenamiento de datos, técnicas y herramientas como R-Studio, que están orientadas a la recuperación de información del disco duro como dispositivo de almacenamiento, tomando en cuenta la metodología que se aplica en informática forense para no invalidar las pruebas o evidencias digitales.

Con la finalidad de escoger la herramienta más adecuada para el desarrollo del proyecto, cuya información hace referencia a las técnicas forenses para la reconstrucción.

1.5.3 Recuperación de Datos

En esta fase se recuperan los datos usando la herramienta R-Studio teniendo en cuenta los mecanismos que se presentaron en la etapa anterior sobre el almacenamiento de datos, demostrando la no alteración de la información de manera que esta no sea inválida, tal como se demuestra en el capítulo I.

1.5.4 Presentación

Después de pasar por las etapas anteriores es el momento de la entrega de los resultados obtenidos habiendo demostrado legalmente que la evidencia existe y que cumple con normas que rige la ley, esto se demuestra en el capítulo IV en el análisis de la evidencia.

Siguiendo con la primera etapa de la metodología, a continuación se realiza el estudio preliminar tanto de los temas relacionados con la informática forense, recuperación de datos y la situación legal actual en el país.

1.6 INFORMATICA FORENSE

Es una ciencia forense que se ocupa de la utilización de los métodos científicos y analíticos aplicables a la investigación de los delitos, donde se utiliza el análisis forense de las evidencias digitales, es decir, de todo tipo de datos guardados en una computadora o sistema informático, que permite identificar, preservar, analizar y presentar datos que sean válidos en n proceso legal. La escena del crimen es el computador y la red a la cual este está conectado.

La ciencia forense necesita de una estandarización de procedimientos y de acciones a tomar, en razón de las características específicas que las infracciones informáticas presentan.

1.7 EVIDENCIA DIGITAL

La evidencia es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella. La evidencia digital es cualquier mensaje de datos almacenado y transmitido por medio de un sistema de información que tenga relación con el conocimiento de un acto que comprometa gravemente dicho sistema y que posteriormente guíe a los investigadores al descubrimiento de los posibles infractores. En definitiva son campos magnéticos y pulsos electrónicos que pueden ser recogidos y analizados usando técnicas y herramientas especiales, no es otra forma de EVIDENCIA LATENTE, necesita para su recolección y preservación principios científicos y un marco legal apropiado.[2]

1.8 PROCESO DE ANALISIS FORENSE

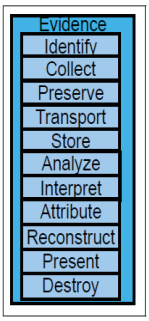
Como parte relevante para el desarrollo del proyecto y de la **metodología** propuesta, como parte del apartado **1.5.1 Estudio Preliminar**, se describe a partir de esta definición, cual es el proceso de análisis forense a una computadora que contienen datos importantes.

Las fases que se presentan a continuación, también se denominan etapas de la cadena de custodia:

---

[2] INTRODUCCION A LA INFORMATICA FORENSE
http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf

Gráfico Nº 1.2 Etapas de la cadena de custodia



Fuente: Introducción a la Informática Forense
Autor: Dr. Santiago Acurio del Pino

1.8.1 Identificación

Para que una evidencia pueda ser aplicada y procesada, primero, debe ser considerada como evidencia, para identificar una evidencia se debe tener en cuenta que cada secuencia de eventos dentro de un computador puede causar interacciones con archivos y archivos del sistema que residen ahí, otros procesos y programas que se ejecutan, archivos que se generan y archivos de registro y auditoria de varios tipos.

Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio del proceso que verifica la integridad y manejo adecuado de la evidencia, la revisión del entorno legal que protege el bien y del apoyo para la toma de decisiones con respecto al siguiente paso una vez revisados los resultados.[3]

1.8.2 Recolección

La recopilación de evidencias permite determinar el método de entrada al sistema, la actividad de los intrusos, su identidad y origen, para todo ello se debe poseer mucha precaución para evitar alterar las evidencias durante el proceso de recolección.

---

[3]COMPUTO FORENSE
httphttp://es.wikipedia.org/wiki/C%C3%B3mputo_forense#Identificaci.C3.B3n

Una evidencia debe ser recolectada con la finalidad de preservar su integridad a través de procesos, incluyendo la preservación de información relacionada al tipo de custodia bajo el cual fue recolectado y preservado.

La IOCE (Organización Internacional de Evidencias en Computadora) define cinco puntos principales para el manejo y recolección de evidencia digital:

- Al recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
- La persona que tenga acceso a evidencia digital original, deberá ser un profesional forense.
- Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.
- Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.
- Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.[4]

Este proceso se completa cuando se ha recolectado y sacado copia de la evidencia original de manera que el medio original no sea preservado sino continúe siendo utilizado con las distintas tecnologías dependiendo de las circunstancias.

1.8.3 Preservación

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia “bit-a-bit” de todo

[4]INFORMATICA FORENSE: GENERALIDADES, ASPECTOS TECNICOS Y HERRAMIENTAS
http://www.criminalistaenred.com.ar/Informatica_F.html

el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.[5]

En esta etapa el especialista en Informática Forense debe usar procedimientos como los denominados HASH CODES o Códigos Aleatorios para asegurar la cadena de custodia. Estos métodos son cifras numéricas realmente largas, específicas para cada archivo y para cada disco, que son calculadas matemáticamente. Si un archivo o disco es cambiado inclusive en su más mínima parte, este Código Aleatorio también cambiará.

1.8.4 Transporte

Las evidencias digitales deben ser transportadas de lugar a lugar generalmente de la escena del crimen hacia un lugar seguro y para esto se debe realizar duplicaciones a nivel de bit para evitar invalidar la prueba, a menudo la evidencia es copiada y enviada electrónicamente o en otros medios.

En el caso de redes se debe mantener la pureza de la evidencia, adecuando ciertas precauciones para mantener el ambiente.

1.8.5 Almacenamiento

El almacenamiento en dispositivos digitales debe ser mantenido por el periodo de tiempo requerido según el propósito. Dependiendo del medio de almacenamiento puede requerir que se cumplan controles de temperatura y humedad.

El almacenamiento debe ser asegurado adecuadamente, para cumplir con la cadena de custodia y en especial las áreas de evidencias que contienen grandes volúmenes de evidencias, deben tener documentos asociados con todas las acciones realizadas de la evidencia y ser asegurados, de tal manera que la evidencia no pueda salir a ningún lado sin haber sido registrada.

---

[5]INFORMATICA FORENSE, INTRODUCCION Y CONTENIDO
http://labs.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido

La **RFC3227**, es la guía para la recolección y almacenamiento de evidencias que tiene como propósito proveer las pautas a seguir en el aspecto de recolección y almacenamiento de evidencias para los casos de incidentes de seguridad.

En este RFC3227, se debe tener en cuenta los siguientes aspectos en cuanto al almacenamiento:

1.8.5.1 El procedimiento de archivo

Las pruebas deben ser estrictamente aseguradas. Además la cadena de custodia debe estar claramente documentada.

1.8.5.2 Cadena de Custodia

El investigador debe ser capaz de describir claramente la manera en que la evidencia fue encontrada, como se la manejó y todo lo que le sucedió.

Lo siguiente debe ser documentado:

- Dónde, cuándo y por quién la evidencia fue descubierta y recogida.
- Dónde, cuándo y por quién la evidencia fue examinada.
- Quién tuvo la custodia de la evidencia, durante qué período y cómo fue almacenada.
- Cuándo la evidencia cambió de custodia, cuándo y cómo ocurrió la transferencia (incluir número de envíos, etc.)

1.8.5.3 Modo de Almacenamiento

Si es posible use medios de almacenamiento común (en lugar de medios de almacenamiento oscuros).

El acceso a la evidencia debe ser extremadamente estricto, y debería ser claramente documentado. Esto hará posible la detección del acceso no autorizado.

1.8.6 Análisis, interpretación y atribución

Es la etapa en la que el investigador busca filtrar todos los objetos recolectados y preservados en la escena del delito a fin de separa los objetos que no tiene

valor como evidencia de los que sí, para esto se utiliza una serie de instrumentos y técnicas para localizar y extraer la evidencia para luego ponerle en el contexto de la investigación.

Para el análisis, interpretación y atribución se procede a realizar las comprobaciones necesarias y a la manipulación de los datos, para ello puede ser tan fácil como arrancar el sistema operativo y mirarlo en modo gráfico, o bien realizar una lectura a nivel físico y determinar la solución mediante los bits.

Es importante tener en cuenta que cada actividad que se realice en el computador tiene un archivo de registro asociado con el respectivo detalle, por lo tanto las secuencias de los eventos aparecen en un registro y estos registros son usados como base para el análisis, interpretación y atribución.

El análisis requiere que se estudie el documento recuperado y esto puede hacerse con las mismas herramientas del sistema operativo, tomando en cuenta los siguientes aspectos:

- Propiedades del Archivo
- Registro de aplicación
- Registro de seguridad
- Registro de sistema
- Diagnóstico de aplicativos
- Sesiones de aplicativos

Con la ayuda de la herramienta en recuperar la información sin alteraciones y revisando cada uno de estos ítems se llega a obtener los detalles del último acceso, modificación del archivo, desde que equipo se accedió, entre otras cualidades con las que se puede ya obtener un juicio sobre la situación.

1.8.7 Reconstrucción

La reconstrucción de los hechos informáticos incluye conceptualmente el establecimiento de la secuencia de producción de actividades en un computador o en redes. La recuperación de Evidencia Digital dañada entra también en esta categoría.

Es importante que en la pericia informática registre cada acción realizada durante su práctica a efectos de hacer posible la evaluación de los protocolos de manejo de

evidencia o bien a efectos de confirmarse los resultados en ampliaciones y aclaratorias del dictamen.

La reconstrucción relacional de los hechos informáticos es importante a efectos de establecer su relación con otro tipo de evidencia del mismo caso. El perito debe tratar de hacer una especie de línea del tiempo cuando la complejidad de los hechos que está evaluando así lo requiera.

1.8.8 Presentación

La evidencia, análisis, interpretación y atribución, por último es presentada en forma de informes periciales, declaraciones y testimonios.

La presentación debe ser entendible y convincente, es decir, se debe reseñar los procedimientos y las técnicas utilizadas para recolectar, preservar y filtrar la evidencia de manera que exista certidumbre en los métodos usados, aumentado así la credibilidad del investigador en un contra examen de los mismo.

1.8.9 Destrucción

Los tribunales a menudo en lo que refiere a las evidencias y otra información relacionada con asuntos legales solicitan ser destruidas o devueltas al final del proceso.

Esto aplica al comercio secreto, patente e información confidencial relacionada con el cliente, derechos de autor de obras y la información de empresas que normalmente disponen pero deben ser retenidas durante el proceso legal.

1.9 DELITO INFORMATICO

Según revistas y el estudio de conceptos de abogados, el delito informático se considera como aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático, como en todo delito aparecen el sujeto activo y el sujeto pasivo:

El sujeto activo, es la persona que tiene conocimiento elevado sobre informática o sistemas de computación

El sujeto pasivo, en este caso puede ser una persona o una institución que cuenta con sistemas automatizado de información.

1.9.1 Tipos de Delitos Informáticos

Las Organizaciones Internacionales tras varios estudios consideran como delitos informáticos a:

- La manipulación de computadoras para cometer fraude.
- Los datos de entrada manipulados.
- Los programas manipulados.
- Los datos de salida manipulados.

1.9.2 Falsificaciones Informáticas

Se considera falsificación a la alteración de datos de los documentos almacenados en forma computarizada, y

Al uso de computadores para efectuar falsificaciones de documentos comerciales.

1.9.3 Legislación Ecuatoriana

El Ecuador actualmente no posee legislación informática, a excepción de la ley de comercio electrónico, firmas y mensaje de datos aprobada en abril de 2007, en el que se le da la importancia necesaria a la información escrita y original.

La ley de propiedad intelectual vigente en el Ecuador desde mayo de 1989 trata sobre programas de ordenador, protección de derechos de autor no como invento o descubrimiento sino como obra literaria.

Al momento existe el Código Orgánico Integral Penal que se encuentra en discusión y pendiente de aprobación, el cual en el TITULO III – DE LAS INFRACCIONES EN PARTICULAR, trata sobre los siguientes temas:

Capítulo Primero

De las infracciones contra los derechos de libertad

Sección Novena

Infracciones contra la propiedad

Artículo 152.- Apropiación fraudulenta por medios electrónicos.- Quienes utilicen fraudulentamente un sistema de información o redes

electrónicas y de telecomunicaciones, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, **manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos o mensajes de datos y equipos terminales de telecomunicaciones, serán sancionados con pena privativa de libertad de tres a cinco años.**

La misma sanción se impondrá si la infracción se hubiese cometido con inutilización de sistemas de alarma o guarda; descubrimiento o descifrado de claves secretas o encriptadas; utilización de tarjetas magnéticas o perforadas; utilización de controles o instrumentos de apertura a distancia; y, violación de seguridades electrónicas, informáticas u otras semejantes.

Quienes alteren los números de serie físicos y electrónicos que identifican un equipo terminal de telefonía móvil, o estén en tenencia de infraestructura para el efecto, quienes activen y comercialicen estos equipos robados o hurtados; serán reprimidos con las penas señaladas. Sin perjuicio de las sanciones administrativas y adopción de medidas cautelares conforme a la Ley Especial de Telecomunicaciones.

Artículo 153.- Estafa.- Quien obtenga para sí o un tercero provecho económico, valiéndose de cualquier ardid o engaño para provocar error en otra perjudicando su patrimonio o el de un tercero, será sancionado con pena privativa de libertad de tres a cinco años.

Igual pena tendrá quien:

1. Disponga bienes litigiosos, bienes embargados o gravados de conformidad con la ley, la autoridad o el contrato;

2. Defraude mediante el uso de tarjeta de crédito, débito o compra, cuando ella hubiere sido alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario;

3. Entregue en calidad de administradora o administrador de una compañía o sociedad sujeta a control información falsa;

4. Entregue en calidad de administradora o administrador, apoderada o apoderado, corredora o corredor de una bolsa de valores, o agente de valores, certificación falsa sobre las operaciones o inversiones que se realicen en ella;

5. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento; o,

6. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor, sea que las transacciones se lleven a cabo en el mercado de valores o a través de negociaciones privadas;

Será sancionado con pena privativa de libertad de cinco a siete años quien estafe realizando uno de los siguientes casos:

1. **Perjudique a más de cinco personas, o cuando el monto del perjuicio sea igual o mayor a cincuenta remuneraciones básicas unificadas del trabajador privado en general; y**,

2. Fraccionare, subdividiere, urbanizare o lotizare sin permiso de autoridad competente.

Será sancionado con pena privativa de libertad de siete a nueve años cuando se estafe a través de una institución financiera o se utilicen fondos públicos o de la seguridad social.

Será sancionado con pena privativa de libertad de seis meses a un año la persona que realice cualquiera de las siguientes infracciones:

1. Engañe a otra sobre la sustancia, peso, cantidad o calidad en la entrega de artículos de primera necesidad; y,

2. Otorgue un contrato ficticio o falsos recibos o facturas.

Si el perjuicio es de ínfima cuantía la pena privativa de libertad será de seis meses a un año.

Capítulo Tercero
Infracciones contra el Buen Vivir
Sección Segunda
Infracciones contra la información

Artículo 203.- Base ilegal de datos.- Quien obtenga, compile, archive, transfiera, comercialice o procese datos personales sin autorización judicial o de su titular; o quien ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; o revelare información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley, será sancionado con pena privativa de libertad de uno a tres años la persona que:

Si las conductas antes descritas se cometen por parte de una persona en ejercicio de un servicio o función pública, será sancionado con pena privativa de libertad de tres a cinco años.

Artículo 204.- Daño informático.- Quien dolosamente, destruya, altere, inutilice, suprima o dañe, los programas, datos, bases de datos, información o cualquier mensaje de datos contenidos en un sistema de información o red electrónica, de forma temporal o definitiva; será sancionado con pena privativa

de libertad de tres a cinco años y multa de diez a veinte remuneraciones básicas unificadas del trabajador privado en general.

Con igual pena serán sancionados en los siguientes casos quienes:

1. Vendan o distribuyan de cualquier manera programas destinados a causar los efectos señalados en el párrafo anterior;

2. Obtengan una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, destinados a causar los efectos señalados en el párrafo anterior; o,

3. Destruyan la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o está vinculada con la defensa nacional la pena privativa de libertad será de cinco a siete años.

Artículo 205.- De la intrusión indebida a los sistemas informáticos, de información o telemáticos.- Son responsables de intrusión indebida a los sistemas informáticos, de información, o telemáticos quien por cualquier medio o fin, y con el ánimo de apoderarse de la información contenida en dichos sistemas, o para descubrir los secretos comerciales o industriales, o bien para vulnerar la intimidad de una persona natural o jurídica, sin su consentimiento o autorización, interfieran, interrumpan o se apoderen de cualquier mensaje de datos, serán sancionados con pena privativa de libertad de tres a cinco años y multa de diez a veinte remuneraciones básicas unificadas del trabajador privado en general.

Si la divulgación o la utilización fraudulenta de los datos o información reservada, los secretos comerciales o industriales, se realiza por la persona o

personas a las cuales se les encomendó su custodia o utilización, serán sancionados con pena privativa de libertad de cinco a siete años.

Artículo 206.- Falsificación electrónica.- Quien utilizando cualquier medio altere, borre o suprima deliberada e ilegítimamente datos informáticos que generen datos no auténticos con la intención que sean tomados o utilizados a afectos legales como auténticos con independencia de que los datos sean legibles o inteligibles será sancionado con pena privativa de libertad de cinco a siete años.

Artículo 207.- Falsedad informática.- Quien copie, clone o imite una página web con la finalidad de obtener la información general que el usuario ingrese en ella, será sancionada con pena privativa de libertad de siete a nueve años.

Artículo 208.- Estafa informática.- Quien defraudare a otra, modificando o suplantando el sistema informático que altere su normal funcionamiento, transmisión o mensajes de datos, será sancionado con pena privativa de libertad de nueve a once años.

En resumen,

Cuadro Nº 1.1 Resumen de Represiones de los Delitos Informáticos

Infracción Informática	Represión	Multa
1. Apropiación fraudulenta por medios electrónicos	3 - 5 años	
2. Base ilegal de datos	1 - 3 años	
3. Daño informático	**3 - 5 años**	**10 - 20 remuneraciones básicas unificadas**
4. Intrusión indebida a los sistemas informáticos	3 - 5 años	10 - 20 remuneraciones básicas unificadas
5. Falsificación electrónica	**5 - 7 años**	
6. Falsedad Informática	7 - 9 años	
7. Estafa Informática	9- 11 años	

Autora: Andrea Medrano

Esta es una pequeña parte del código penal a ser discutida y analizada por la asamblea nacional en cuanto a delitos informáticos, sin embargo para otros aspectos relacionados con temas legales informáticos que aún no han sido estudiados, propuestos o aceptados a nivel nacional, la fuente de consulta son las legislaciones de otros países desarrollados en tecnología.

CAPITULO II

ALMACENAMIENTO Y RECUPERACION DE DATOS EN MEDIOS MAGNETICOS

2.1 GRABACION EN MEDIOS MAGNETICOS

Los usuarios han usado una variedad asombrosa de materiales y medios para guardar información, técnicamente llamados medios de grabación o almacenamiento de datos, cualquier substancia que pueda ser sistemáticamente transformada se puede usar para grabar información

Existieron varias técnicas de almacenamiento inicialmente, tal como el almacenamiento de información en papel, usando como método la perforación sobre el papel, pero con el pasar del tiempo el mismo se tornó voluminoso, y surgió la necesidad de crear medios que almacenen más datos pero que ocupen menos espacio físico, por lo que se crearon discos plásticos o de metal que acaparan más información, llamados discos duros.

A continuación se explica cómo se realiza el almacenamiento de datos, como se requiere en la metodología en el capítulo I, en el Análisis de Información, para entender después hasta dónde y cómo se realiza la recuperación de la información de un disco duro.

2.1.1 Principios físicos

Los medios de almacenamientos para realizar su función se basan en cuatro principios físicos, los mismos que son:

A. Presentar corriente eléctrica para producir campos magnéticos
B. Existen materiales suaves que se magnetizan con facilidad, a penas el campo eléctrico es expuesto al cuerpo. Cuando se aleja el campo eléctrico el cuerpo se desmagnetiza. A estos cuerpos se los conoce como Materiales Magnéticos Suaves.

C. En materiales magnéticos suaves, cuando el material es magnetizado su resistencia eléctrica cambia y el valor de la resistencia eléctrica regresa a su valor original cuando el campo magnetizante se apaga o aleja, este fenómeno se denomina Magneto-Resistencia (MR). A esta especificación existe una variación; la Magneto-Resistencia Gigante (GMR), que consiste en que el efecto Magneto-Resistencia es más fuerte y se da en materiales de películas delgadas.
D. Existen cuerpos que se magnetizan con mayor dificultad, ya que para estos es necesario un campo magnético más fuerte, pero cuando son magnetizados por más que se desmagneticen mantienen su valor. Estos se denominan Materiales Magnéticos Duros, o Magnetos Permanentes.

Estos principios son usados por industrias que se especializan en leer, escribir, eliminar y recuperar datos con cabezas grabadoras magnéticas en discos de almacenamiento u otros medios magnéticos.

Aplicaciones en almacenamiento de datos:

- Cabeza de Escritura: Se usan para escribir bits de información en dispositivos de almacenamiento, específicamente en discos que usan platos giratorios que se magnetizan, para esto necesitan de los dos primeros principios básicos vistos anteriormente, es decir, un campo magnético y un cuerpo que se magnetice.
- Cabeza de lectura.- Para escribir, las cabezas hacen uso de los tres primeros principios, es decir, que aparte del campo magnético y del cuerpo que se magnetiza, tiene el principio de la Magneto-Resistencia y adicionalmente son perceptibles a los campos magnéticos de los medios magnéticos.
- Disco Duro.- Usan principalmente el último principio, es decir, que cuando un medio es magnetizado guarda su valor permanentemente, los discos duros se magnetizan de manera indestructible, en dirección norte o sur determinado por el campo de escritura.

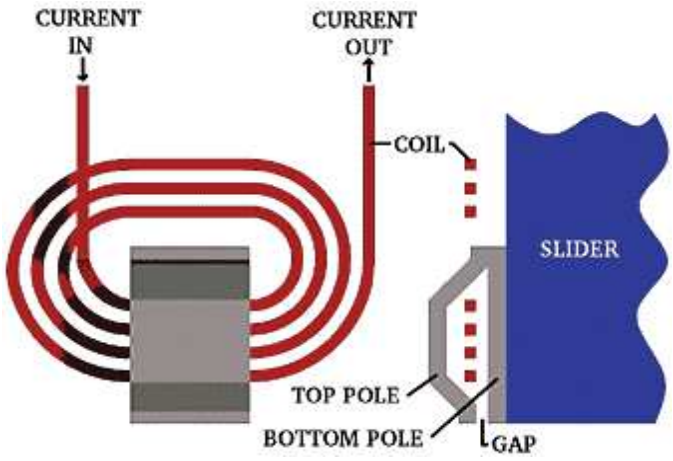
2.1.2 Escribiendo Datos Magnéticos

El gráfico que se presenta a continuación, muestra una cabeza de escritura, que en la parte superior cuenta con un espiral que está cubierto por dos capas de material magnético suave tal como se ve abajo y al lado derecho una parte de la cabeza cortada perpendicularmente y vista de lado.

En el gráfico, en la parte derecha se visualiza que las capas en la parte inferior tienen un espacio entre sí, pero en la parte superior las capas se encuentran unidas, este escenario es para que las capas magnéticas se magneticen sin dificultad, cuando pase por el espiral una corriente eléctrica y de esta manera actúen como polos Norte y Sur de un electro-magneto.

En una cabeza real, la distancia desde el espacio hasta la parte superior del rollo es de aproximadamente 30 mm.[6]

Gráfico Nº 2.1 Una cabeza de escritura



Fuente: Informática Forense
Autora: Beatriz Acosta

En el extremo inferior, el espacio de la cabeza de escritura, es el lugar en que el campo de escritura sale de la cabeza al espacio.

[6] INFORMATICA FORENSE: GENERALIDADES, ASPECTOS TECNICOS Y HERRAMIENTAS
http://gluc.unicauca.edu.co/wiki/images/1/1d/InfoForense.pdf

Debido a esto cuando el disco de almacenamiento pasa cerca de la cabeza de escritura, el disco o material magnético duro se magnetiza permanentemente y toma el valor o la polaridad que le transmite la cabeza de escritura, si el valor de la corriente eléctrica cambia, la polaridad de en la cabeza de escritura cambia y por su puesto el valor en el disco también cambiará.

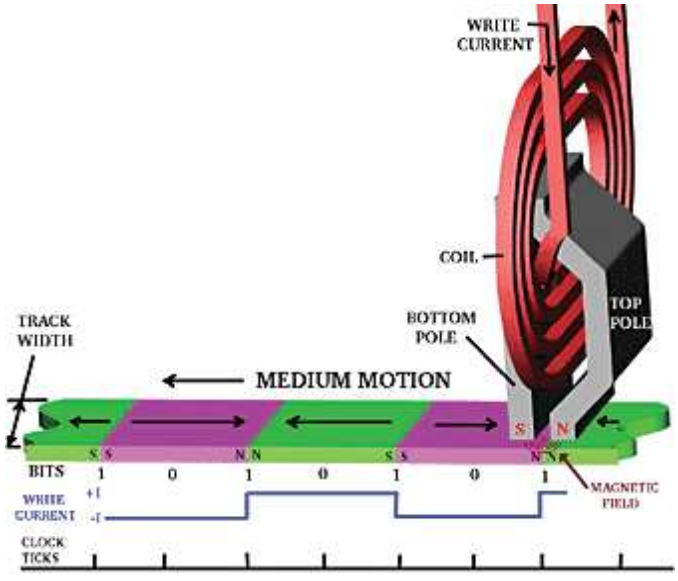
Estos valores de polaridad se almacenan en los discos a manera de dígitos binarios, es decir, en bits, ceros y unos. Este caso se entiende gráficamente en el gráfico 4.

Un bit uno es el cambio de polaridad de la corriente.

Un bit cero es la ausencia de cambio de polaridad en la corriente.

Por lo tanto cuando un disco gira cerca de la cabeza de escritura y no hay dirección magnética o flujo de corriente se guardará ceros, pero cuando hay dirección magnética guarda unos.

Gráfico Nº 2.2 Escribiendo datos en un medio de almacenamiento



Fuente: Informática Forense
Autora: Beatriz Acosta

La rotación del disco está sincronizado por un reloj interno que regula los ticks con celdas de bits, que guardan unos cuando la polaridad cambia de Norte a Sur o de Sur a Norte y ceros cuando hay polaridad Norte constante o Sur constante, una vez que los bits se escriben sobre la superficie del disco, este valor magnético no cambiará hasta que nuevos patrones magnéticos se sobrescriban sobre estos.

Es importante que cuando un campo magnético se va a transmitir, la cabeza de lectura pase muy cerca al disco magnetizado para que pueda captar bien la información, ya que su fuerza se desvanece rápidamente a medida que la cabeza de grabación se aleja.

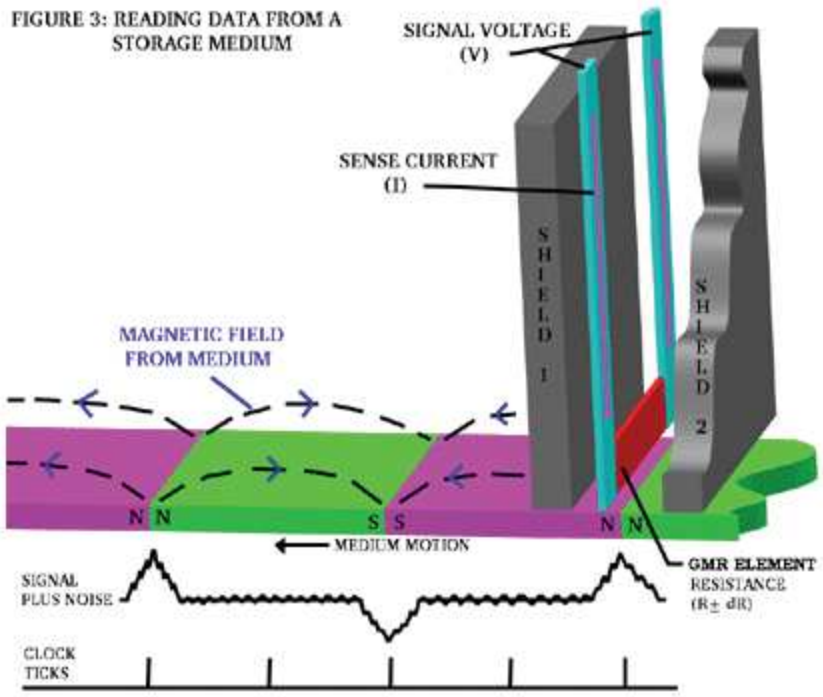
2.2 LEYENDO DATOS MAGNÉTICOS

Los datos magnéticos son leídos por cabezas de lectura a través de resistores magnéticos sensitivos, conocidos como Válvulas Spin, estas válvulas descargan el efecto Magneto-Resistencia Gigante (GRM), el proceso que hacen estas cabezas es ubicarse cerca de la lámina de almacenamiento o disco giratorio para poder captar los valores del disco que ya están escritos, basta con que las cabezas se alejen solo un poco del objetivo para que no puedan tomar fielmente el valor escrito en el disco.

En la lectura de un disco de los bits escritos, pasan corrientes magnéticas por la cabeza de lectura (GMR) que detectan cambios en la resistencia eléctrica debido al cambio de voltaje, esta señal es transmitida por los canales sensores de la cabeza de lectura, en conjunto con el ruido eléctrico que está siempre presente en la transmisión de datos que usan circuitos eléctricos.

Esta señal junto con el ruido se transportan por cables a los circuitos electrónicos en el disco duro hasta que la secuencia de tiempo de los impulsos se decodifique en unos y ceros. Este proceso se ve graficado a continuación.

Gráfico Nº 2.3 Leyendo datos desde un medio de almacenamiento



Fuente: Informática Forense
Autora: Beatriz Acosta

2.3 ANÁLISIS DE DISCOS

El análisis de discos es una técnica de bastante ayuda para el tema de la informática forense, ya que además de poseer el disco archivos de gran valor y que pueden incriminar a culpables en varios casos, también posee información como claves y usuarios que han usado equipos que son evidencias para casos legales.

Las personas al no conocer cual es el verdadero funcionamiento de los discos, piensan que al suprimir un archivo, este es eliminado por completo del equipo, esto no es así, ya que queda registrada la marca en el disco físico y esta información no es borrada a menos que se utilicen herramientas especializadas en la eliminación de datos en un dispositivo de almacenamiento.

Personas que conocen del tema como informáticos forenses pueden explotar de gran manera su conocimiento poniendo en práctica herramientas forenses que recuperen información que ha sido borrada supuestamente.
A continuación se presenta teorías sobre cómo se almacena y destruye datos en un disco o medio de almacenamiento.

2.3.1 File Slack

Cuando los archivos son creados, el sistema operativo guardan esta información en espacios de tamaño fijo llamado clusters que crea el disco duro, en raras ocasiones el tamaño del archivo coincide con el tamaño del cluster, de manera que cuando el fichero se almacena queda espacio disponible en el cluster, este espacio entre el final del archivo y el final del cluster se denomina File Slack.
Este espacio, se va ocupando de manera aleatoria, ya que la memoria va almacenando aleatoriamente información en los bloques o clusters y si llega a faltar espacio, entonces se asignan sectores disponibles de los clusters para completar el espacio sobrante con información que se encuentra en la memoria del sistema.
El File Slack o Slack Space, en la informática forense es analizado porque puede contener valiosa información.

2.3.2 Archivo Swap de Windows

El sistema operativo Microsoft crea apuntes o direcciones a manera de mapas, que registran los lugares específicos en donde se encuentran estos espacios de memoria disponible, este archivo que guarda estas indicaciones se denomina archivo Swap de Windows o archivos de paginación.
Una computadora normalmente usa la memoria primaria o RAM para almacenar información usada para operaciones actuales, pero el archivo Swap sirve como memoria disponible para información adicional.
Estos archivos tienen un tamaño que oscila entre los 20 MB y 200 MB.

Al usar el archivo Swap la computadora tiene la capacidad de usar más espacio en memoria virtual, ya que es el espacio físico disponible que la memoria usa para hacer sus operaciones, como por ejemplo el ingresar a una base de datos, usuarios y cuentas a las que se ingresan, así como actividades en el internet y que se almacenan de manera transparente al usuario, esta información es valiosa para investigaciones forenses y que solo se las puede encontrar de esta manera.

2.3.3 Almacenamiento no Asignado

Es el espacio en un disco duro que contiene potencialmente los archivos intactos, subdirectorios o archivos temporales que fueron creados pero luego fueron suprimidos por una aplicación de computador, por el sistema operativo o por el usuario.

Cuando los archivos se eliminan, no han sido borrados de manera permanente ya que se conservan en un espacio de almacenamiento no asignado o también llamado Unallocated File Space, por lo tanto los archivos aun se encuentran pero ocultos y pueden ser recuperados con herramientas especializadas en informática forense.

2.4 ELIMINACIÓN DE DATOS

En los apartados anteriores se ha estudiado como se almacena información en los discos duros, cuáles son los procesos y en donde quedan guardados los datos, pero para especialistas en informática forense es necesario también conocer cuál es el proceso, las herramientas o técnicas que se deben usar para eliminar datos de un dispositivo de manera definitiva, los mismos que se analizan a continuación.

2.4.1 Eliminación de Datos en un Medio Magnético

La eliminación de datos en realidad no es un tema tan simple como muchas personas creen, pues el hecho de borrar información involucra seguir métodos o procedimientos que permiten desaparecer datos de manera definitiva de dispositivos, que en ciertos casos es necesario, y más aun cuando los medios

de almacenamiento usan materiales que se magnetizan para almacenar información.

Debido a esto, organizaciones internacionales como el Departamento de Defensa de los Estados Unidos (DoD) y la organización Defense Scurity Service, cuentan con una serie de documentación que indican como borrar información de dispositivos magnéticos, matrices con procedimientos a seguir para limpiar medios, remover información delicada de manera segura y de varios dispositivos.

2.4.2 Desmagnetización de Medios Magnéticos

El método más usado para la eliminación permanente de datos de un dispositivo magnético, como lo es el disco duro, es la destrucción física del medio, usando varios métodos con tal de pulverizar la evidencia. Pero existe una técnica llamada Desmagnetización o conocida también como Degaussing en inglés, que limpia o sanitiza de manera definitiva los datos que han sido almacenados anteriormente, la Desmagnetización es un proceso que consiste en aplicar un campo magnético sobre un medio digital de manera que limpie al disco, existen dos manera de desmagnetizar un medio de almacenamiento magnético:

2.4.2.1 Desmagnetización Magnética.

Consiste en usar potentes imanes que generan fuertes campos magnéticos sobre el medio para borrar los datos. El imán hace todo el trabajo y no hay necesidad de energía eléctrica.

2.4.2.2 Desmagnetización Electromecánica

Utiliza la acumulación de energía eléctrica, cuando la electricidad alcanza el nivel necesario esta es descargada y la energía resultante remueve la información de la superficie magnética.

Organizaciones como, National Security Agency (NSA) evalúa varios desmagnetizadores para satisfacer la necesidad de limpiar los medios magnéticos, ya que esta técnica es muy útil para el gobierno americano.
Mientras que organizaciones como el National Institute of Standards and Technology (NIST) recomiendan variedad de métodos para la destrucción física total de los medios magnéticos.
La Desmagnetización se usa como método anti forense y se lo utiliza rara vez, debido al alto costo de las máquinas y es difícil para el consumidor final pagar altos precios y optan por la destrucción de la evidencia.

2.4.3 Eliminación de Datos en CDs

El CD guarda los datos en una lámina reflectiva que se encuentra en la parte superior y que es cubierta por policarbonato, la lámina almacena los datos y estos son leídos por láser, pueden guardarse por largos periodos de tiempo, es por eso que para eliminar la información es necesario destruir el CD para asegurarse que la data se borre permanentemente. Existen algunos métodos que se recomiendan para esto:

- Romper en pedazos el CD, cortándolo con alguna herramienta asegurándose de que la lámina reflectiva se corte también.
- Quitar la lámina reflectiva y destruirla
- Regar químicos fuertes sobre la capa superior, logrando así que la lámina se desvanezca.
- Aplicar campos magnéticos fuertes al CD, como por ejemplo de un horno microondas, sin embargo este método no es muy recomendable debido al contacto entre el campo magnético y a los metales que contiene el CD.
- La sobrescritura de datos sobre CDs reescribibles asegura que la información que estaba inicialmente se pierda, ya que los datos actuales toman su lugar.[7]

[7] INFORMATICA FORENSE: GENERALIDADES, ASPECTOS TECNICOS Y HERRAMIENTAS
http://gluc.unicauca.edu.co/wiki/images/1/1d/InfoForense.pdf

2.5 RECUPERACIÓN DE INFORMACIÓN DE DISPOSITIVOS DE ALMACENAMIENTO

La recuperación de datos nace a través de daños o defectos en los dispositivos de almacenamiento y eliminación voluntaria o involuntaria de información, esta recuperación se puede hacer de medios como CD, DVD, HDD o cualquier otro dispositivo electrónico.

Cuando el dispositivo tiene problemas en ser accedido para leer los datos, lo que usualmente se hace es tratar de acceder al medio desde otro lugar lógico o físico, lógicamente puede ser desde otro volumen de datos y físicamente, instalándolo en otro equipo, en el caso de que sea un disco duro, con la finalidad de rescatar la información y crear una copia de lo obtenido.

En el caso de que los datos son eliminados consciente o inconscientemente, estos pueden ser recuperados con herramientas especializadas en hacer esta actividad, a menos que la información se haya sobrescrito por otra reciente.

2.5.1 Recuperación Física de Información de Discos Duros

Un método de recuperación de la información es la reparación física, esta técnica consiste en retirar los platos del disco duro dañado para ubicarlos en otro que esté habilitado, pero este proceso no se lo puede realizar en un ambiente abierto, ya que cualquier impureza que alcance los platos del disco duro imposibilitará la recuperación de datos, comprometiendo así la evidencia y limitando el proceso de recuperación.

2.5.2 Recuperación Lógica de Información de Discos Duros

Para la recuperación lógica, se utilizan herramientas o aplicativos que salvan la información de discos que han sido supuestamente perdidos, estos aplicativos se instalan y ejecutan en otro lugar para no sobrescribir los datos, este software es usualmente usado por usuarios conocedores en el tema.

Existe una posibilidad mínima de recuperar información que ya fue sobrescrita usando microscopios electrónicos de transmisión de escaneado, sin embargo el acceso a estas herramientas es costoso y no existen muchos ejemplares de estos microscopios.

2.5.2.1 Archivos del Sistema Corrompidos

En algunos casos el disco duro no puede ser leído debido a daños en los archivos del sistema. En la mayoría de casos al menos una porción de la información original puede ser recuperada reparando los archivos del sistema usando software especializado en recuperación de información.

Este tipo de recuperación de información puede ser realizada por usuarios conocedores, ya que no se requiere de equipos especializados, sin embargo dependiendo del caso, esto debe ser tratado por expertos en informática forense.[8]

2.6 TECNICAS FORENSES PARA LA RECONSTRUCCION

Una de las técnicas mas importantes para comprobar la integridad de la información recuperada, es decir, que no ha sido modificada en comparación con la información original y sea una copia exacta de otra es el uso de algoritmos informáticos.

Estos métodos son aplicados por herramientas que se dedican a la informática forense y que son reconocidos a nivel mundial por ejemplo, la herramienta EnCase Forensic utiliza el algoritmo Hash, así como la herramienta Forensic Toolkit usa el algoritmo MD5 y SHA1, y la herramienta de R-Studio usa el algoritmo MD5 en su versión técnica, a continuación se detalla en qué consisten estos algoritmos:

2.6.1 Algoritmo de Hash

Este algoritmo es una función de comprobación de integridad de ficheros, es decir, esta función una vez que se tiene un conjunto de ficheros, le asigna un conjunto de bits, estos bits dependen completamente del contenido de los ficheros, si una parte del fichero varía, el conjunto de bits ya no se será el mismo, este mismo proceso sucede cuando a un mensaje se le aplica el algoritmo de Hash.

[8] DATA RECOVERY: http://en.wikipedia.org/wiki/Data_recovery#cite_note-4

Las aplicaciones más usadas sobre este algoritmo son:

- Integridad de archivos o contenidos.- Si el emisor quiere asegurarse de que al enviar un mensaje al receptor, este no le llegue adulterado, lo que se hace antes de enviar el mensaje es calcular la función Hash, una vez que se ha enviado y ha recibido el receptor, este debe calcular la misma función Hash sobre el archivo y si coinciden los dos resultados, tanto el del emisor como el del receptor, entonces se concluye que el envío ha sido exitoso y el mensaje no ha sido alterado.
- Seguridad de contraseñas.- Para la autenticación de sistemas operativos o acceso a páginas web se requiere de un usuario y contraseña, estos requisitos se almacenan en una base de datos, pero no se almacenan de manera clara sino como producto de la función Hash, con la finalidad de que intrusos no puedan tomar la información ni actuar maliciosamente.[9]

2.6.2 Algoritmo MD5

El algoritmo MD5 (Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits, es la evolución del algoritmo MD4.

Este algoritmo brinda la seguridad de que un archivo descargado del internet no ha sido alterado o modificado. Sobre un archivo bajado de internet se puede comprobar integridad usando una herramienta MD5, contra el MD5 del primer archivo.

"El MD5 también se puede usar para comprobar que los correos electrónicos no han sido alterados usando llaves públicas y privadas".[10]

[9] ALGORITMO DE HASH: http://es.scribd.com/doc/46651/Algoritmos-de-HASH

[10] ALGORITMO MD5: http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=117&Itemid=26

2.6.3 Algoritmo SHA-1 (Secure Hash Algorithm 1 o Algorimo de Hash Seguro 1)

El algoritmo SHA, es una forma de función de Hash, es un algoritmo que tiene 5 funciones de hash, lo que hace que sea un algoritmo de control seguro y están basados en el diseño del algoritmo MD5, pero más robusta.

Los 5 SHA son: SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512, de los cuales el más usado es el SHA-1 que da como resultado 160 bits de un mensaje de hasta 264 bits.

De la misma manera que los algoritmos explicados anteriormente, sirven para comprobar confidencialidad, ya que no pueden existir resultados distintos en los algoritmos, cuando el mensaje tanto de salida como el de entrada son los mismos.

El resultado del algoritmo depende del contenido del mensaje, si el contenido varía también lo hará el resultado del algoritmo.

El resumen de estas funciones son de un solo sentido, lo que significa que de un mensaje original se produce un resultado y de este resultado no se puede obtener el mensaje original.

Estos algoritmos se usan para las firmas digitales, comprobando integridad y solo la persona que tenga la clave del mensaje original podrá leerlo caso contrario no será posible.[11]

2.7 LIMITACIONES DE LA RECUPERACION

Existen aspectos que hacen que la recuperación de la información se vea limitada, estos son:

- Sobrescritura de datos en sectores que estaban ocupados con información.
- Daños físicos, como golpes o caídas que ocasionen la destrucción en el medio de almacenamiento,
- Desmagnetización de medios magnéticos, que se explicó en el *punto 2.4.2*

[11] SECURE HASH ALGORITHM: http://maytics.web44.net/web_documents/secure_hash_algorithm.pdf

CAPITULO III

CASO PRÁCTICO

El presente caso se realiza en base a la metodología propuesta en el capítulo 1 párrafo 1.5, que se aplica con la herramienta y técnicas que cumplen con el objetivo de la recuperación de información considerada como evidencia digital, sin invalidar ni alterar información.

Para realizar la demostración del proyecto, se analizaron varias herramientas, entre estas, la más usada a nivel mundial, EnCase Forensics y Forensic Toolkit, que debido a la restricción de las mismas en cuanto a la obtención de la versión de prueba, se procedió a hacer uso de la herramienta R-Studio, que cumple con los objetivos planteados inicialmente para el proyecto, más adelante se detalla la descripción del entorno de trabajo, sobre el que se lleva a cabo el desarrollo.

3.1 INTRODUCCION A LA PRUEBA DE CONCEPTO

Por su naturaleza la informática forense tiene como objetivo, el analizar evidencias que colaboren a llevar adelante una causa judicial mediante el descubrimiento de información que no fue necesariamente perdida por falla del dispositivo ni por error humano sino por una actividad oculta para borrar, adulterar u ocultar datos, el presente caso se basa en un supuesto delito en el cual se tiene bajo poder el equipo contenedor de la posible evidencia, al mismo que se debe realizar el proceso de análisis forense para demostrar la recuperación de la evidencia; y en conjunto con el detalle del visor de sucesos del equipo, tratar de identificar y esclarecer quien fue el causante y cuando aconteció el delito.

3.2 DESCRIPCION DEL ENTORNO DE TRABAJO

La empresa XYZ, tiene aproximadamente 100 empleados, los mismos que almacenan su información de manera local y adicionalmente existe la política de que la información más importante para la empresa, se almacene en

carpetas públicas, ya que esta información se direccionará hacia un servidor de archivos.

Este servidor tiene la función de respaldar información de todos los usuarios de la empresa, eso explica su alta importancia, pues de existir algún tipo de contratiempo que provoque su mal funcionamiento o el acceso de personas no deseadas al equipo con malas intenciones sobre la información, podría causar grandes pérdidas a la empresa.

Para el desarrollo del proyecto se tiene el siguiente caso; el administrador del servidor de archivos, no aplicó las políticas y seguridades respectivas al servidor de manera que alguna persona desconocida accedió al equipo y eliminó información importante para la empresa.

El objetivo del desarrollo del proyecto como primer plano es demostrar la recuperación de datos que estaban alojados en el servidor, para realizar esta acción se utilizará la herramienta R-Studio, que tiene como funcionalidad la reconstrucción de información a pesar de que esta haya sido eliminada, realizando configuraciones y usando filtros propios de la utilidad para llevar a cabo el objetivo de reconstrucción de la evidencia; y en segundo plano realizar un análisis forense sobre el caso con ayuda de las herramientas del propio sistema operativo para conocer qué persona fue la que accedió el archivo o desde qué equipo se tuvo acceso por última vez y en base a investigaciones poder aplicar la sanción penal correspondiente al culpable.

3.3 JUSTIFICACION DEL USO DE LA HERRAMIENTA R-STUDIO

La herramienta R-Studio es apta para aplicarla en análisis forenses ya que para la recuperación de información aplica al algoritmo MD5, y con esto se asegura que la información no haya sido alterada; Puede crear adicionalmente archivos de imagen, tal como pide la que se haga en el proceso de análisis forense en el Capítulo I, la Organización Internacional de Evidencias en Computadora (IOCE), ó la Recuperación a través de Red, entre estas bondades existen otras que serán explicadas a continuación y que son el justificativo del porqué del uso de la herramienta para el análisis forense.

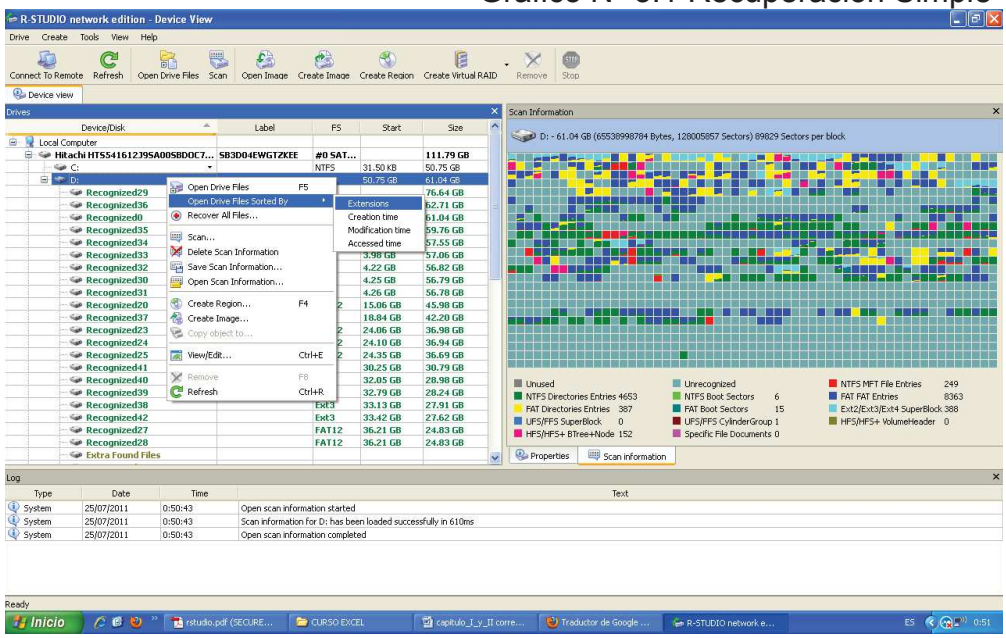
3.4 GENERALIDADES DE LA HERRAMIENTA R-STUDIO

R-Studio es una herramienta poderosa en restablecimiento y recuperación de datos. Dotado con nuevas tecnologías únicas de recuperación de datos, para poder rescatar archivos de FAT12/16/32, NTFS, NTFS5 (creados o actualizados por Windows 2000/XP/2003/ Vista/Windows 7), y particiones Ext2/Ext3/Ext4 FS (Linux). Funciona en discos locales y de red, aun si tales particiones están formateadas, dañadas, o han sido eliminadas. Los ajustes flexibles de parámetros le dan control absoluto en la recuperación de datos.

La herramienta brinda principalmente las siguientes bondades:

- Recuperación Simple.- La recuperación simple puede ser de archivos eliminados que residen en el disco lógico visible al sistema operativo.

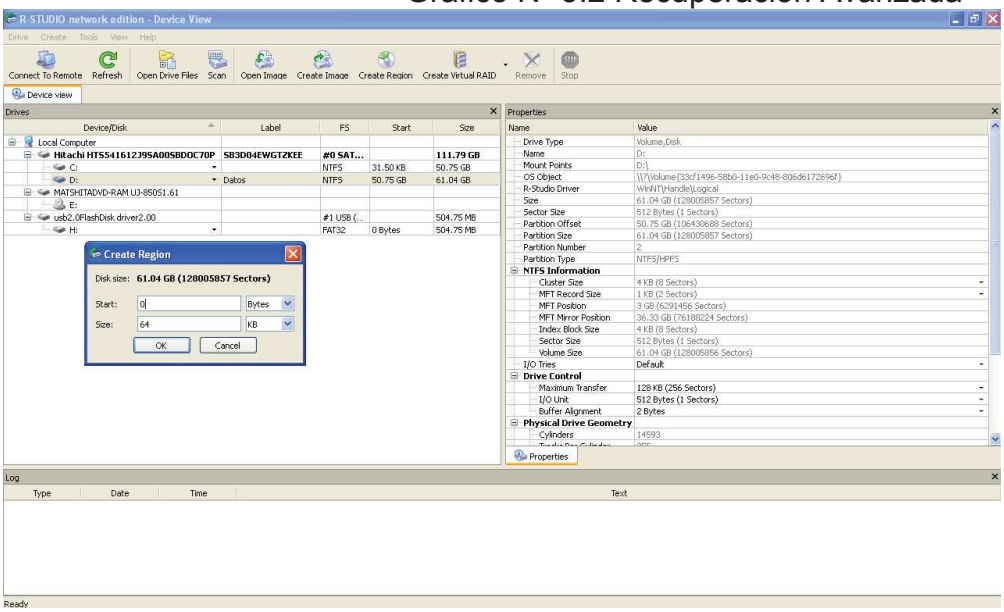
Gráfico Nº 3.1 Recuperación Simple



Autora: Andrea Medrano

- Recuperación Avanzada.- Esta recuperación es minuciosa, ya que analiza la estructura del objeto, puede escanear regiones específicas en el disco creadas por el usuario;

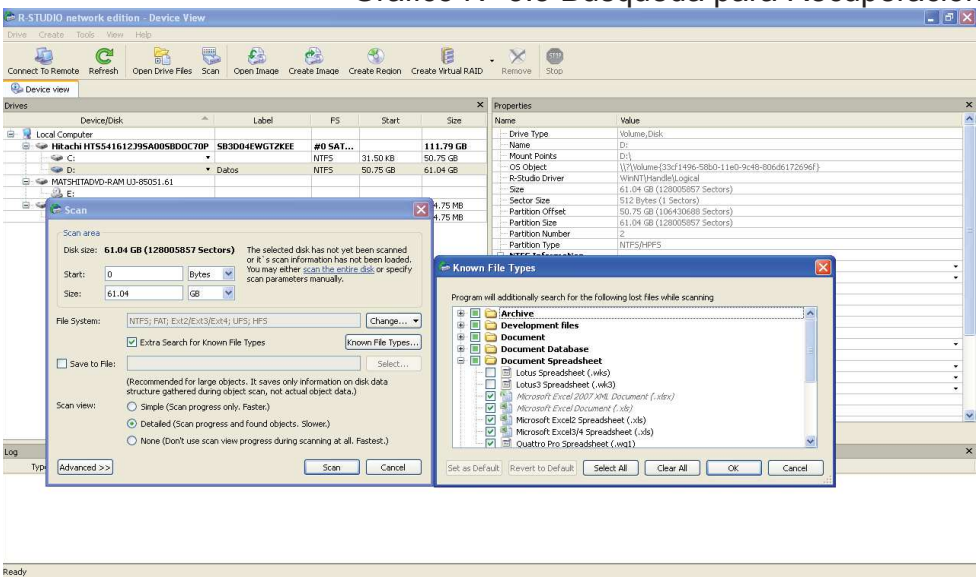
Gráfico Nº 3.2 Recuperación Avanzada



Autora: Andrea Medrano

Y, adicionalmente permite hacer búsqueda según criterios, como por ejemplo según extensiones de archivos.

Gráfico Nº 3.3 Búsqueda para Recuperación

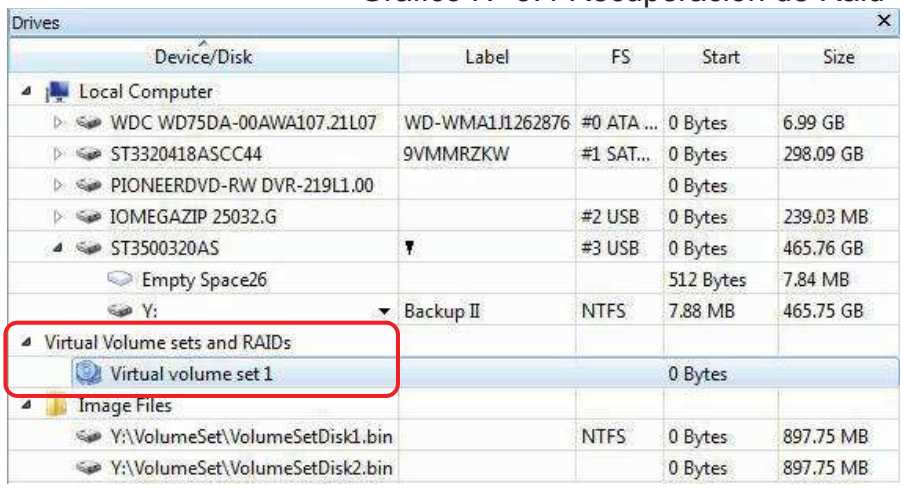


Autora: Andrea Medrano

- Recuperación de RAID.- La herramienta detecta y procesa volúmenes configurados como RAIDs, los mismos que pueden ser analizados y

recuperados. Cada volumen del RAID es reconocido como un volumen distinto y se puede trabajar como con cualquier otro dispositivo.

Gráfico Nº 3.4 Recuperación de Raid

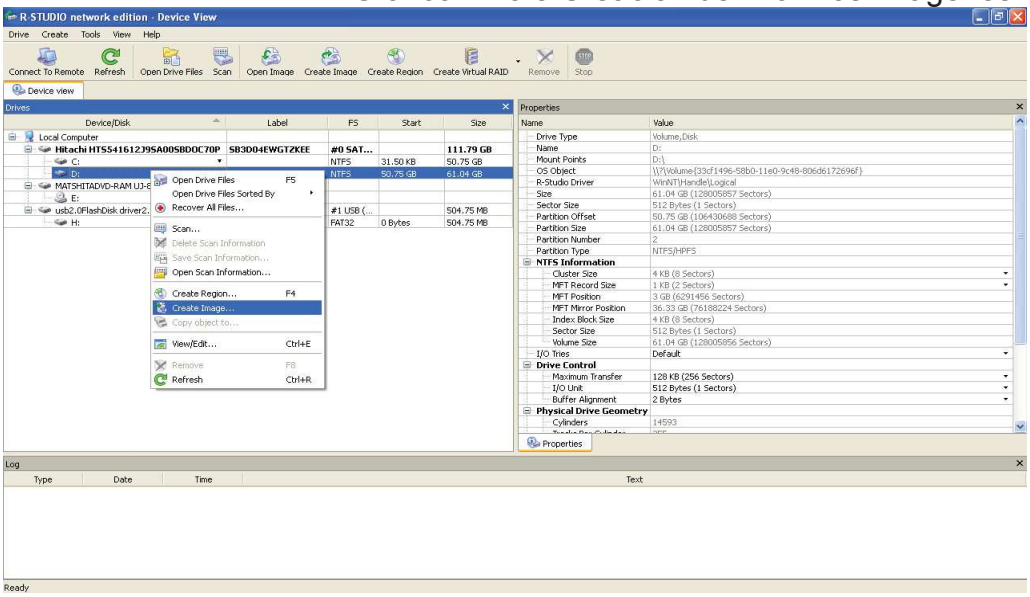


Autora: Andrea Medrano

- Creación de Archivos de Imagen.- Una imagen es una copia exacta de un volumen, cuando se crea una imagen se trabaja de la misma manera que con cualquier dispositivo.

  Las imágenes tienen como ventaja el no alterar la evidencia original por cualquier tipo de suceso que llegara a ocurrir.

Gráfico Nº 3.5 Creación de Archivos Imágenes



Autora: Andrea Medrano

- Recuperación a través de la Red.- Es la recuperación de información a través de cualquier otro equipo que sea parte del dominio de la máquina afectada, siempre y cuando tenga permisos de administrador.
  Para esta característica se debe instalar R-Studio Agent.

3.5 IMPLEMENTACIÓN DE LA HERRAMIENTA

R-Studio, es una herramienta de propiedad de R-Tools Technology Inc., quien es el proveedor principal de utilidades poderosas para la recuperación de datos, restablecimiento, imágenes de disco y seguridad de datos para la familia del sistema operativo de Windows.

Para adquirir estas aplicaciones en conjunto con sus respectivos manuales se puede realizar mediante compra en línea desde su sitio web www.r-tt.com.

R-Studio permite la recuperación de archivos:

- Que han sido retirados sin la Papelera de reciclaje, o cuando la Papelera de Reciclaje se ha vaciado,
- Eliminados por ataque de virus o falla de energía,
- Después de que la partición con los archivos fue formateado, incluso para un sistema de archivos diferente,
- Cuando la estructura de particiones en un disco duro ha sido cambiada o dañada. En este caso, R-Studio pueden escanear el dispositivo tratando de encontrar particiones previamente existentes y recuperar los archivos de las particiones encontradas.
- De discos con sectores defectuosos. En este caso, R-Studio puede copiar primero el disco entero o parte en un archivo de imagen y luego procesar dicho archivo de imagen.

3.5.1 Requerimientos del sistema

- Procesador Intel compatible con plataformas que corran sistemas operativos Windows 9x/ME/NT4.0/2000/XP/2003/Vista/7.
- Por lo menos 32 MB de RAM, un mouse, y suficiente espacio en disco para recuperar archivos, imágenes, etc.

- Privilegios de Administrador son requeridos para instalar R-Studio utilities bajo Windows NT/2000/XP/2003/Vista/2008/7.
- Conexión de red para recuperación de datos sobre la red.

3.5.2 Instalación de la herramienta

Antes de iniciar con el proceso de instalación se debe tener en cuenta que los datos buscados se encontraban en la unidad de disco “D:”, con la finalidad de que la herramienta no se ubique en una unidad distinta.

La versión de instalación es R-Studio 5.1, al dar doble clic sobre el ícono del instalador,

Gráfico Nº 3.6 Icono de Instalación

Autora: Andrea Medrano

Aparece una ventana que indica el inicio de la instalación, presionar siguiente.

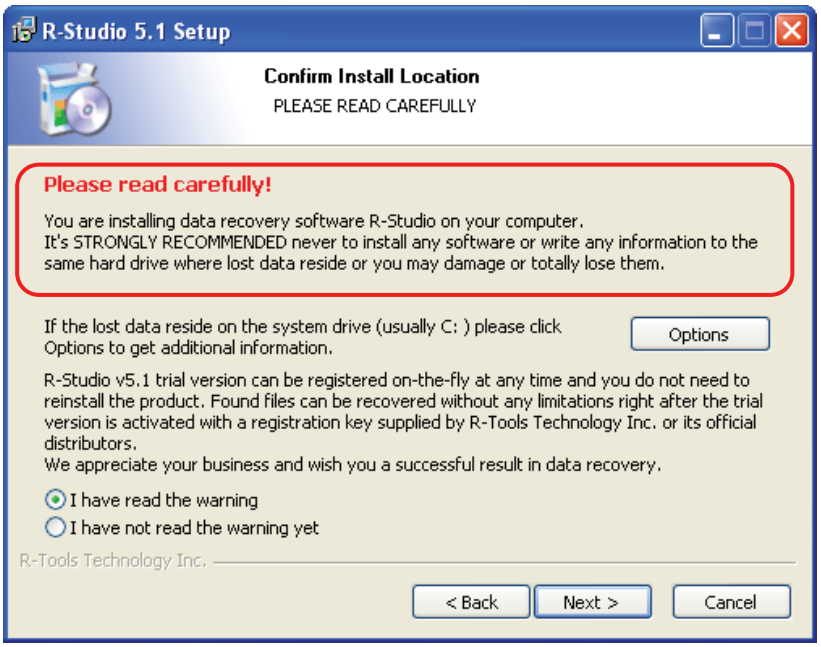
Gráfico Nº 3.7 Ventana de Inicio

Autora: Andrea Medrano

La siguiente ventana solicita que, se instale la herramienta en un lugar que no afecte al espacio del disco sobre el que se pretende recuperar la información,

puede ser otro dispositivo de almacenamiento o una partición del disco distinta a la que contiene los datos que nos interesan, presionar sobre la confirmación de haber leído la alerta y presionar siguiente.

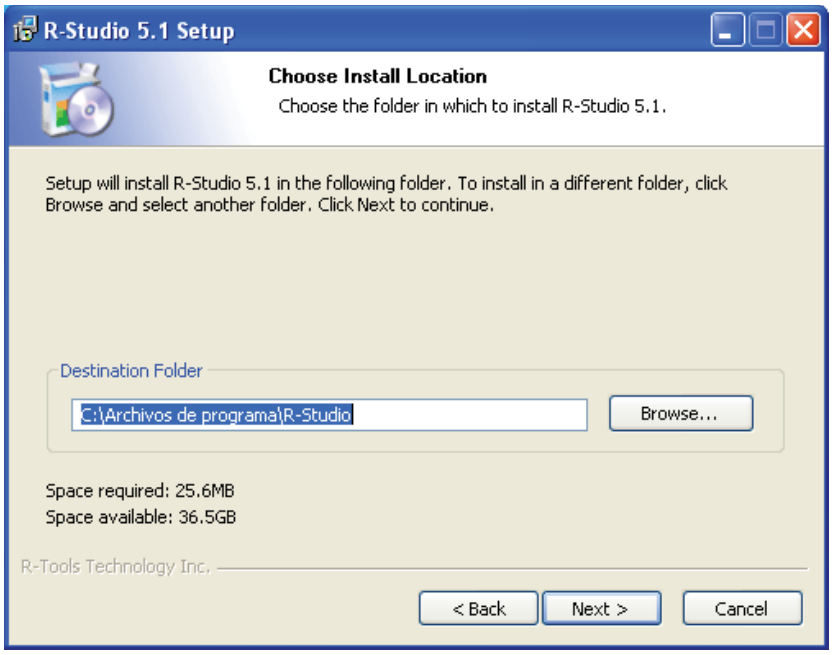
Gráfico Nº 3.8 Advertencia de Instalación



Autora: Andrea Medrano

Elegir la ruta específica en la que se va a instalar la herramienta, para este caso lo instalaremos en la unidad “C:” y así no modificar a la unidad “D:”. Verificar si existe espacio físico suficiente para poder operar correctamente, y presionar siguiente.

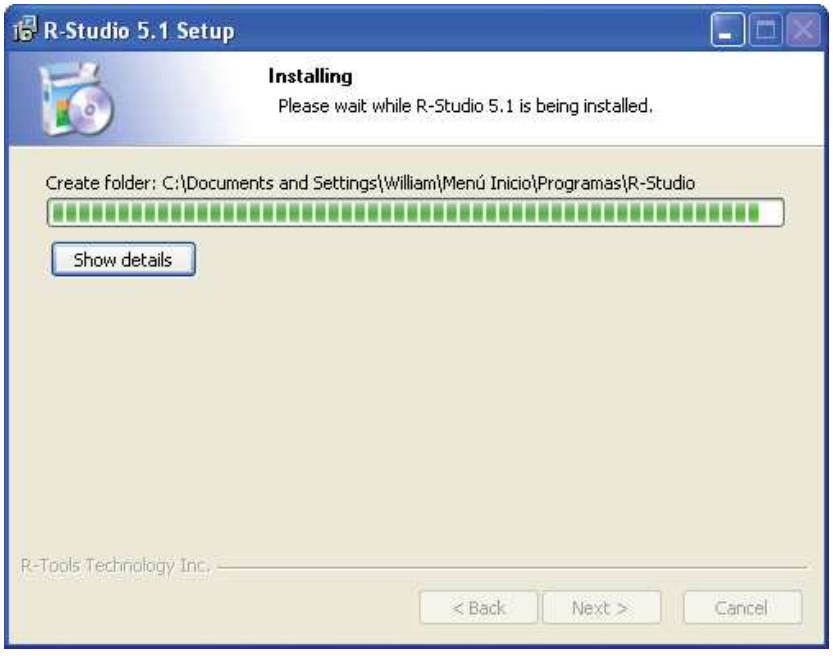
Gráfico Nº 3.9 Ruta de Instalación



Autora: Andrea Medrano

Seguido de esto se observa el proceso de instalación, si no existieron problemas anteriores una ventana similar a la que se presenta debe aparecer.

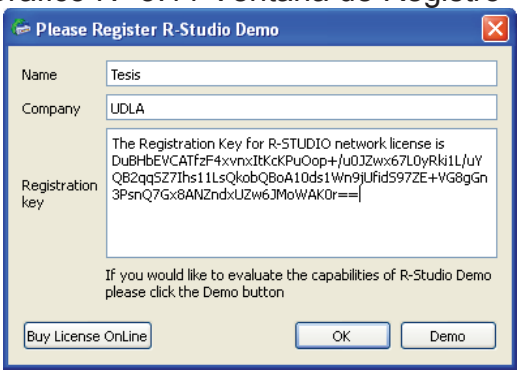
Gráfico Nº 3.10 Proceso de Instalación



Autora: Andrea Medrano

Para terminar se debe ingresar la clave de registro y el resto de credenciales, si está correcto la ventana de registro exitoso debe aparecer.

Gráfico Nº 3.11 Ventana de Registro



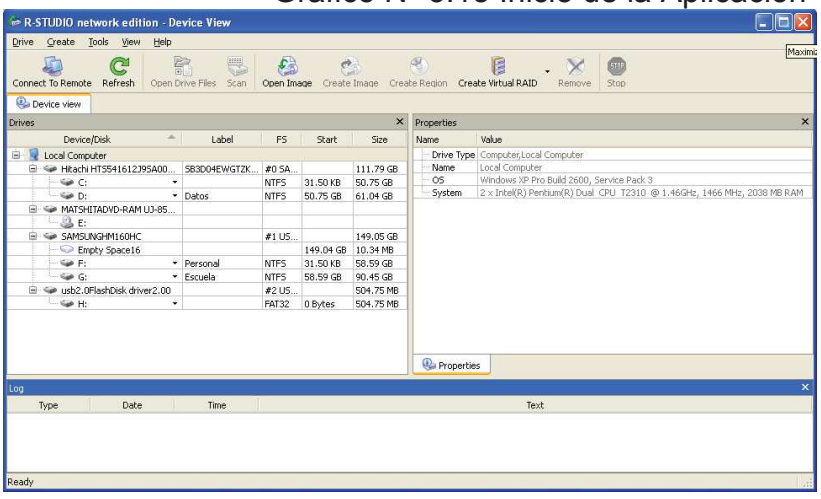
Autora: Andrea Medrano

Gráfico Nº 3.12 Registro Exitoso

Autora: Andrea Medrano

Finalmente se despliega la venta de inicio de R-Studio, en la que ya se puede continuar trabajando.

Gráfico Nº 3.13 Inicio de la Aplicación



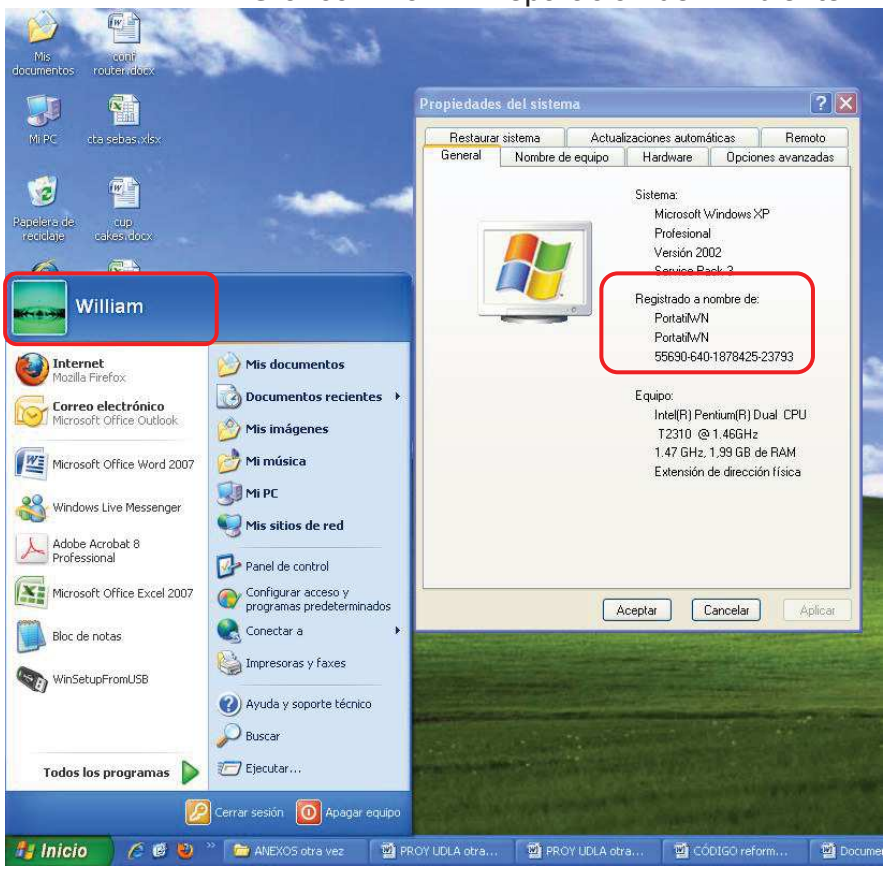
Autora: Andrea Medrano

3.6 PREPARACION DEL AMBIENTE DE PRUEBAS

Después de la implementación y para tener claro el panorama, las siguientes pantallas muestran los archivos que el equipo tiene inicialmente como evidencia y que alguna persona por motivos desconocidos eliminó algunos de estos.

El objetivo del ejercicio es representar que existen archivos en un principio y después de eliminarlos conscientemente; la herramienta con configuraciones personalizadas debe reconstruir la evidencia sin afectarla.
El ambiente se desarrolla en el equipo registrado a nombre de “PortatilWN” y con el usuario “William”, que es necesario especificarlo en este momento para la demostración a futuro de la recuperación de la información y conocer el usuario que interactuó por última vez con los archivos eliminados.

Gráfico Nº 3.14 Preparación del Ambiente 1

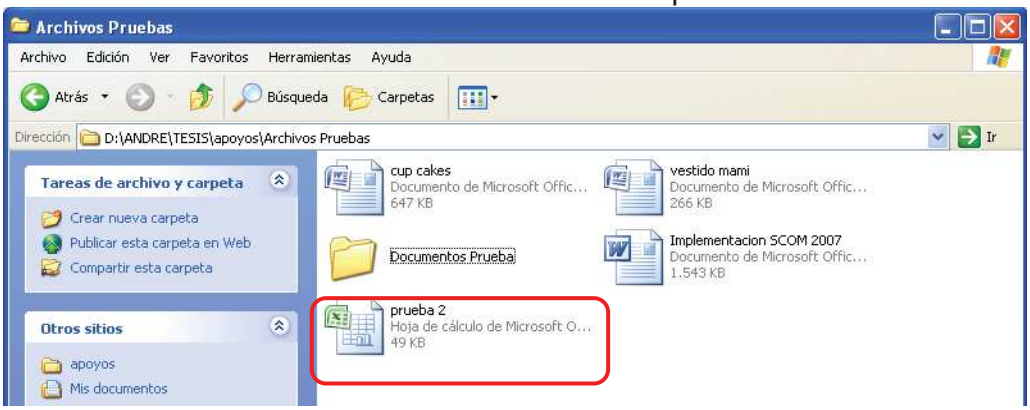


Autora: Andrea Medrano

Los archivos que interesan recuperarse se encuentran en la ruta 'D:\ANDRE\TESIS\apoyos\Archivos Pruebas', así:

- prueba2.xls

Gráfico Nº 3.15 Preparación del Ambiente 2

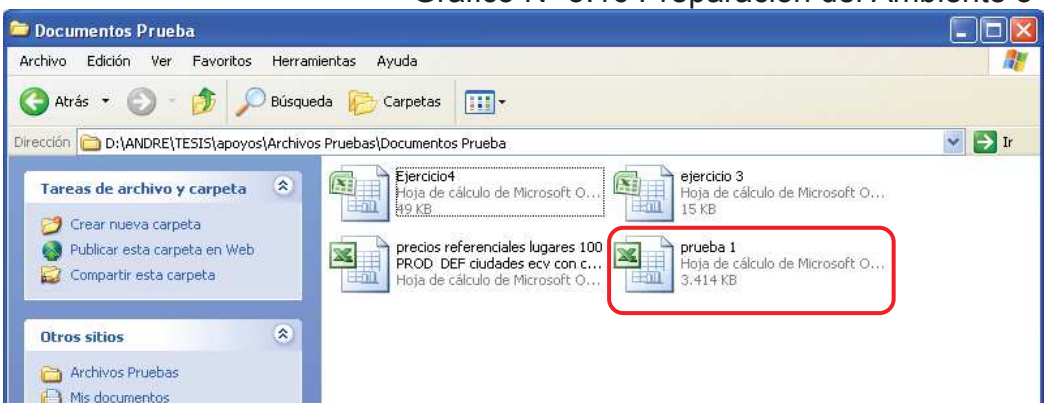


Autora: Andrea Medrano

Y, en el directorio 'D:\ANDRE\TESIS\apoyos\ArchivosPruebas\Documentos Prueba', se encuentra el archivo:

- prueba 1.xls

Gráfico Nº 3.16 Preparación del Ambiente 3



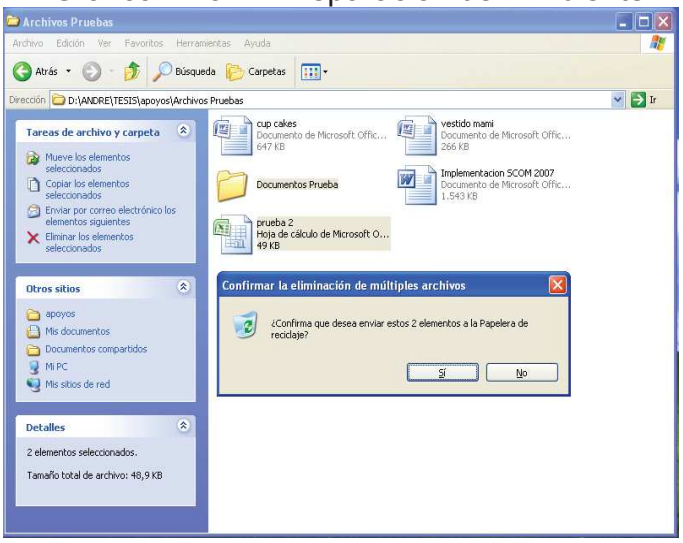
Autora: Andrea Medrano

Sin embargo para el ejemplo, se eliminan:

- El archivo prueba 1.xls, y
- El directorio Documentos Tesis

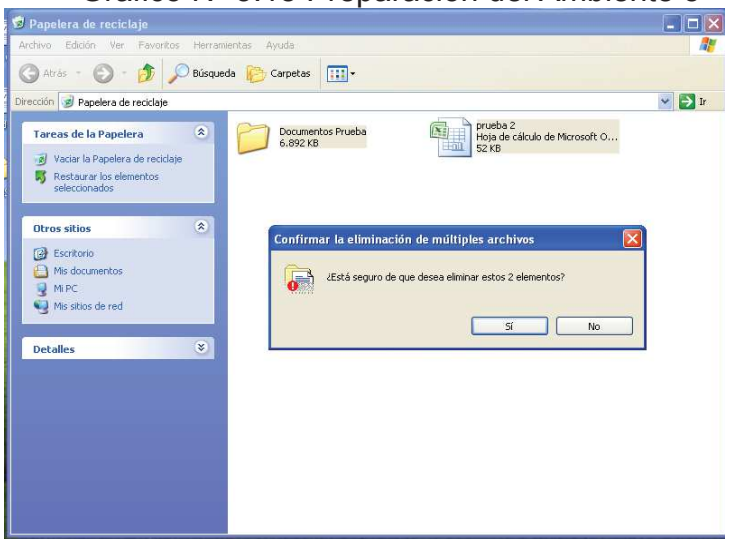
Tanto de la carpeta Archivos Prueba y de la papelera de reciclaje.

Gráfico Nº 3.17 Preparación del Ambiente 4



Autora: Andrea Medrano

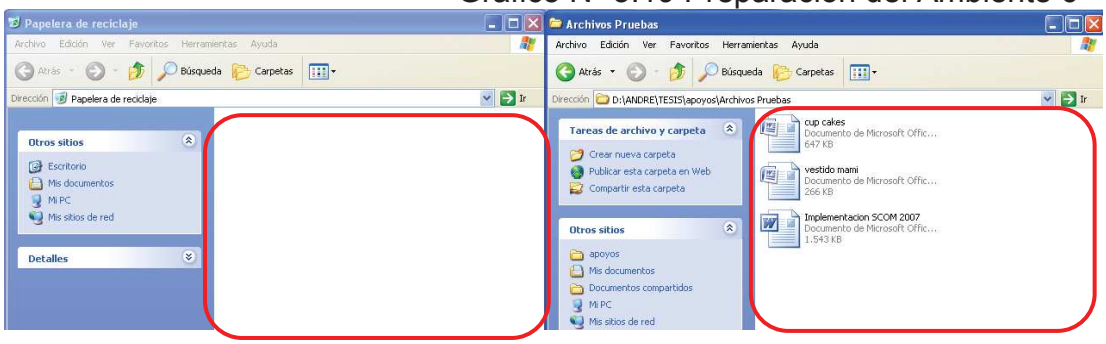
Gráfico Nº 3.18 Preparación del Ambiente 5



Autora: Andrea Medrano

De manera que la papelera de reciclaje y el directorio ‘D:\ANDRE\TESIS\apoyos\ArchivosPruebas’ queda así;

Gráfico Nº 3.19 Preparación del Ambiente 6



Autora: Andrea Medrano

3.7 DEMOSTRACION DE LA RECUPERACION

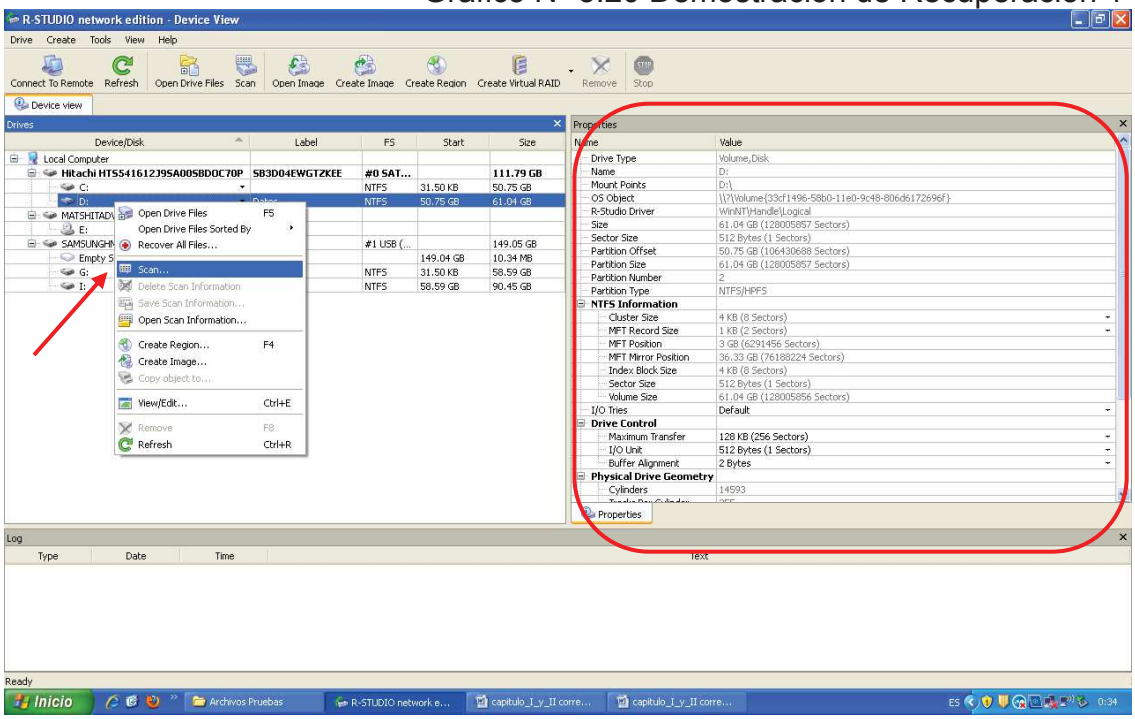
Para realizar la recuperación se lo realiza en base a la metodología al apartado de la Recuperación de Datos que recomienda no alterar la información de manera que ésta no sea invalidada.

Partiendo de lo anterior como situación actual, se procede a realizar el escaneo de la información en la unidad D: con la herramienta R-Studio para la reconstrucción, de la siguiente manera:

En la ventana principal aparecen todas las unidades de disco existentes en el equipo, al ubicarse en cada unidad de disco al lado derecho de la pantalla se muestran sus respectivas propiedades.

Recordando que la información requerida se encuentra inmersa en la unidad D:, se debe dar clic derecho sobre la unidad y entre las propiedades que aparecen en la ventana, seleccionar la opción de escaneo Scan.

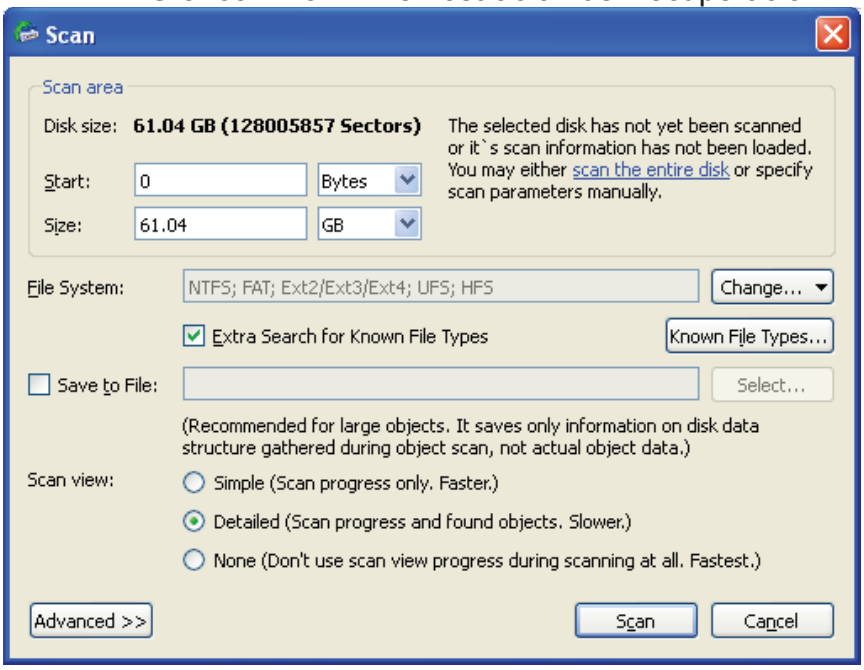
Gráfico Nº 3.20 Demostración de Recuperación 1



Autora: Andrea Medrano

Una vez seleccionada la opción de escaneo, se despliega una ventana que indica sobre qué sectores se desea hacer la búsqueda, como no se conoce entre que sectores estaba la información, se debe dejar que se haga el escaneo sobre todo el disco duro y en el tipo de vista de escaneo, seleccionar la vista detallada para conocer los objetos que se van encontrando.

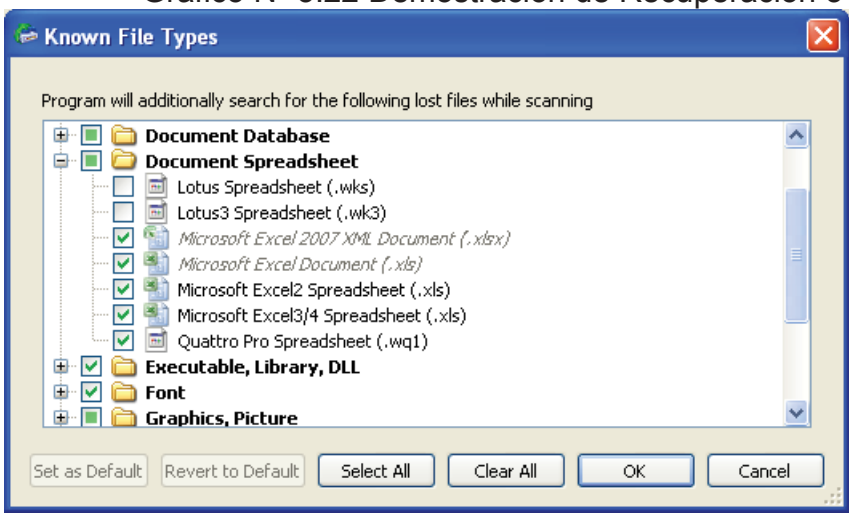
Gráfico Nº 3.21 Demostración de Recuperación 2



Autora: Andrea Medrano

El tipo de recuperación se puede filtrar según criterios que brinda la misma herramienta, para este caso el filtro de búsqueda se realizará por extensiones en el tipo de archivos conocidos, esto depende de las necesidades que presente el caso.

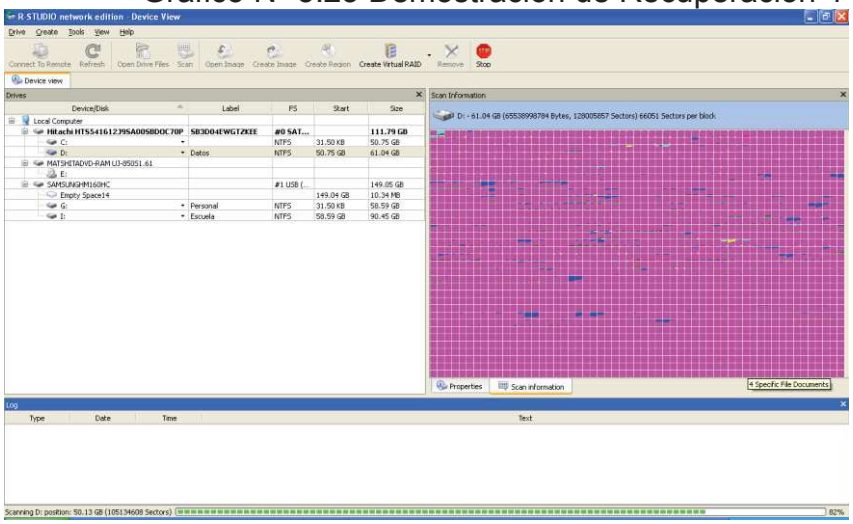
Gráfico Nº 3.22 Demostración de Recuperación 3



Autora: Andrea Medrano

Durante el proceso de escaneo se presenta una ventana similar a la que se muestra a continuación:

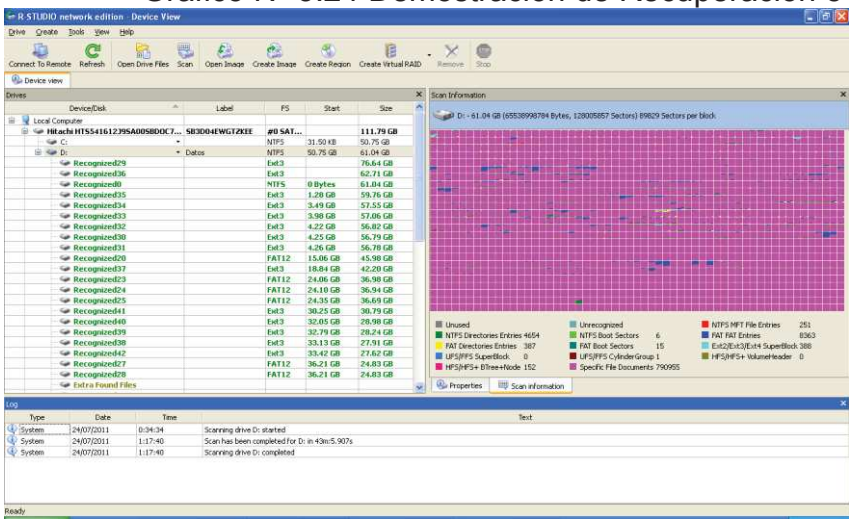
Gráfico Nº 3.23 Demostración de Recuperación 4



Autora: Andrea Medrano

Cuando la búsqueda se termina, la herramienta muestra el detalle de la información encontrada y agrupada por carpetas, las mismas que deben ser analizadas una a una para conocer en qué lugar se encuentran los datos relacionados con el caso.

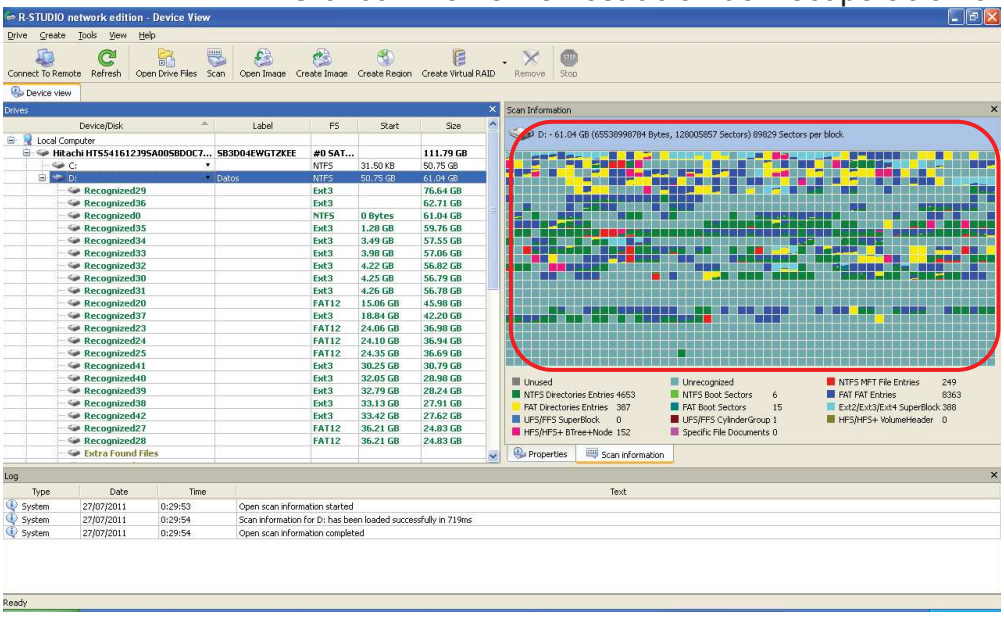
Gráfico Nº 3.24 Demostración de Recuperación 5



Autora: Andrea Medrano

La venta muestra al lado derecho el panel de información escaneada por sectores que se representan por cuadros pequeños de colores.

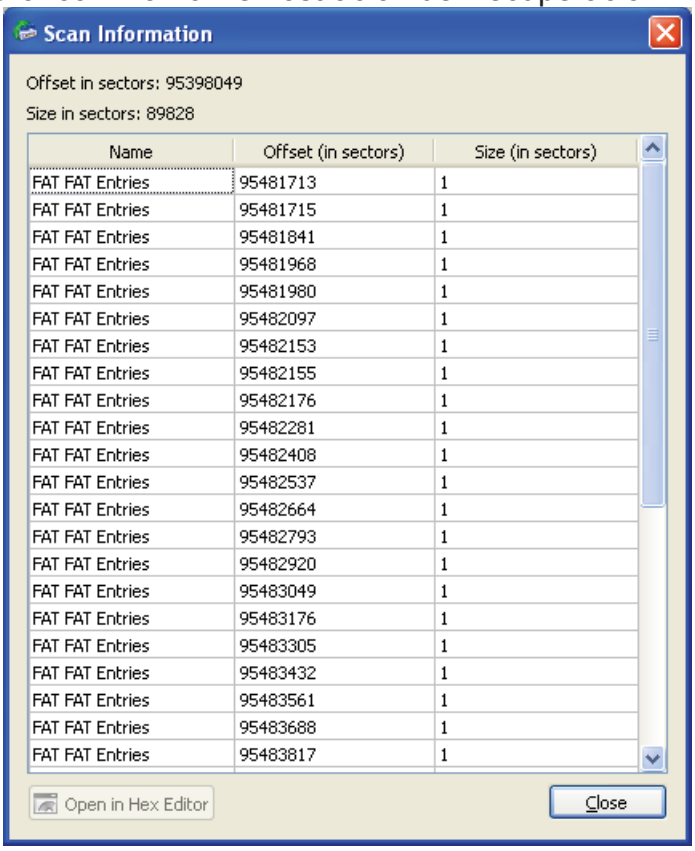
Gráfico Nº 3.25 Demostración de Recuperación 6



Autora: Andrea Medrano

Al ingresar a cada uno de los sectores, se despliega una ventana que describe la información que contiene ese sector, así:

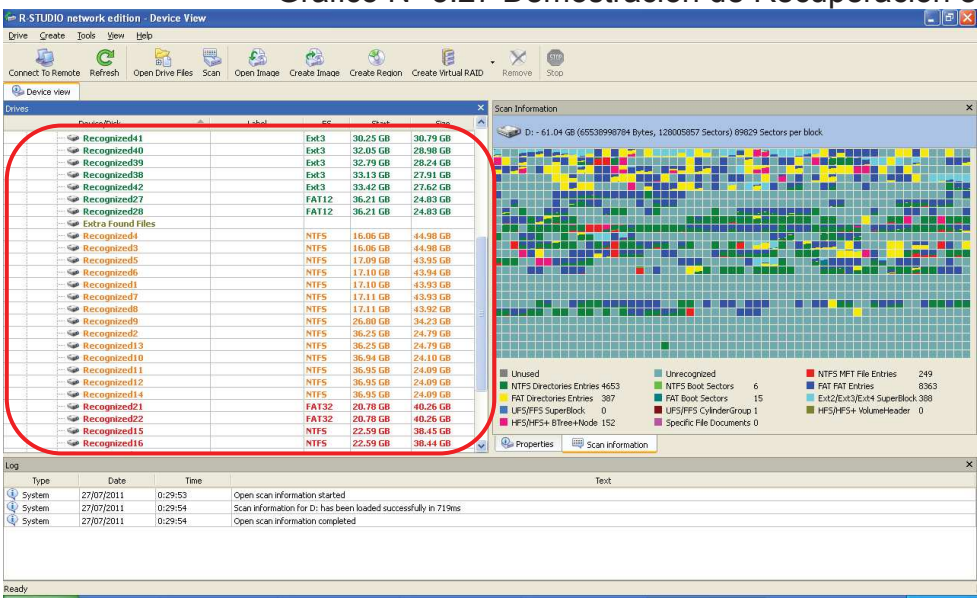
Gráfico Nº 3.26 Demostración de Recuperación 7



Autora: Andrea Medrano

En el lado izquierdo de la ventana, en el panel de dispositivos, la información encontrada se presenta agrupada en carpetas de diferentes colores dependiendo del tipo de archivo que se ha encontrado, la descripción se detalla a continuación:

Gráfico Nº 3.27 Demostración de Recuperación 8



Autora: Andrea Medrano

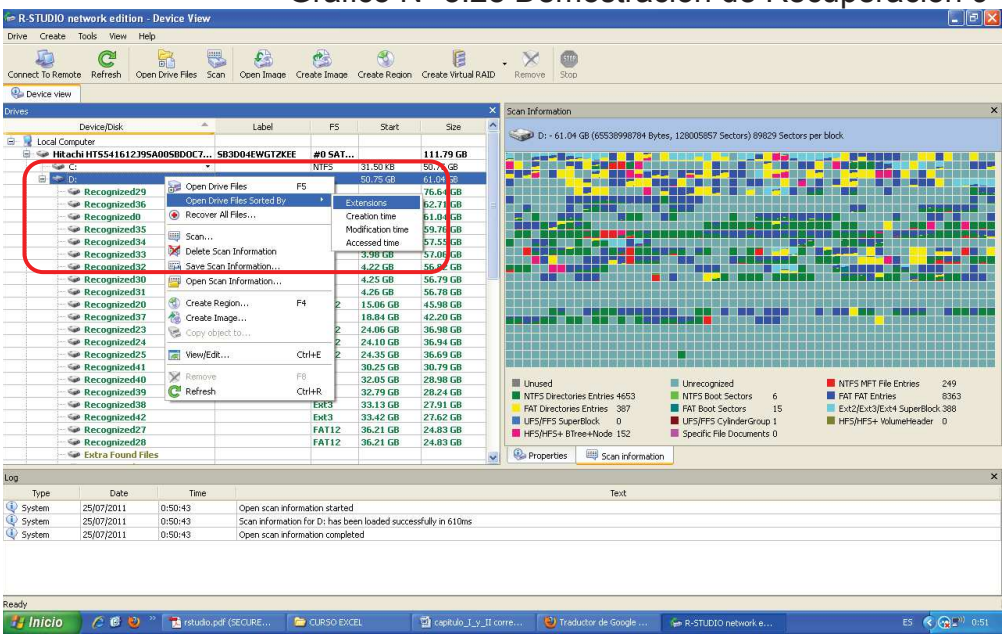
Cuadro Nº 3.1 Recuperación por Colores

Recognized1	Solo archivos de entrada que se han encontrado para esta partición
Recognized2	Registros de arranque y archivos de entrada que se han encontrado para esta partición
Recognized3	Solo Registros de arranque que se han encontrado para esta partición
Extra Found Files	Archivos que se han encontrado en la búsqueda según un tipo de archivo desconocido.

Autora: Andrea Medrano

Un criterio de filtrar los archivos encontrados, es ordenar los documentos por extensiones, para aplicar el filtro se debe dar clic derecho sobre la partición escaneada y ordenar por extensión.

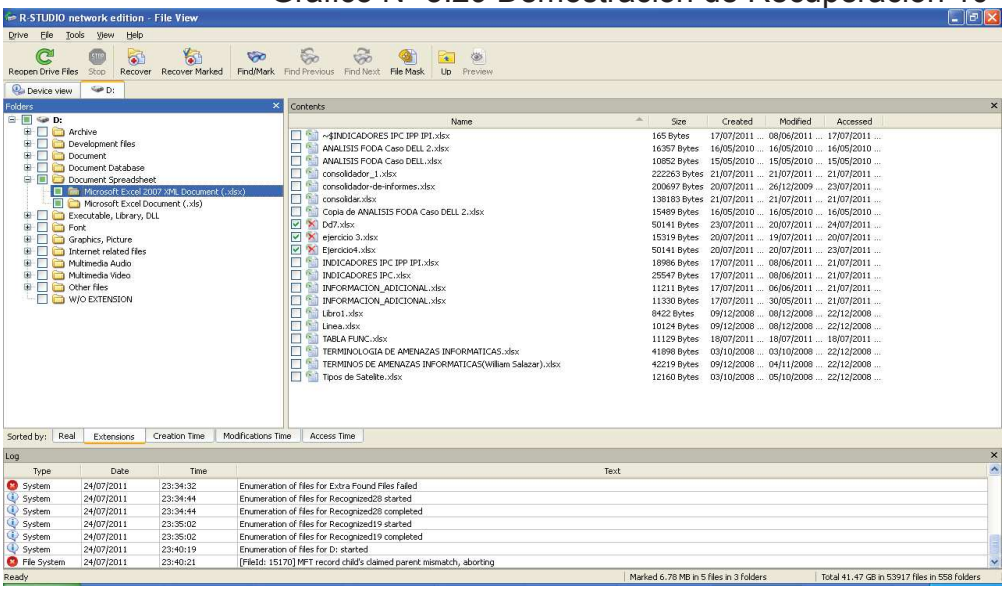
Gráfico Nº 3.28 Demostración de Recuperación 9



Autora: Andrea Medrano

Según el criterio de filtrado, la herramienta despliega una ventana que tiene el resultado de la búsqueda. En este momento se empieza a hacer el análisis sobre todos los registros recuperados, dependiendo del caso se debe ir marcando los archivos que puedan apuntar a ser una evidencia digital, es decir que, posiblemente contengan información que se relacione con el delito.

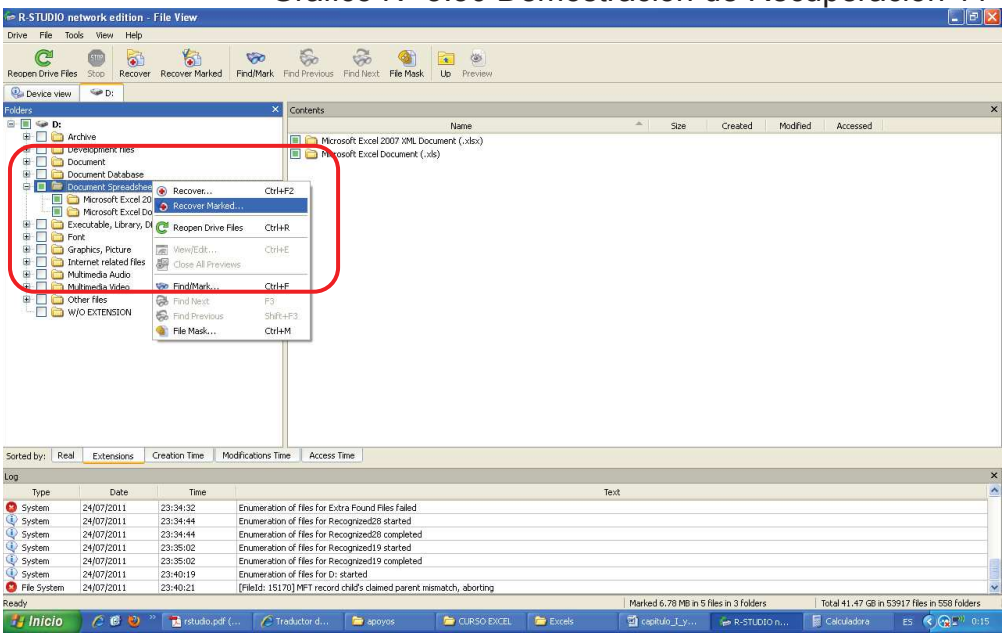
Gráfico Nº 3.29 Demostración de Recuperación 10



Autora: Andrea Medrano

Una vez seleccionados los archivos, dar clic derecho y escoger la opción “Recuperar Marcados”

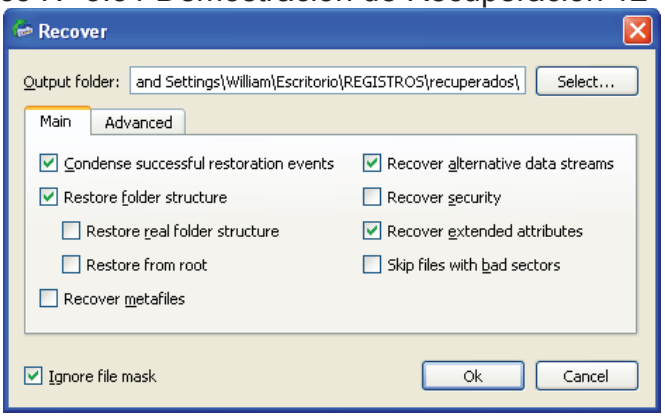
Gráfico Nº 3.30 Demostración de Recuperación 11



Autora: Andrea Medrano

La herramienta arroja una ventana que, solicita se escoja la ruta en donde se va a guardar la información recuperada, se debe tener en cuenta que por seguridad y para no alterar la evidencia esta recuperación se almacena en otra partición u otro dispositivo de almacenamiento.

Gráfico Nº 3.31 Demostración de Recuperación 12

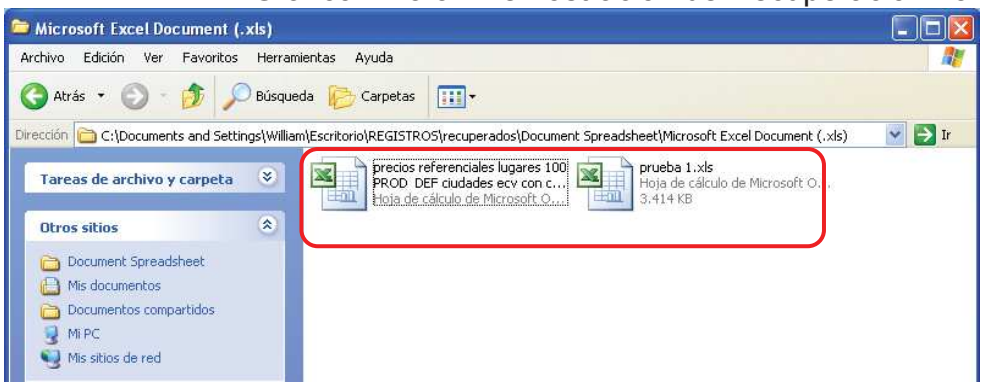


Autora: Andrea Medrano

Finalmente se puede apreciar los archivos que aparentemente estaban eliminados y que ahora sirven de evidencia para poder apoyar a la resolución de delitos.

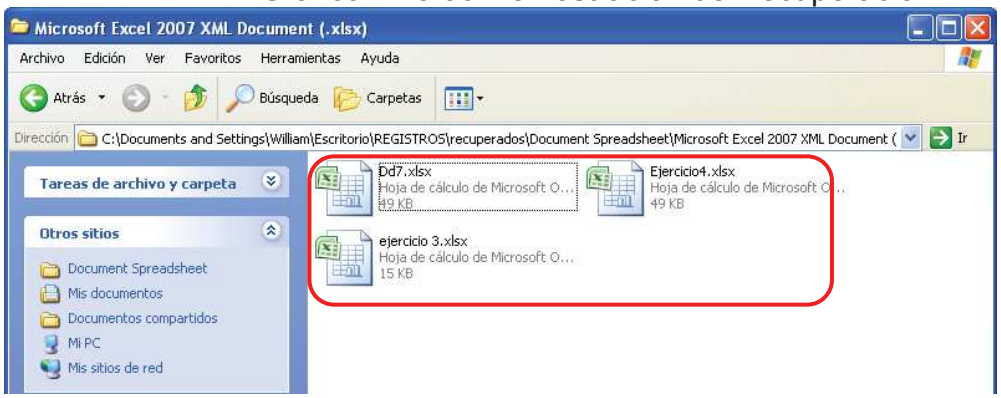
Como resultado tenemos los archivos recuperados que al inicio del capítulo se eliminaron para poder realizar la práctica.

Gráfico Nº 3.32 Demostración de Recuperación 13



Autora: Andrea Medrano

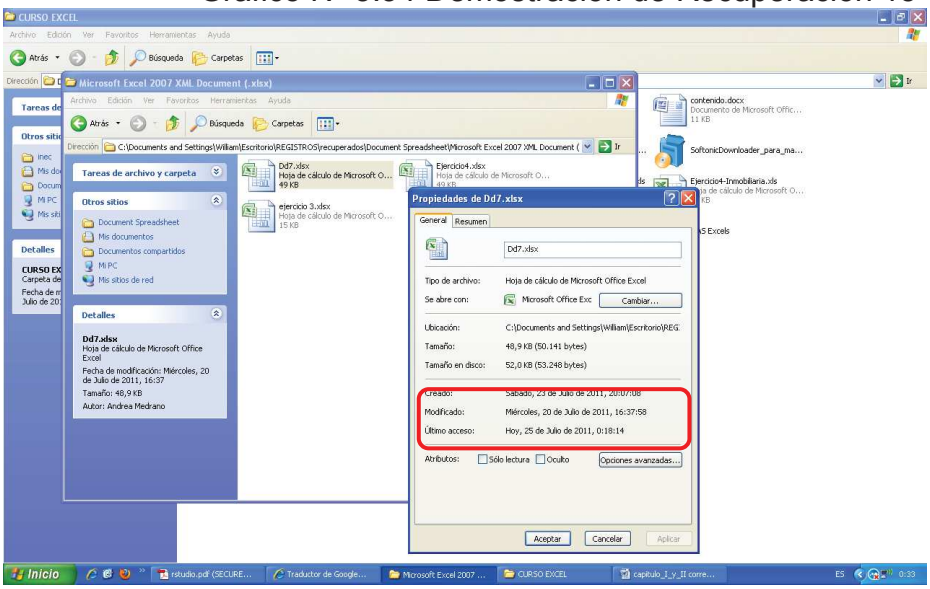
Gráfico Nº 3.33 Demostración de Recuperación 14



Autora: Andrea Medrano

Para asegurarse de que los archivos recuperados son los mismos que se buscaban, se puede verificar las propiedades del archivo y analizar cuando fue creado, cuándo fue modificado y cuál fue su último acceso.

Gráfico Nº 3.34 Demostración de Recuperación 15



Autora: Andrea Medrano

CAPITULO IV

ANÁLISIS Y DETECCION DE RESULTADOS

4.1 ANÁLISIS DE LA EVIDENCIA

Cumpliendo con la metodología en la etapa de Presentación y con el Proceso de Análisis Forense en cuanto al Análisis, Interpretación y Atribución, en este apartado se realiza los pasos propuestos, es decir, analizar las propiedades de los archivos recuperados, en conjunto con los registros del sistema operativo para conocer los eventos y los usuarios que modificaron o tuvieron actividad sobre el equipo, sobre los archivos, y demás acciones de Microsoft Office que se produjeron.

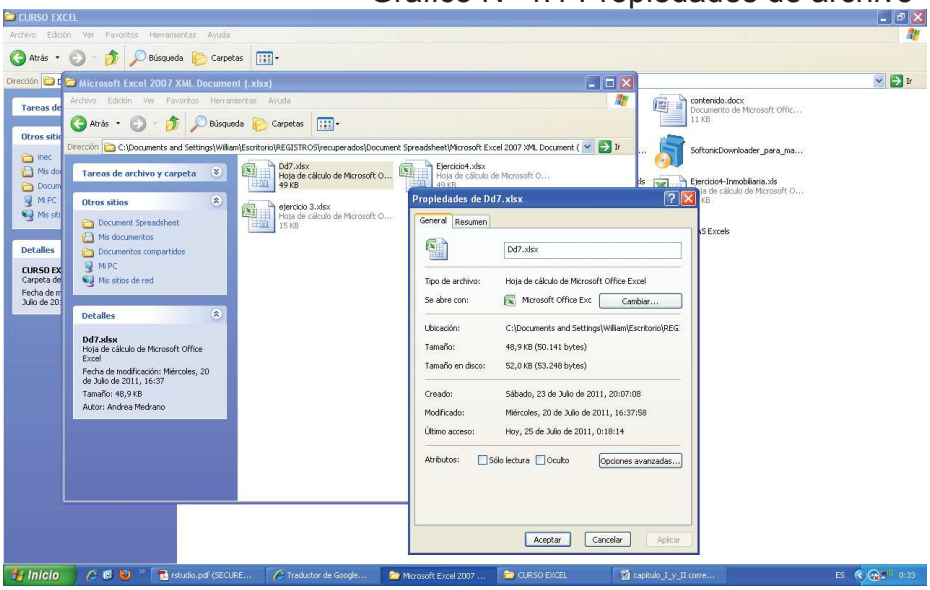
4.1.1 Propiedades del Archivo

Según el reporte de las propiedades del archivo recuperado, se observa que existen eventos en las siguientes fechas:

- Fecha de creación: Sábado, 23 de Julio de 2011
- Fecha de Modificación: Miércoles, 20 de Julio de 2011
- Fecha de Último Acceso: Lunes, 25 de Julio de 2011

Lo que significa que el archivo tuvo algún tipo de actividad el Sábado, 23 de Julio de 2011.

Gráfico Nº 4.1 Propiedades de archivo



Autora: Andrea Medrano

Estas características ayudan a descartar rangos de tiempo y especificar cuándo se cometió el delito.

4.1.2 Visor de Sucesos

Otro método que es de vital importancia para el análisis de un caso son los registros que guarda el equipo, estos eventos se guardan en tres registros:

a) Registro de aplicación

El registro de aplicación contiene eventos registrados por los programas. Por ejemplo, un programa de base de datos puede grabar un error de archivo en el registro de aplicación. Los desarrolladores del programa de software determinan los eventos que se escriben en el registro de aplicación.

b) Registro de seguridad

El registro de seguridad graba eventos como intentos válidos y no válidos de inicio de sesión, así como eventos relacionados con el uso de recursos como crear, abrir o eliminar archivos. Por ejemplo, cuando la auditoría del inicio de sesión está habilitada, se graba un evento en el registro de seguridad cada vez que un usuario intenta iniciar sesión en el equipo. Debe haber iniciado sesión como Administrador o como miembro del grupo Administradores para poder

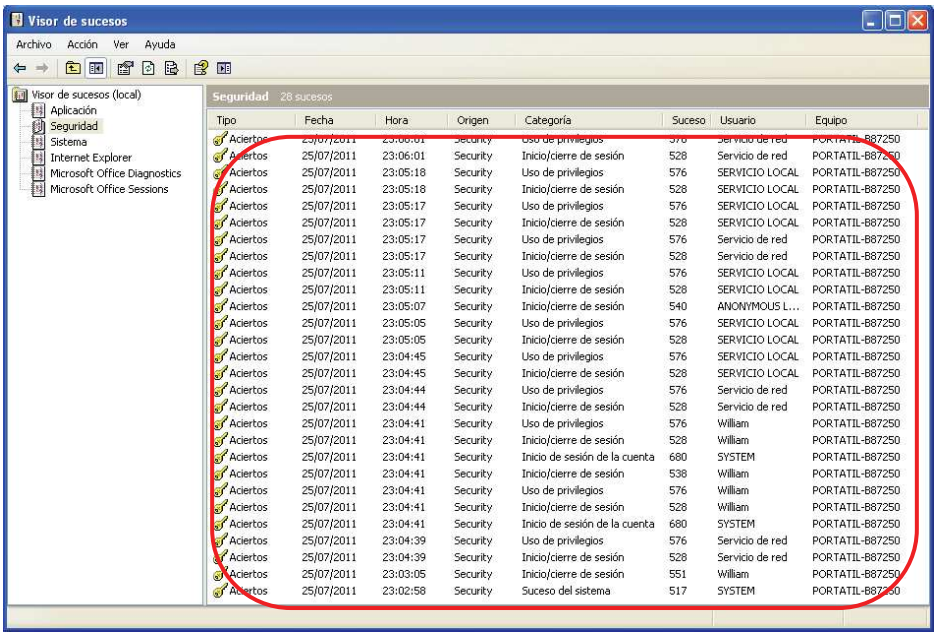
activar, utilizar y especificar qué eventos se grabarán en el registro de seguridad.

c) Registro del sistema

El registro del sistema contiene eventos grabados por los componentes del sistema de Windows XP. Por ejemplo, si un controlador no se carga durante el inicio, se grabará un evento en el registro del sistema. Windows XP determina previamente los eventos registrados por los componentes del sistema. [12]

En el registro de seguridad se aprecian las fechas en que se inició sesión en el equipo, pero tienen un tiempo de duración específico, el usuario con el que se accedió al equipo y en el caso de que el equipo esté ligado a un domino, el nombre del equipo del que se accede al sistema.

Gráfico Nº 4.2 Visor de Sucesos



Autora: Andrea Medrano

Los registros también guardan eventos que se ejecutaron sobre los archivos de Microsoft Office, estos son añadidos automáticamente por el Office y son:

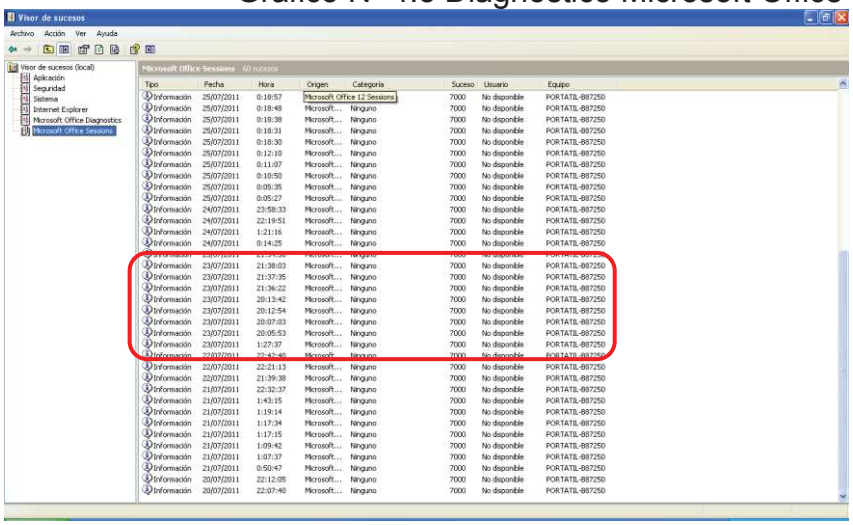
d) Diagnostico de Microsoft Office, y

[12] CÓMO ADMINISTRAR REGISTROS DEL VISOR DE SUCESOS: http://support.microsoft.com/kb/308427/es

e) Sesiones de Microsoft Office.

En la ventana siguiente se muestra que hubo actividad en el Office, el Sábado, 23 de Julio de 2011, durante un tiempo prudente para manipular información, indica que usuario y desde el equipo registrado a nombre de PortatilWN que se realizó la sesión a las aplicaciones de Microsoft Office.

Gráfico Nº 4.3 Diagnóstico Microsoft Office



Autora: Andrea Medrano

Finalmente para que la prueba sea considerada una evidencia válida, depende del contenido, de las alteraciones que se hayan realizado al o los archivos y principalmente cuál es el interés que existió para haber efectuado estas acciones sobre la información.

Con el análisis realizado y las pruebas obtenidas, se puede aplicar las leyes explicadas en el Capítulo I del proyecto, en la Legislación Ecuatoriana, en el Capítulo Tercero de las Infracciones contra el Buen Vivir, en la sección Segunda de las Infracciones contra la información, en el artículo 204 que habla sobre el Daño Informático, al culpable se le podría aplicar la pena privativa de libertad de tres a cinco años y multa de diez a veinte remuneraciones básicas unificadas del trabajador privado en general.

Así mismo, en el apartado sobre el que se hace referencia, si para obtener la información se obtiene una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

destinados a causar los efectos maliciosos la infracción será de cinco a siete años de pena privativa de libertad.

4.2 ANALISIS COSTO BENEFICIO

El análisis de costos se realiza con la finalidad de tener la idea clara de si el proyecto “Informática Aplicada a la Investigación Forense como Medio de Pruebas – Evidencia Digital” es rentable o no, a través del análisis comparativo de información sobre los costos que implican el hacer uso de la herramienta, contratar un análisis forense sobre el disco duro y el ambiente del delito, estos aspectos contra los beneficios que el estudio y la herramienta facilitan para recuperar la información, que no se debe olvidar que es invaluable para una empresa. De la adición de estos dos factores se obtiene el resultado y la mejor decisión a ser aplicada para el bien de la compañía.

Adicionalmente que se demostrará quién o quienes fueron las personas implicadas en el caso y conocer los intereses que originan el delito.

Es prudente mencionar que para resolver el juicio el presente proyecto se apoya en las leyes locales que se enfocan en el delito informático.

4.2.1 Costo de la herramienta EnCase Forensic

Cabe recalcar que los costos que se presentan a continuación fueron propuestos por uno de los proveedores de EnCase Forensic, estos documentos se presentan en los anexo, con el nombre “Cotización EnCase Forensic”.

Cuadro Nº 4.1 Costo EnCase Forensic

Cant.		Descripción	Precio Unitario	Precio Total
		MIGRACIÓN DE VERSIÓN		
1		EnCase Forensic V7 (+EDS) + SMS 1 yr	$ 4.384,00	$ 4.384,00
			Subtotal	$ 4.384,00
			Iva	$ 526,08
			Total	$ 4.910,08

Autora: Andrea Medrano

Fuente: Satélite S.A.

4.2.2 Costo de la herramienta R-Studio

El costo de la herramienta que se presenta a continuación, son los precios publicados en el internet en su página oficial:

http://www.data-recovery-software.net

Cuadro Nº 4.2 Costo R-Studio

Cant.		Descripción	Precio Unitario	Precio Total
		LICENCIA		
1		R-STUDIO network Technician	$ 899,00	$ 899,00
			Total	$ 899,00

Autora: Andrea Medrano

Fuente: http://www.data-recovery-software.net

4.2.3 Costo por Análisis Forense

La información que se muestra a continuación fue proporcionada por laboratorios Vilma Zapata, que actualmente presta servicios al mercado.

El costo siguiente cubre la recuperación de información de un disco duro y el análisis forense sobre este.

Cuadro Nº 4.3 Costo Análisis Forense

Cant.		Descripción	Precio Unitario	Precio Total
1		Recuperación de Información, Análisis Forense de disco duro	$ 180.00	$ 180,00
			12% IVA	$ 21,60
			Total	$ 201,60

Autora: Vilma Zapata

4.2.4 Costo Unificado

El costo total unificado para realizar la recuperación de la información más el contrato del servicio y la adquisición de la herramienta R-Studio, con la que se desarrollo el proyecto, corresponde a mil cien con sesenta y seis dólares.

Cuadro Nº 4.4 Costo Unificado

Cant.		Descripción	Precio Unitario	Precio Total
1		R-STUDIO network Technician	$ 899.00	$ 899,00
1		Recuperación de Información, Análisis Forense de disco duro	$ 201,60	$ 201,60
			Total	$ 1.100,66

Autora: Andrea Medrano

4.2.5 Beneficios no Tangibles

Teniendo como antecedente que la información es un recurso que no tiene precio, cualquier costo que se proponga para el proceso de recuperación de datos a la empresa XYZ, éste siempre será menos costoso que el hecho de perder información y ver a ésta comprometida en situaciones que se mal usa la información para intereses ajenos, por lo tanto el gasto que se realice en pagar

mil cien con sesenta y seis dólares, para adquirir la herramienta para la recuperación y el análisis forense es un ahorro representable para la empresa, ya que esta podría verse involucrada en casos legales serios.

El no prevenir la pérdida de información se considera un desastre y tiene un costo incalculable, pero cuando ya ha sucedido, lo importante es buscar alternativas para recuperar información en su totalidad, y evitar pérdidas que representen a la empresa o que sirvan de respaldo para cuando la información ha sido ya relacionada con algún caso legal.

El uso de la herramienta en conjunto con la aplicación de la metodología para evidencias digitales en cuanto a la recuperación de información de los dispositivos de almacenamiento, tiene un costo que no puede ser comparado con el valor de la información contenida en los dispositivos de almacenamiento.

Los dispositivos de almacenamiento contienen información de alta importancia, desde datos completos sobre la estructura de una empresa, hasta datos personales como cuentas bancarias, claves, etc. Ésta información involucra el costo de la estructura y conformación de la empresa, claves de cuentas bancarias personales, que no se compara con la ganancia de da como resultado la herramienta.

La adquisición de la herramienta posee beneficios a nivel tanto personal como empresarial ya que permite recuperar información que se creía perdida, lo que hace que los investigadores estén seguros de que la integridad de los datos no se verá comprometida y resolverá delitos con herramientas forenses.

Entre los beneficios de la herramienta uno de estas es copiar toda la estructura y contenido del dispositivo a manera de imagen hacia cualquier otro lugar que no sea el mismo que se está recuperando, con la finalidad de poder manipular esta información desde otro lugar y así no afectar la evidencia original, de tal manera que la información de la empresa esté respaldada en otro lugar.

Escanear y recuperar información desde cualquier lugar de la red con privilegios que permitan realizar esta acción, es otra característica que evita la alteración de la evidencia original y representa una ganancia para la empresa, ya que se podría recuperar información individual de los empleados.

El mayor beneficio de la recuperación de información luego de haber analizado los datos, es apoyar al esclarecimiento de casos forenses que dependen de la reconstrucción de la evidencia para cualquier caso legal en el que este involucrado el establecimiento.

Es importante conocer una vez que se ha recuperado la evidencia, que los datos originales sean los mismos que los datos reconstruidos, para lo que existen algoritmos de encriptación que permiten compara la información original con la actual, estos algoritmos realizar operaciones matemáticas que indican si la información fue editada o si permanece intacta. Adicionalmente esto implica que la empresa se vea en la obligación de aplicar políticas sobre como almacenar información y qué tipo de información almacenar y tener respaldos actualizados en cualquier dispositivo distinto del contenedor original.

Para el proyecto, se demuestra que la persona involucrada en casos legales informáticos por el momento se regirá a leyes propuestas por abogados, pero nada que se asiente sobre temas definitivos, ya que actualmente nuestra ley orgánica de lo penal se encuentra en discusión para la aprobación.

En el caso de que la ley estuviese vigente y no en discusión, la penalidad que se le aplicaría al culpable sería con respecto a daños informáticos, lo que implica de tres a cinco años de prisión con multa de diez a veinte remuneraciones unificadas y falsificaciones electrónicas que conlleva entre cinco y siete años de prisión.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- A pesar de que en el mercado se comercializa varias herramientas empresariales robustas para el análisis y la recuperación de datos, se optó por la aplicación R-Studio, ya que el gran limitante con el resto de herramientas fue el costo, sin embargo R-Studio respondió exitosamente a las pruebas sometidas y se presenta como una solución económica respecto a otras del mismo tipo.

- Para el proyecto se aplicó la metodología propuesta con base a estándares y documentos que ya han sido usados y que dieron resultados efectivos en situaciones similares, permitiendo así que el proceso de recuperación de datos siga patrones recomendados para obtener resultados positivos, como consecuencia los datos sin alteraciones, así mismo el presente caso se relacionó con la parte legal ecuatoriana para establecer las sanciones que se aplicarían al culpable.

- Se logró demostrar el proceso de recuperación de información, el mismo que para la empresa XYZ se vuelve imprescindible, usando la herramienta y las técnicas forenses en cuanto al tratamiento de la evidencia digital explicadas en el proyecto.

- Uno de los aspectos que se cubrió con este proyecto, es el tema legal relacionado con informática en el país, en conjunto con la evidencia digital y su tratamiento, teniendo en cuenta que dichas leyes están en estudio de aprobación.

- En el Ecuador el tema de la informática forense aún está en vías de desarrollo, la ley Ecuatoriana no posee legislación informática, lo que hace que para este tipo de situaciones, se tenga como apoyo

estándares u organizaciones internacionales recomendados, además de herramientas especializadas en la recuperación de datos.

- Para recuperar la evidencia digital, no se debe respaldar sobre el mismo dispositivo de almacenamiento o volumen en donde se presume que está alojada la evidencia, pues lo único que se logrará al hacer esto es que se sobrescriba la evidencia y se pierda.

- Los dispositivos de almacenamiento, en donde se encuentre alojada información a ser recuperado, no debe ser manipulada para no anular la validez de la evidencia, ni se debe guardar más información sobre el mismo dispositivo ya que puede sobrescribir datos que se quiere recuperar.

- El uso de la evidencia digital debe regirse obligatoriamente a las recomendaciones y mecanismos propuestos por organizaciones a nivel mundial, como el procedimiento para el mantenimiento de la cadena de custodia mencionada en el proyecto, la contaminación de la evidencia digital invalidaría cualquier caso que haga referencia a esta.

- La relación entre el área informática y judicial tienen mucho que ver en este campo ya que si la una prescinde de la otra, el resultado no tiene éxito y un caso no puede ser evaluado legalmente.

5.2 RECOMENDACIONES

- Se recomienda seguir los estándares estudiados para la recuperación y tratamiento de la información para que no se altere e invalide la evidencia y pueda ser usada en casos legales.

- Es primordial conocer en estos casos que la cadena de custodia, es un procedimiento indispensable a seguir, para cuidar los indicios materiales afines al delito, ya que se debe garantizar que la evidencia que se tenía en un principio es la misma que se presenta para tomar decisiones en un caso legal.

- Según estándares y organizaciones internacionales de evidencias de computadores (IOCE), un punto que se debe aplicar siempre a una evidencia, es sacarle una copia para que la original no pierda validez y sea preservada para distintos estudios legales.

- Establecer medidas y adquirir nuevas costumbres sobre el uso de información y equipos informáticos para evitar pérdidas irrecuperables y que estos se vean afectados o relacionados con delitos.

- Estudiar sobre herramientas que brinden características robustas en la recuperación de evidencia digital, teniendo en cuenta los algoritmos de encriptación que estén más vigentes y que aún no hayan sido violados por terceras personas.

- En base a lo estudiado es prudente que las personas adaptemos una conducta humana sobre el orden y cuidado, dándole la importancia que se merece al costo de la información, de esta manera se evitará la propagación de delitos informáticos, como el establecer políticas de seguridad sobre un equipo, asignando claves de acceso, permitiendo o denegando el ingreso a usuarios sobre ciertos directorios y archivos.

- La recuperación de información debe ser realizada por personal con perfil de sistemas informáticos con conocimientos legales, ya que debe saber cómo funciona el almacenamiento de datos en dispositivos y las penalidades que se deben aplicar cuando se comete infracciones relacionadas con datos confidenciales.

GLOSARIO

Evidencia.- es un término que procede del latín evidentĭa y que permite indicar una certeza manifiesta que resulta innegable y que no se puede dudar. En el derecho, una evidencia es una prueba determinante en un proceso judicial. Puede utilizarse para designar a aquello que permite demostrar la verdad de un hecho de acuerdo a los criterios establecidos por la ley.

Forense.- Es la aplicación de prácticas científicas dentro del proceso legal, básicamente, la ciencia forense, es un conjunto de ciencias que la ley usa para atrapar a un criminal, ya sea física, química, matemática, y muchas más. El trabajo de los investigadores forenses es extenso ya que consiste en la recolección de las evidencias y el proceso de las mismas.

Cadena de Custodia.- es el procedimiento de control que se emplea para los indicios materiales afines al delito, desde su ubicación, hasta que son valorados por los diferentes funcionarios encargados de administrar justicia, y que tiene como finalidad no viciar el manejo que de ellos se haga, y así evitar la contaminación, alteración, daños, reemplazos, contaminación o destrucción. Desde la ubicación, fijación, recolección, embalaje y traslado de la evidencia en la escena del siniestro, hasta la presentación al debate, la cadena de custodia debe garantizar que el procedimiento empleado ha sido exitoso, y que la evidencia que se recolectó en la escena, es la misma que se está presentando ante el tribunal, o el respectivo dictamen pericial.

Hash Codes.- se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.

Rfc3227.- Guía Para Recolectar y Archivar Evidencia. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con

intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal.

Delito informático.- El delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjucio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad.

Magnetoresistencia.- La magnetorresistencia es una propiedad que tienen ciertos materiales de variar su resistencia eléctrica cuando son sometidas a un campo magnético. Las cabezas lectoras de los discos duros están compuestas por un grupo de elementos tal que su resistencia eléctrica depende del campo magnético. Los “bits” en un disco duro se guardan como un pequeño imán. La cabeza de lectura magnetoresistiva (MR) tiene una resistencia eléctrica que varía cuando pasa por encima del “pequeño imán” que es un bit. Por tanto, cuando un bit pasa por debajo de la cabeza lectora hay una variación de la resistencia que puede detectarse fácilmente.

Dispositivo de Lectura y Escritura.- está formado por un conjunto de brazos paralelos a los platos, alineados verticalmente y que también se desplazan de forma simultánea, en cuya punta están las cabezas de lectura/escritura. Por norma general hay una cabeza de lectura/escritura para cada superficie de cada plato. Los cabezales pueden moverse hacia el interior o el exterior de los platos, lo cual combinado con la rotación de los mismos permite que los cabezales puedan alcanzar cualquier posición de la superficie de los platos. Cada plato posee dos caras, y es necesaria una cabeza de lectura/escritura para cada cara.

Disco Scsi.- (Small Computer System Interface). Interfaz estándar para transferencia de datos entre periféricos en el bus de la computadora. Tanto la

placa madre como el dispositivo deben soportar y disponer de un controlador SCSI.

Cluster.- Un clúster es la unidad de almacenamiento en un disco (ZIP, rígido o flexible) con una determinada cantidad fija de bytes. Un disco está dividido en miles de clústeres de igual tamaño y los archivos son repartidos y almacenados en distintos clústeres. El tamaño se determina en el formateo del disco y suele ser de 512 bytes, pero la cifra puede ascender a 4.096 bytes.

File Stack.- Los archivos son creados en varios tamaños dependiendo de lo que contengan. Los sistemas basados en DOS, Windows 95/98/ME/XP y Windows NT/2000 almacenan los archivos en bloques de tamaño fijo llamados clusters, en los cuales raramente el tamaño de los archivos coinciden perfectamente con el tamaño de uno o muchos clusters.
El espacio de almacenamiento de datos que existe desde el final del archivo hasta el final del cluster se llama "file slack".

Archivo Swap.- Los sistemas operativos Microsoft Windows utilizan un archivo especial como un "cuaderno de apuntes" para escribir datos cuando se necesita memoria de acceso aleatorio adicional, a estos archivos se les conoce como Archivos Swap de Windows o archivos de paginación.

Degaussers.- Remover el magnetismo de un dispositivo. Suele utilizarse el término inglés Degauss para hacer referencia a desmagnetizar monitores y otros dispositivos como pantallas que utilizan CRT (tubo de rayos catódicos).

Rsa.- (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. En la actualidad, RSA es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

Raid.- Redundant Array of Independent Disks, es un conjunto redundante de discos independientes, hace referencia a un sistema de almacenamiento que usa múltiples discos duros o SSD entre los que se distribuyen o replican los datos.

Microscopio Electrónico de Transmisión de Escaneado.- Este microscopio no explora superficies , por el contrario el haz de electrones incidente atraviesa la muestra o espécimen observado y la sombra de detalles finos o ultra-estructura es capturada en una pantalla fosforescente con propiedades de emisión de luz, ubicada en la parte inferior de la columna. El tener una adecuada preparación de la muestra da lugar a una excelente definición de imagen. Son múltiples las facetas en las que interviene este tipo de microscopio. Así, en control de calidad señalamientos morfológicos, conformación de agregados, técnicas forenses, determinación de estratos en restauración y diferenciación histológica entre otros.

BIBLIOGRAFIA

- **LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS,** Congreso Nacional del Ecuador
- **ACURIO DEL PINO**, Santiago, Introducción a la Informática Forense, Ecuador, 2007

- **R-STUDIO USER MANUAL**
  http://www.r-tt.com/downloads/rstudio.pdf
- **AUDITORIA FORENSE**
  http://www.criptored.upm.es/guiateoria/gt_m592b.htm
- **FUNDAMENTAL OF DIGITAL FORENSIC EVIDENCE**
  http://all.net/ForensicsPapers/HandbookOfCIS.pdf
- **INFORMÁTICA FORENSE**
  http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf
- **INTRODUCCION A LA INFORMATICA FORENSE**
  http://www.elhacker.net/InfoForenseWindows.html
  http://www.criptored.upm.es/guiateoria/gt_m592b.htm
  http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf
- **COMPUTO FORENSE**
  http://es.wikipedia.org/wiki/C%C3%B3mputo_forense#Identificaci.C3.B3n
- **INFORMATICA FORENSE, INTRODUCCION Y CONTENIDO**
  http://labs.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido
- **INFORMATICA FORENSE: GENERALIDADES, ASPECTOS TECNICOS Y HERRAMIENTAS**
  http://gluc.unicauca.edu.co/wiki/images/1/1d/InfoForense.pdf
- **ALGORITMO DE HASH**
  http://es.scribd.com/doc/46651/Algoritmos-de-HASH

- **ALGORITMO MD5**: http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=117&Itemid=26
- **SECURE HASH ALGORITHM**: http://maytics.web44.net/web_documents/secure_hash_algorithm.pdf
- **CÓMO ADMINISTRAR REGISTROS DEL VISOR DE SUCESOS**: http://support.microsoft.com/kb/308427/es
- **CADENA DE CUSTODIA**: http://es.wikipedia.org/wiki/Cadena_de_custodia
- **MICROSCOPIA ELECTRÓNICA** http://www.javeriana.edu.co/Facultades/Ciencias/neurobioquimica/libros/celular/microelectrans.htm
- **REPARACION DISCOS DUROS** http://www.manualespdf.es/manual-recuperar-datos/

ANEXOS

LEY DE COMERCIO ELECTRONICO

“LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS”

EL H. CONGRESO NACIONAL

Considerando:

Que, el uso de sistemas de información y de redes electrónicas, incluida la Internet ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.

Que, es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos.

Que, se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura.

Que, a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia.

Que, es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales.

En uso de sus atribuciones, expide la siguiente:

“LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS”

TÍTULO PRELIMINAR

Artículo 1.- Objeto de la Ley .- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

TÍTULO I

DE LOS MENSAJES DE DATOS

CAPÍTULO I

PRINCIPIOS GENERALES

Artículo 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Artículo 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Artículo 4.- Propiedad Intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Artículo 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de

datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Artículo 6.- Información escrita.- Cuando la Ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.

Artículo 7.- Información original.- Cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

Se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta Ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente;

Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente Ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Artículo 8.- Conservación de los mensajes de datos.- Toda información sometida a esta Ley, podrá ser conservada; éste requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

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 o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
c) Que se conserve todo dato que permita determinar el origen, el destino del 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 establezca en el Reglamento a esta Ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.
La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

Artículo 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.
La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta Ley, los cuáles podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.
No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Artículo 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,
b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

Artículo 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:

a) **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.

b) **Momento de recepción del mensaje de datos.-** Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario.

c) 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; y,

d) **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.

Artículo 12.- Duplicación del mensaje de datos.- Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

TITULO II
DE LAS FIRMAS ELECTRÓNICAS, CERTIFICADOS DE FIRMA ELECTRONICA, ENTIDADES DE CERTIFICACION DE INFORMACIÓN, ORGANISMOS DE PROMOCIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS.

CAPÍTULO I
DE LAS FIRMAS ELECTRÓNICAS

Artículo 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al

mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Artículo 14.- Efectos de la firma electrónica. La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Artículo 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular**;**
b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;
c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.
d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,
e) Que la firma sea controlada por la persona a quien pertenece.

Artículo 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley.

Artículo 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;
b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
d) Verificar la exactitud de sus declaraciones.
e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia.
f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
g) Las demás señaladas en la Ley y sus reglamentos.

Artículo 18.- Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el Reglamento a esta ley señale.

Artículo 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por:

a) Voluntad de su titular;
b) Fallecimiento o incapacidad de su titular**;**
c) Disolución o liquidación de la persona jurídica, titular de la firma;
d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

CAPÍTULO II

DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Artículo 20.- Certificado de firma electrónica.- 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.

Artículo 21.- Uso del certificado de firma electrónica.- El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta Ley y su reglamento.

Artículo 22.- Requisitos del certificado de firma electrónica.- El certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

a) Identificación de la entidad de certificación de información.
b) Domicilio legal de la entidad de certificación de información.
c) Los datos del titular del certificado que permitan su ubicación e identificación.
d) El método de verificación de la firma del titular del certificado.
e) Las fechas de emisión y expiración del certificado.
f) El número único de serie que identifica el certificado.
g) La firma electrónica de la entidad de certificación de información.
h) Las limitaciones o restricciones para los usos del certificado; y,
i) Los demás señalados en esta Ley y los reglamentos.

Artículo 23.- Duración del certificado de firma electrónica.- Salvo acuerdo contractual**,** el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta Ley.

Artículo 24.- Extinción del certificado de firma electrónica.- Los certificados de firma electrónica**,** se extinguen, por las siguientes causas:

a) Solicitud de su titular;
b) Extinción de la firma electrónica, de conformidad con lo establecido en el Art. 19 de esta Ley; y,
c) Expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Artículo 25.- Suspensión del certificado de firma electrónica.- La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley;
b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,
c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Artículo 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley, cuando:

a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,
b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada.

La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

Artículo 27.- Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

Artículo 28.- Reconocimiento internacional de certificados de firma electrónica.-

Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta Ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador**.** El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta Ley y su reglamento.

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

CAPÍTULO III

DE LAS ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN

Artículo 29.- Entidades de Certificación de Información.- 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.

Artículo 30.- Obligaciones de las entidades de certificación de información acreditadas.- Son obligaciones de las entidades de certificación de información acreditadas:

a) Encontrarse legalmente constituidas, y estar registradas en el Consejo Nacional de Telecomunicaciones;
b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;
c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información;

d) Mantener sistemas de respaldo de la información relativa a los certificados;
e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos, previo mandato del Superintendente de Telecomunicaciones, en los casos en que se especifiquen en esta Ley;
f) Mantener una publicación del estado de los certificados electrónicos emitidos;
g) Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;
h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente Ley, y hasta por culpa leve en el desempeño de sus obligaciones.
1. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados; e,
i) Las demás establecidas en esta Ley y los Reglamentos.

Artículo 31.- Responsabilidades de las entidades de certificación de información acreditadas.- Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta Ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.
Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio.

Artículo 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta Ley.

Artículo 33.- Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.
El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros.

Artículo 34.- Terminación contractual.- La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor.

Artículo 35.- Notificación de cesación de actividades.- Las entidades de certificación de información acreditadas, deberán notificar al Organismo de Control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto.

CAPÍTULO IV
DE LOS ORGANISMOS DE PROMOCIÓN Y DIFUSIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS.

Artículo 36.- Organismo de Promoción y Difusión.- Para efectos de esta Ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior.

Artículo 37.- Organismo de Regulación, Autorización y Registro de las entidades de certificación acreditadas.- El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas.
En su calidad de organismo de autorización podrá además:

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones.
b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; y
c) Las demás atribuidas en la Ley y en los reglamentos.

Artículo 38.- Organismo de Control de las entidades de certificación de información acreditadas.- Para efectos de esta Ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas.

Artículo 39.- Funciones del Organismo de Control.- Para el ejercicio de las atribuciones establecidas en esta Ley, la Superintendencia de Telecomunicaciones tendrá las siguientes funciones:

a) Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y las prácticas comerciales restrictivas, competencia desleal y protección al consumidor, en los mercados atendidos por las entidades de certificación de información acreditadas;
b) Ejercer el control de las entidades de certificación de información acreditadas en el territorio nacional y velar por su eficiente funcionamiento;
c) Realizar auditorías técnicas a las entidades de certificación de información acreditadas;
d) Requerir de las entidades de certificación de información acreditadas, la información pertinente para el ejercicio de sus funciones;
e) Imponer, de conformidad con la Ley, sanciones administrativas a las entidades de certificación de información acreditadas, en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio;
f) Emitir los informes motivados previstos en esta Ley;
g) Disponer la suspensión de la prestación de servicios de certificación para impedir el cometimiento de una infracción; y,
h) Las demás atribuidas en la Ley y en los reglamentos.

Artículo 40.- Infracciones administrativas.- Para los efectos previstos en la presente Ley, las infracciones administrativas se clasifican en leves y graves.

Infracciones leves:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por el organismo de control; y,
2. Cualquier otro incumplimiento de las obligaciones impuestas por esta Ley y sus reglamentos a las entidades de certificación acreditadas.

Estas infracciones serán sancionadas, de acuerdo a los literales a) y b) del artículo siguiente.

Infracciones graves:

1. Uso indebido del certificado de firma electrónica por omisiones imputables a la entidad de certificación de información acreditada;
2. Omitir comunicar al organismo de control, de la existencia de actividades presuntamente ilícitas realizada por el destinatario del servicio;
3. Desacatar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción;
4. El incumplimiento de las resoluciones dictadas por los Organismos de Autorización Registro y Regulación, y de Control; y,
5. No permitir u obstruir la realización de auditorías técnicas por parte del organismo de control.

Estas infracciones se sancionarán de acuerdo a lo previsto en los literales c) y d) del artículo siguiente.

Las sanciones impuestas al infractor, por las infracciones graves y leves, no le eximen del cumplimiento de sus obligaciones.

Si los infractores fueren empleados de instituciones del sector público, las sanciones podrán extenderse a la suspensión, remoción o cancelación del cargo del infractor, en cuyo caso deberán observarse las normas previstas en la Ley.

Para la cuantía de las multas, así como para la gradación de las demás sanciones, se tomará en cuenta:

a) La gravedad de las infracciones cometidas y su reincidencia;
b) El daño causado o el beneficio reportado al infractor; y,
c) La repercusión social de las infracciones.

Artículo 41.- Sanciones.- La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

a) Amonestación escrita;
b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;
c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica;
d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica;

Artículo 42.- **Medidas cautelares**.- En los procedimientos instaurados por infracciones graves, se podrá solicitar a los órganos judiciales competentes, la adopción de las medidas cautelares previstas en la ley que se estimen necesarias, para asegurar la eficacia de la resolución que definitivamente se dicte.

Artículo 43.- Procedimiento.- El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones.

TÍTULO III
DE LOS SERVICIOS ELECTRÓNICOS, LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PÚBLICOS.

CAPITULO I
DE LOS SERVICIOS ELECTRÓNICOS

Artículo 44.- **Cumplimiento de formalidades.-** Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la Ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha Ley.

CAPÍTULO II
DE LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA.

Artículo 45.- Validez de los Contratos Electrónicos.- Los contratos podrán ser instrumentados mediante mensajes 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,

Artículo 46.- Perfeccionamiento y Aceptación de los contratos electrónicos.- El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las Leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.
La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

Artículo 47.- Jurisdicción.- En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas revistas por el Código de Procedimiento Civil Ecuatoriano y esta Ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario.

Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta Ley y demás normas legales aplicables.

Cuando las partes pacten someter las controversias a un procedimiento arbitral, en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje.

CAPÍTULO III
DE LOS DERECHOS DE LOS USUARIOS O CONSUMIDORES DE SERVICIOS ELECTRÓNICOS

Artículo 48.- Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos

sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

Artículo 49.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,
b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;
2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;
3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento para actualizar la información proporcionada; y,
4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

Artículo 50.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.

Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.

La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la Internet, se realizará de conformidad con la Ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.

En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o servicio de que se trate.

En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente Ley.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.

CAPÍTULO IV
DE LOS INSTRUMENTOS PÚBLICOS

Artículo 51.- Instrumentos Públicos Electrónicos.- Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente.
Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la Ley y demás normas aplicables.

TÍTULO IV
DE LA PRUEBA Y NOTIFICACIONES ELECTRÓNICAS

CAPÍTULO I
DE LA PRUEBA

Artículo 52.- Medios de prueba.- 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.

Artículo 53.- Presunción.- Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la Ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

Artículo 54.- Práctica de la prueba.- La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los

elementos necesarios para su lectura y verificación, cuando sean requeridos;

b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados;

c) El faxcímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta Ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la Ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

Artículo 55.- Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la Ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectué con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Artículo 56.- Notificaciones Electrónicas.- Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no

puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo electrónico, de un abogado legalmente inscrito, en cualquiera de los Colegios de Abogados del Ecuador.

Las notificaciones a los representantes de las personas jurídicas del sector público y a los funcionarios del Ministerio Público que deben intervenir en los juicios, se harán en las oficinas que estos tuvieren o en el domicilio judicial electrónico en un correo electrónico que señalaren para el efecto.

TITULO V
DE LAS INFRACCIONES INFORMÁTICAS
CAPÍTULO I
DE LAS INFRACCIONES INFORMATICAS

Artículo 57.- Infracciones Informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente Ley.

Reformas al Código Penal

Artículo 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Artículo ....- 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.

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.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Artículo ...- Obtención y utilización no autorizada de Información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Artículo 59.- Sustitúyase el Art. 262 por el siguiente:
"Art. 262.- 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".

Artículo 60.- A continuación del Art. 353, agréguese el siguiente artículo innumerado: **"Art.…- 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 telemático, ya sea:

1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2. Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este
Capítulo.”

Artículo 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

“Art.....- 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.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art. .....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.”.

Artículo 62.- A continuación del Art. 549, introdúzcase el siguiente artículo innumerado:

“Art.... Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años
y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la

transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

"Art. ….- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Artículo 63.- Añádase como segundo inciso del artículo 563 del Código Penal el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando los medios electrónicos o telemáticos".

Artículo 64.- A continuación del numeral 19 del Art. 606 añádase el siguiente:

"..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

DISPOSICIONES GENERALES

Primera.- Los certificados de firmas electrónicas, emitidos por entidades de certificación extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la Ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.

Segunda.- Las entidades de certificación de información acreditadas podrán prestar servicios de sellado de tiempo. Este servicio deberá ser acreditado

técnicamente por el Consejo Nacional de Telecomunicaciones. El Reglamento de aplicación de la Ley recogerá los requisitos para este servicio.

Tercera.- Adhesión.- Ninguna persona está obligada a usar o aceptar mensajes de datos o firmas electrónicas, salvo que se adhiera voluntariamente en la forma prevista en esta Ley.

Cuarta.- No se admitirá ninguna exclusión restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en la presente Ley y su reglamento.

Quinta.- Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor.

Sexta.- El Consejo Nacional de Telecomunicaciones tomará las medidas necesarias, para que no se afecten los derechos del titular del certificado o de terceros, cuando se produzca la revocatoria del certificado, por causa no atribuible al titular del mismo.

Séptima.- La prestación de servicios de certificación de información por parte de entidades de certificación de información acreditadas, requerirá de autorización previa y registro.

Octava.- El ejercicio de actividades establecidas en esta ley, por parte de instituciones públicas o privadas, no requerirá de nuevos requisitos o requisitos adicionales a los ya establecidos, para garantizar la eficiencia técnica y seguridad jurídica de los procedimiento e instrumentos empleados.

Novena.- Glosario de Términos.- Para efectos de esta ley los siguientes términos serán entendidos conforme se definen en este artículo:

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

Red Electrónica de Información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Servicio Electrónico: Es toda actividad realizada a través de redes electrónicas de información.

Comercio Electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Intimidad.- El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a

la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley.

Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Certificado electrónico de información: Es el mensaje de datos que contiene información de cualquier tipo.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Dispositivo de emisión.- Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.

Emisor: Persona que origina un mensaje de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quién, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Quiebra técnica: Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta Ley y su reglamento.

Factura electrónica.- Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

Décima.- Para la fijación de la pena en los delitos tipificados mediante las presentes reformas al Código Penal, contenidas en el Título V de esta Ley. Se tomarán en cuenta los siguientes criterios: el importe de lo defraudado, el

quebranto económico causado, los medios empleados y cuantas otras circunstancias existan para valorar la infracción.

DISPOSICIONES TRANSITORIAS

Primera.- Hasta que se dicte el reglamento y más instrumentos de aplicación de esta Ley, la prestación del servicio de sellado de tiempo, deberá cumplir con los requisitos de seguridad e inalterabilidad exigidos para la firma electrónica y los certificados electrónicos.

Segunda.- El cumplimiento del artículo 57 sobre las notificaciones al correo electrónico se hará cuando la infraestructura de la Función Judicial lo permita, correspondiendo al organismo competente de dicha función organizar y reglamentar los cambios que sean necesarios para la aplicación de esta Ley y sus normas conexas.

Para los casos sometidos a Mediación o Arbitraje por medios electrónicos, las notificaciones se efectuarán obligatoriamente en el domicilio judicial electrónico en un correo electrónico señalado por las partes.

DISPOSICIÓN FINAL

El Presidente de la República, en el plazo previsto en la Constitución Política de la República, dictará el reglamento a la presente Ley.

La presente Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la sala de sesiones del Pleno Nacional del Ecuador, a los diez días del mes de abril del año dos mil dos.

COTIZACION COSTO ENCASE

SATELITE
Tecnología & Seguridad

Francisco Hernández de Girón Oe4-61 y Av. América
Telefax 245-7447/ 331-8996
www.satelite-ec.com Email: ventas@satelite-ec.com

Quito, 27 de julio de 2011

Señorita:
Andrea Medrano

Presente.-

PROFORMA SF- 2701

Cant.		Descripción	Precio Unitario	Precio Total
		MIGRACIÓN DE VERSIÓN		
1		EnCase Forensic V7 (+EDS) + SMS 1 yr	$ 4,384.00	$ 4,384.00
			Subtotal	$ 4,384.00
			Iva	$ 526.08
			Total	$ 4,910.08

NOTAS:

Tiempo de entrega: 30 dias luego de la orden de compra
Soporte Técnico:
Validez de Oferta: **30 días**
Forma de pago: 60 % con la orden de compra
40 % contra entrega

Atentamente

Sixto Flores R.
Asesor Comercial
Satelite-com

COSTO ANÁLISIS FORENSE

PROFORMA No. 185

Fecha:	**23 de Noviembre de 2011**
Empresa:	
RUC:	
Dirección:	
Teléfono:	**098208716**
Atención:	**Andrea Medrano**

Diagnóstico, Recuperación de Información, Análisis Forense de disco duro:

Valor: 180 + IVA

Atentamente,

Lucy Zapata
Teléfono 2225936 / 6034244
Celular: 099 839 219