UNIVERSIDAD NACIONAL DE INGENIERÍA

RECINTO UNIVERSITARIO SIMÓN BOLÍVAR.

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN.

INGENIERÍA EN COMPUTACIÓN.

MANUAL INTERACTIVO DE INFORMATICA FORENSE.

AUTOR(ES):

Br. Abigail Navarrete Torres

Br. Yalmar Lira González

Datos del Tutor: MSc. Gloria Talía Flores Quintana

Managua, Diciembre 2013.

Contenido

Introducción

El presente documento constituye el trabajo de investigación y recolección de datos elaborados como tesina, para la obtención del Título en Ingeniero en Computación. En el mismo se aborda información de interés, antecedentes de la informática forense en Nicaragua, justificación del trabajo, un esbozo del marco teórico y el desarrollo de una pequeña aplicación interactivo.

La Informática Forense es una nueva tendencia de las tecnologías computacionales que se encarga de realizar un análisis minucioso de los sistemas informáticos o computacionales, con el fin de buscar y analizar evidencia que colabore a una institución, en una situación relacionada al fraude, ataques a la seguridad de documentos, equipos, información confidenciales, entre otros.

La informática forense utiliza un conjunto de técnicas y herramientas tanto de hardware y como software para determinar datos potenciales o relevantes, en la recuperación de información, evidencias que permitan conocer o establecer a las instituciones que soliciten su aplicación la posibilidad de un daño o perdidas, tanto de equipos, información o monetarias, en un ataque; o bien saber si dichas pérdidas fueron provocadas de forma accidental.[1]

[1] http://www.informaticaforense.com.ar/informatica_forense.htm

Objetivos

Objetivo General:

Dotar a la Facultad de Electrotecnia y Computación de la Universidad Nacional de Ingeniería, de un manual interactivo sobre informática forense, el mismo permitirá a los estudiantes conocer las definiciones y características fundamentales de esta área de la informática, así como las ventajas que tiene su utilización.

Objetivos Específicos:

1. Realizar una recopilación de la información esencial acerca de la informática forense para lograr fundamentar la herramienta interactiva a desarrollar.

2. Dotar a los alumnos de la Facultad de Electrotecnia y Computación una herramienta interactiva que permita facilitar el aprendizaje de la informática forense.

3. Vincular el uso de la informática forense con las actividades educativas de la carrera de computación.

Antecedentes

La informática forense hace su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los 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. Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.[2]

En Nicaragua se ha escuchado hablar muy poco del tema, tanto así que las instituciones educativas superiores adolecen de cursos relacionados con el mismo, es hasta el año 2011 a finales que algunas instituciones inician cursos libres y de otras índoles para mostrar el uso de la misma. Sin embargo es importante también contar con la constitución y la creación de leyes que protejan el uso de los equipos informáticos y documentos digitalizados, actualmente las leyes para estos fines a penas se discuten en el seno de algunas instituciones.

Actualmente en Nicaragua el ente regulador de las comunicaciones Instituto Nicaragüense de Telecomunicaciones y Correos (Telcor) hizo conocer a la comisión sobre el tema de seguridad de las telecomunicaciones la reforma a la constitución política de la Republica de Nicaragua donde especifica que las empresas de telecomunicaciones del país deberán de tener instalados sus equipos de transmisión en Nicaragua y no como lo es actualmente donde la mayoría tiene sus servidores de comunicación fuera del país.[3]

Así mismo el director de Telcor Orlando Castillo dentro de las reformas a las regulaciones propuso el mantener las bases de datos y registros informáticos dentro del país, donde el gobierno podrá tener acceso a ellos únicamente por

[2] http://informaticaforense.mex.tl/237044_Antecedentes.html
[3] Periódico el nuevo diario de Nicaragua 12 de noviembre de 2013, Sección Política, CSE y Telcor respaldan reforma a Constitución.

razones de seguridad nacional ya que dentro de las redes sociales y en internet pueden las personas pueden intentar hacer cosas indebidas. [4]

Con estas reformas a la constitución en cuanto a los temas de seguridad informática dentro y fuera del país, se estará realizando un gran avance en cuanto al control del uso de la información y la introducción de la informática forense tomando en cuenta los aspectos que esta nueva ciencia trata de regular para mantener la estabilidad dentro del país y el continente.

[4] Periódico la prensa de Nicaragua 06 de noviembre de 2013, Sección Ámbitos, Telcor: en las redes sociales hay gente haciendo "cosas que no deben".

Justificación

La carencia de documentación actualizada relacionada al análisis forense tanto en las instituciones de educación superior como en las empresas, conlleva a la desinformación de todas las ventajas que esta puede brindar a las instituciones Nicaragüense; saber que herramientas utilizar y que técnicas son las más adecuadas acordes a las necesidades y posibilidades del país es de suma importancia hoy en día.

El trabajo investigativo propuesto, indica la realización de una herramienta interactivo que permita proporcionar toda la información relacionada al tema de una forma fácil de aprender, incluyendo videos, casos de estudio, y aplicaciones para validar y evaluar los conocimientos adquiridos de una manera sencilla.

Marco Teórico

Historia de la Informática Forense

1978: Florida reconoce los crímenes de sistemas informáticos en el "Computer Crimes Act en casos de sabotaje, copyright, modificación de datos y ataques similares.

1980: Se inició el campo de la informática forense.

1981: Nace Copy II PC de Central Point Software se usa para la copia exacta de disquetes.

1982: Peter Norton publica UnErase: Norton Utilities 1.0

1984: Programa fue creado Medios Magnéticos del FBI, después se convirtió en Jefe del Equipo de Análisis Digital (CART).

1986: Clifford Stoll colabora en la detección del hacker Markus Hess.

1987: Se crea la High Tech Crime Investigation Association (HTCIA), asociación de Santa Clara.

1988: Se crea la International Association of Computer Investigative Specialists (IACIS), que certificará a profesionales de agencias gubernamentales en el Certified Forensic Computer Examiner.

1989: El documento Stalking the Wily Hacker, contando lo ocurrido, es transformado en el libro El huevo del cuco anticipando una metodología forense.

1992: El libro "A forensic methodology for countering computer crime, de P. A. Collier y B. J. Spaul acuña en el término "computer forensics".

1993: Se celebra la primera Conferencia Internacional sobre la Evidencia Digital.

1995: Se funda la Organización Internacional de Evidencia Digital (IOCE).

1996: La Interpol organiza los International Forensic Science Symposium, como foro para debatir los avances forenses.

1997: En diciembre, los países del G8 en Moscú declararon que "los funcionarios encargados de hacer cumplir la ley deben estar capacitados y equipados para hacer frente a los delitos de alta tecnología."

1998: En Marzo, el G8 nombrado el IICE para crear los principios internacionales, los procedimientos regessem relacionados con la evidencia digital.

1999: El trabajo total de la FBI en informática forense superior a 2000 casos a través del análisis de 17 terabytes de datos.

2000: El primer laboratorio regional de Informática Forense del FBI.

2001: En agosto nace la Digital Forensic Research Workshop (DFRWS), un nuevo grupo de debate y discusión internacional para compartir información.

2003: El trabajo total del FBI en casos forenses informáticos excede 6500, a través del análisis de 782 terabytes de datos.

2004: Los Servicios de Ciencia Forense del Reino Unido planean desarrollar un registro de expertos cualificados, y muchas organizaciones Europeas, incluyendo la Red Europea de Institutos de Ciencia Forense publicaron líneas básicas para investigadores digitales.

2005: Se celebra el Reto Rediris v2.0, junto con la Universidad Autónoma de México.

2006: Se celebra el III Reto Rediris, en el cual había 3 premios para los mejores de España y 3 para los mejores de Iberoamérica.[5]

[5] http://www.datarecovercenter.co/Servicios/Informatica-Forense/Auditoria-e-Investigacion-Forense/Historia-de-la-Informatica-Forense
https://sites.google.com/site/sykrayolab/historia-de-la-informatica-forense

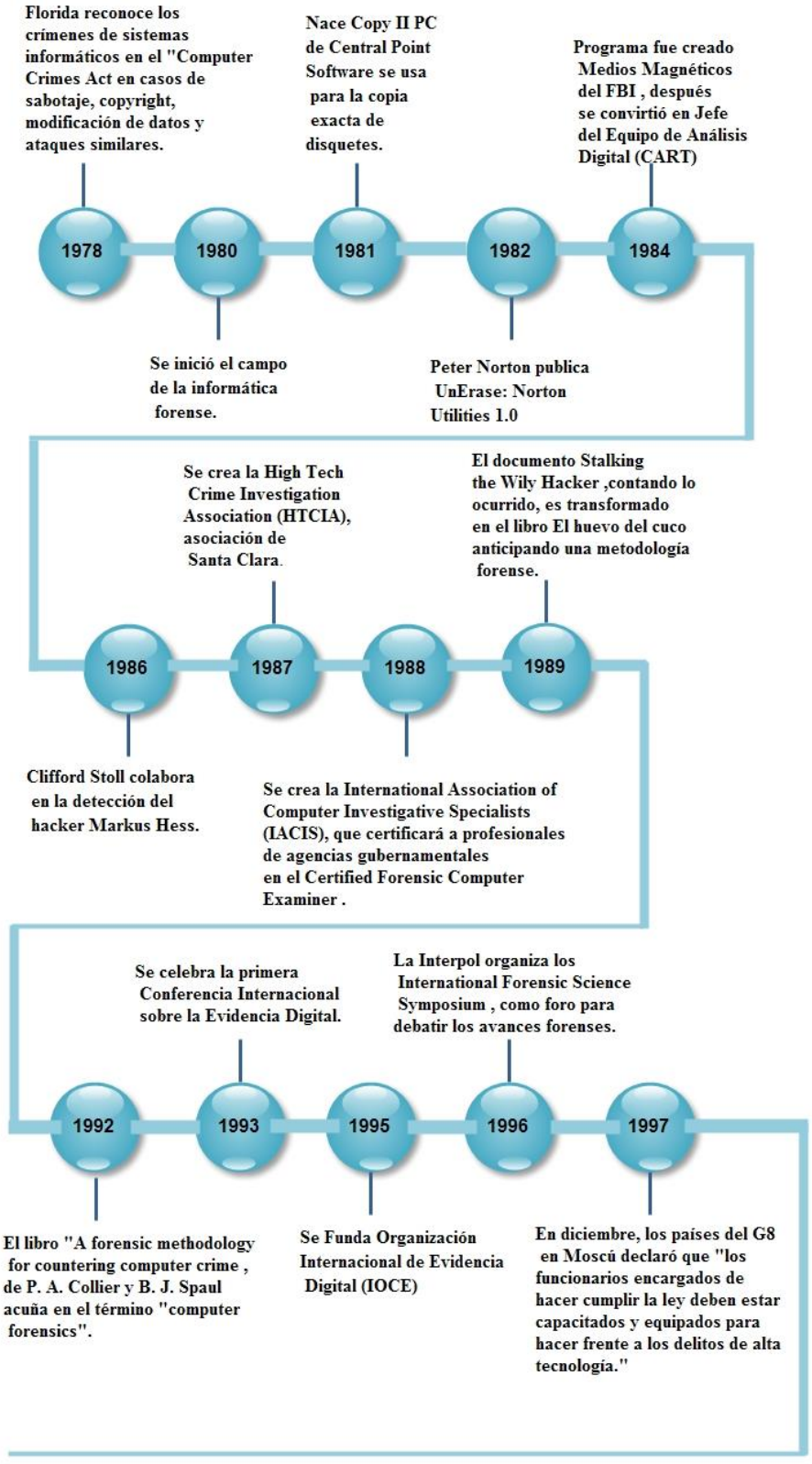


Imagen.1.Historia Informática forense parte 1.

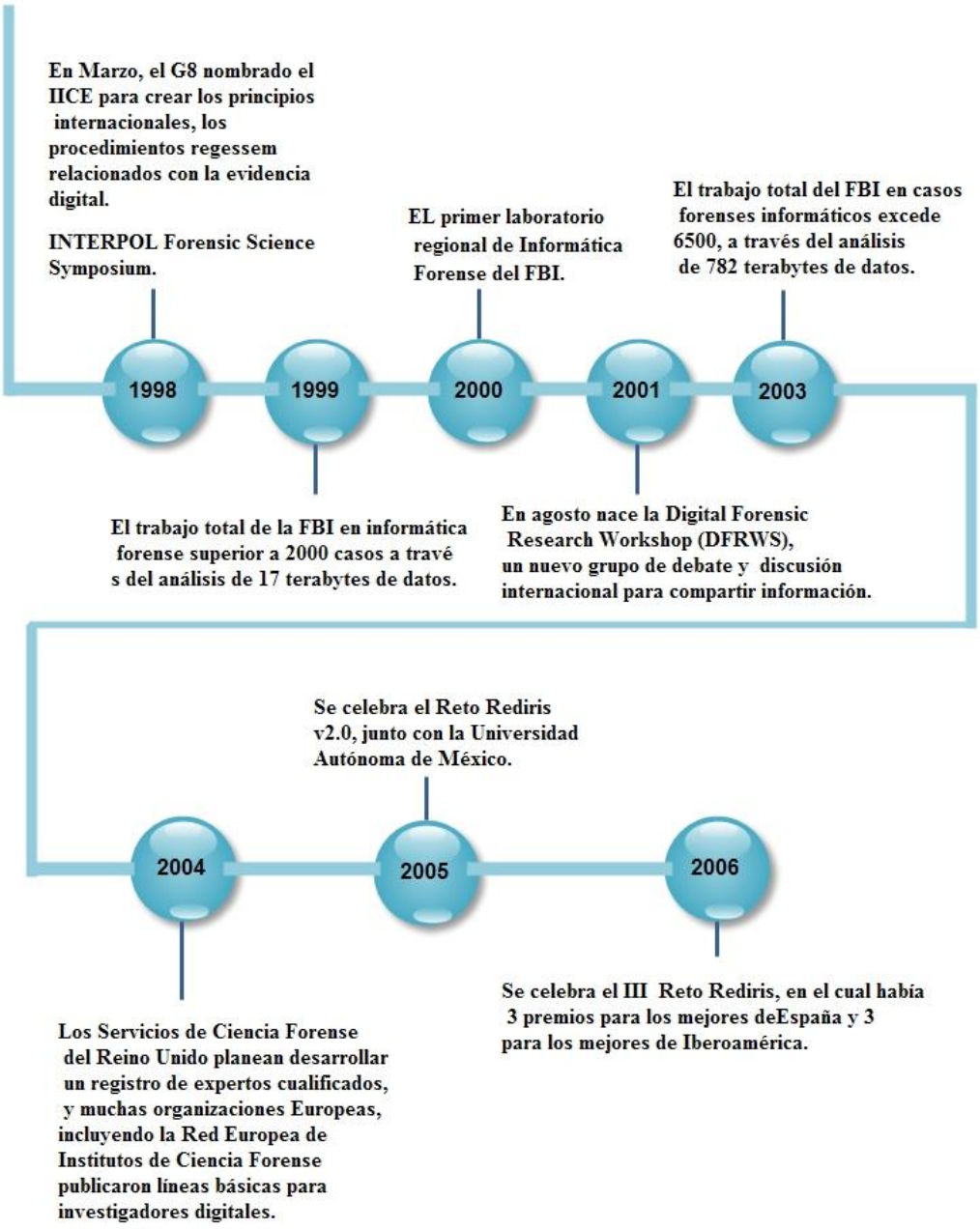


Imagen.2.Historia Informática Forense parte 2.

Datos

Cuando hablamos a cualquier tipo de información nos referimos a datos como fotografías, música, gráficos o cualquier otro tipo de información que le pertenezca a persona física identificada o identificable.

La información que pertenece a una persona identificada hace referencia a la información de una persona física y ésta nos indica directamente a que persona se refiere sin necesidad de realizar un proceso de investigación en el cual se averiguara a quien pertenece. Ejemplo de este tipo de información es la cedula de identidad cuya información contiene la identidad exacta de una persona física determinada, la tarjeta de vacuna, expediente médico, cuenta bancaria, mensaje de correo electrónico etc.

La información que pertenece a una persona identificable es aquella que hace referencia a una persona física pero esta no contiene datos suficientes para poder averiguar su identidad. Un ejemplo de este tipo de información es el ADN, la dirección IP dinámica de la computadora[6], la cual se tenga que relacionar con una persona específica, la ropa que uno usa etc.

Los datos de carácter personal son:

Datos especialmente protegidos:

Información que se protege de manera muy personal y no se anda divulgando a todo mundo, ejemplo: Ideología, religión, origen racial o étnico, salud y vida sexual.

[6] Es un número IP que se le asigna a un dispositivo (ver glosario).

Datos de carácter identificativo:

Información que se relaciona directamente con una persona, ejemplo: No de cedula, dirección, imagen, voz, numero del INSS, nombre y apellidos, huella/firma, tatuajes o marcas en el cuerpo, firma electrónica[7].

Datos relativos a las características personales:

Información que se relacione con la forma de ser de una persona, ejemplo: estado civil, edad, sexo, lugar de nacimiento, idioma, propiedades físicas y medidas del cuerpo.

Datos académicos y profesionales:

Información que se relaciona con la educación de la persona, ejemplo: Títulos, constancia de notas, experiencia profesional, pertenecía a alguna institución de educación.

Datos de Empleo:

Información que relacione a una persona en un trabajo, ejemplo: puesto de trabajo, profesión, datos de la nómina que no tengan que ver el aspecto económico, historial de la persona como trabajador.

Datos que aportan información comercial:

Información que se relacione con una persona y con sus actividades dentro del comercio de un país, ejemplo: negocios, autorización comercial, publicaciones, o medio de comunicación, creaciones artísticas, científicas o técnicas.

Datos económicos, financieros y de seguros:

Información que se relacione a una persona con la capacidad de generar dinero y aportar a la economía de un país, ejemplo: créditos, inversiones, ingresos, plan de jubilación, impuestos, historial de créditos, subsidios, hipotecas, tarjeta de crédito.

[7] Es el proceso que permite relacionar e identificar a un individuo o equipo informático, (ver glosario).

Datos relativos a transacciones de bienes y servicios:

Información que relacione a una persona con cualquier servicio relacionado con las tracciones o compromiso de una persona que una persona realice, ejemplo, transacciones financieras, indemnizaciones, servicios y bienes que tanto suministra o recibe una persona (servicio de agua, energía eléctrica, teléfono, internet, etc.)[8]

Informática

Es la ciencia que utiliza maquinas computacionales para tratar los datos (introducir, procesar, presentar la información) de forma automatizada auxiliándose de programas [9] creados por el razonamiento humano.

Cómputo forense o informática forense

Se puede definir como una rama del cómputo que se encarga de recolectar, analizar datos que se encuentran en cualquier sistema para utilizarlos y puedan ser aceptados en un proceso legal.

Ésta a su vez utiliza técnicas científicas y de análisis especializados en la infraestructura tecnológicos[10] las cuales permiten identificar, preservar la información, analizarla y posteriormente presentarla de forma que todos los datos sean válidos en un proceso judicial.

Delito informático

Es todo acción que se realiza ya sea de manera involuntaria o voluntaria para cometer un crimen utilizando un medio de cómputo. [11]

[8] Conceptos-Basicos-de-Proteccion-de-Datos-Personales.pdf
[9] Es la parte de la computadora que no se puede tocar, (ver glosario).
[10] Es la agrupación de dispositivos de hardware y software que integran una empresa, (ver glosario).
[11] http://www.monografias.com/trabajos97/nocion-delitos-informaticos/nocion-delitos-informaticos.shtml

Clasificación de los delitos informáticos.

a. Como instrumento o medio. El criminal presenta una conducta perversa en la cual se auxilian del uso de computadoras como un medio o método o instrumento para realizar el ilícito.

b. Como fin u objetivo. El criminal presenta una conducta perversa con el fin de dañar la computadora, accesorios o programas como entidad física.[12]

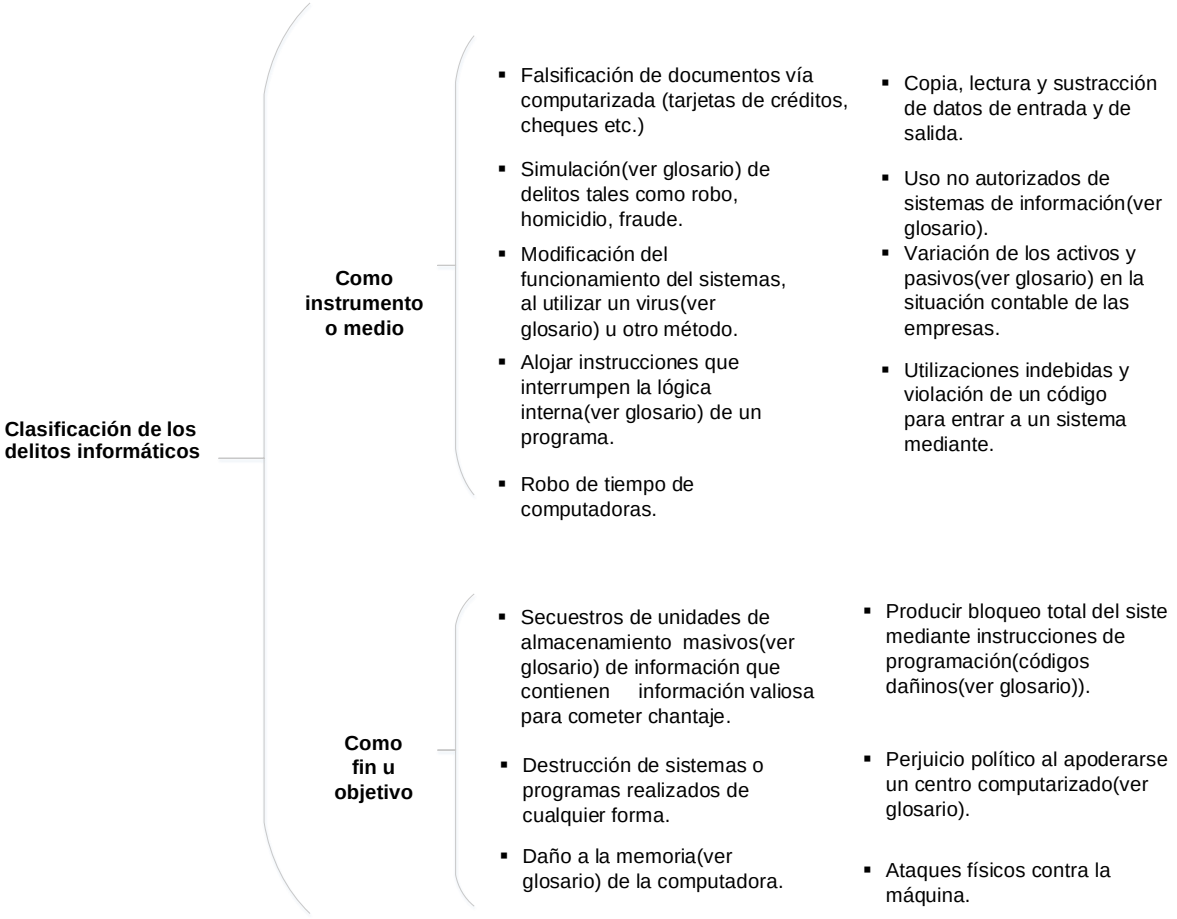


Imagen.3.Clasificación de los delitos informáticos.

[12] http://ditumbeschullepe.galeon.com/aficiones2454509.html

Dentro de los delitos informáticos podemos establecer:

Sujeto activo

Son aquellos sujetos que poseen la capacidad o habilidad de utilizar los sistemas informáticos; debido al maneja de datos e información de carácter sensible, estos en varios casos no se desenvuelven en tareas laborales que favorecen la participación de este tipo de delitos, es decir no necesariamente laboran en el área de informática o directamente en la empresa que se comete el crimen.[13]

Sujeto Pasivo

Son aquellos sujetos que se les conocen como víctimas del delito, en ocasiones es la persona jurídica que por titular que la ley protege y al quien recae la responsabilidad aun cometida por el sujeto activo. Podemos decir que la victimas puede ser cualquier persona, institución del gobierno, empresas de crédito que se valen de la ayuda y utilización de sistemas automatizados de información que están de una u otra manera enlazados con otros sistemas.[14]

Evidencia Digital.

Es una forma de prueba física, formada por campos magnéticos[15] y pulsos electrónicos[16], que pueden ser reunidos y analizados con instrumentos y métodos especializados. Este tipo de pruebas son frágiles y deben de ser recolectadas con mucho cuidado para garantizar su legitimidad[17]. Por ejemplo tenemos imágenes, correos electrónicos, archivos, hardware[18] de la computadora así como otro dispositivo tecnológico.

[13] http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp
[14] http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
[15] Es el fluido de la corriente eléctrica que fluye por un medio, (ver glosario).
[16] Son pulsos electromagnéticos que generan un voltaje ya sea alto 1 o bajo 0, (ver glosario).
[17] Es un término que hace referencia a que un objeto o situación, (ver glosario).
[18] Es todo aquello físico de la computadora que podemos ver y tocar, (ver glosario).

La evidencia se clasifica así:

a. *Evidencia inculpatoria.* Soportada por una teoría dada.

b. *Evidencia exculpatoria.* Contradice una teoría dada.

c. *Evidencia de manipulación*. Este tipo de evidencia no tiene relación con ninguna teoría pero si muestra que el sistema fue alterado para eludir la identidad del sistema o persona que accedió a los datos.

Principios de la informática forense.

Son necesarios al momento de examinar ya sea una computadora o un cadáver:

Cadena de Custodia.

Este tipo de tarea presenta quien y cuando la adquirió, que persona se encargó de protegerla y quienes han tenido contacto con la evidencia.

Evitar la contaminación.

Mantener los datos intactos después de haberse cometido el delito es esencial al iniciar un proceso investigativo forense o informático, ya que el uso de una herramienta contaminado puede ser el causante de una mala deducción o análisis de las causas del crimen.

Actuar metódicamente.

La persona que vaya a realizar la investigación debe proteger cada uno de los procesos que realizo al momento de la investigación, es decir documentar los resultados recibidos durante el análisis de los datos, proteger los instrumentos que utilizo, con el objetivo de que cualquier sujeto externa pueda comprobar y revisar los mismos. Al tener validado y documentado todo el proceso investigativo genera tranquilidad al investigador, ya que de ser muy metódicos en los procesos científicos que se aplican en estos casos, existe la posibilidad que una tercera persona pueda copiar sus resultado usando la misma evidencia.

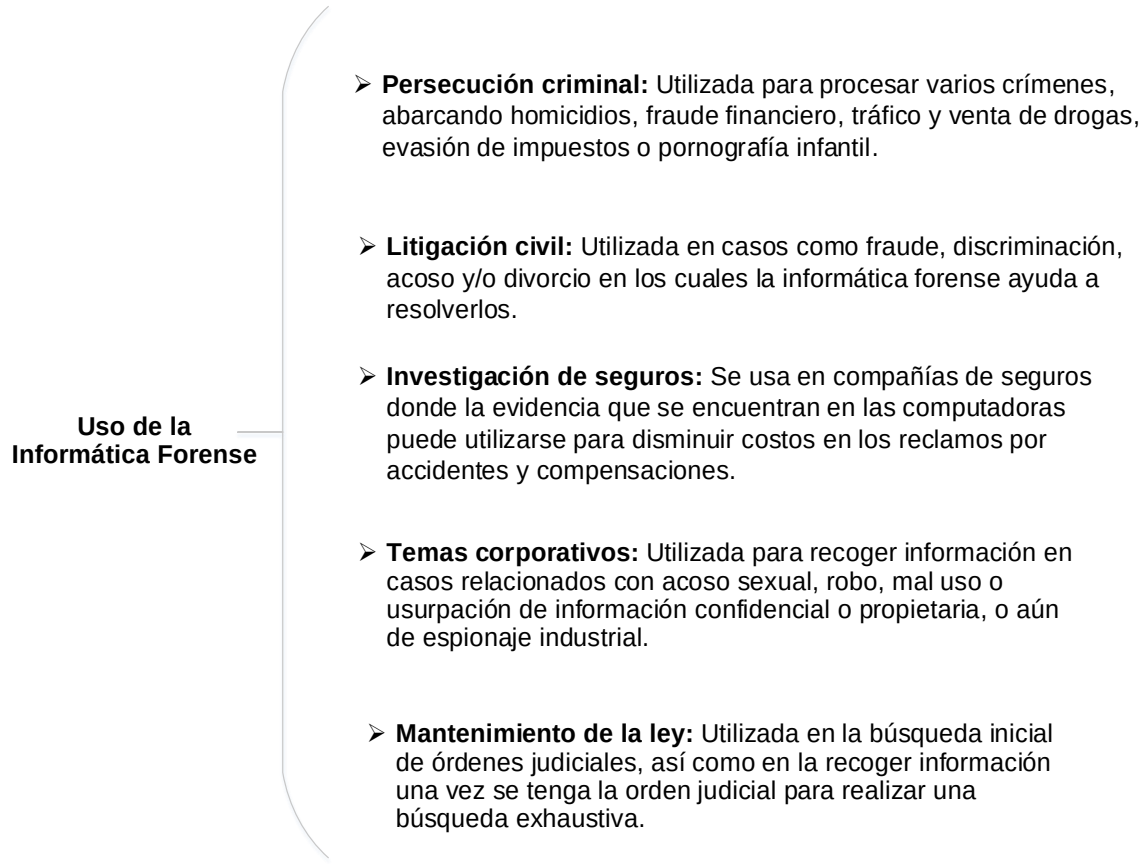
Controlar la cadena de custodia.

Cada uno de los elementos relacionados con el caso y en responsabilidad del investigador debe de controlarse de manera rápida y con formalidad especial para documentar cada uno de los sucesos realizados con la evidencia para obtener una mejor administración de las pruebas.

La informática forense tiene como propósito:

- Sospechas de actos no autorizados dentro de la organización.
- Ataques contra los sistemas informáticos de la organización.
- Sustracción de información sensible o confidencial de la organización.
- Intentar probar autorías o no autorías ante una acusación.
- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.[19]

[19] http://www.slideshare.net/Fundaciocatic/analisis-forense-busca-de-evidencias



20

Imagen.4.Uso de la informática forense

Se analizarán las dos principales vertientes

1. Análisis forense de dispositivos de almacenamiento para examinar evidencias.

2. Análisis forense de sistemas telemáticos con el objetivo de detectar actividades no autorizadas.

Importante: Sin importar que en cada caso las herramientas utilizadas varían, los pasos del proceso de análisis a seguir poseen la misma estructura y son requisitos del mismo.

[20] http://www.criminalistaenred.com.ar/Informatica_F.html

Proceso de análisis forense relacionado con un caso de ejemplo

Identificación

En esta fase de la investigación debe de quedar esclarecido el procedimiento que se debe de continuar a partir de los datos aportados en cuanto a conocer los antecedentes, situación actual y para tomar la mejor decisión a la hora de la búsqueda de información.

Así también es necesario tener información sobre el equipo informático, posición y uso en la red así como datos relativos a los problemas detectados para que estos datos demuestren la necesidad de la auditoria forense[21].

Caso de estudio

Antecedentes del incidente

El incidente ocurrió en una empresa Pyme[22] donde el administrador de sistemas noto la existencia de una cuenta que él no había creado en su sistema de ERP[23] en el servidor por lo que desconfía de algún ingreso no autorizado, y desconoce el alcance de dicho delito.

Se conoce que el sistema donde se presentó el conflicto es un servidor Windows 2003, donde la función que este desempeña principalmente es brindar acceso al sistema ERP a través de la web y hace poco tiempo se había cambiado al uso de este servidor.

Dada la información proporcionada por el administrador de sistemas el servidor se intentaba mantener actualizado y no se sabe cómo ingresaron al sistema.

[21] Es un procedimiento donde se usan técnicas de investigación criminalística, (ver glosario).
[22] Pequeña y mediana empresa, (ver glosario).
[23] El sistema de planificación de recursos empresariales, (ver glosario).

También aclaro que hay más personas que disponen del uso de cuentas privilegiadas en el sistema y que ocupaban dichas cuentas no solo para trabajos administrativos sino también personales o ejecución de aplicaciones que no requieren de privilegios de administrador para ejecutarse.

Preservación

En ésta fase se realiza una revisión y creación de un clonado del dispositivo[24] que vaya hacer analizado.

Para asegurar la integridad de los datos se debe realizar una comprobación es imprescindible salvaguardar la integridad de los datos realizando una comprobación checksum[25] del original y de la copia creada.

Hay que tener cuidado al realizar el clonado o imagen del dispositivo de tal manera que no se cambie nada de la imagen de la imagen creada. La fuente dispositivo de la clonación debe permanecer bajo custodia para asegurar su autenticidad.

En esta etapa se pueden realizar los siguientes pasos:

1. Montaje del dispositivo[26].
2. Obtener las particiones del dispositivo[27].
3. Realizar la suma de verificación (checksum) del dispositivo original objeto de la auditoria.
4. Creación de una imagen para trabajar con ella (clonado).
5. Una vez realizado el clonado se comprobará el checksum obtenido con el checksum del original.

[24] Se trata de un copiado, (ver glosario).
[25] Es un método que detecta que el proceso de copiado de disco sea correcto, (ver glosario).
[26] Es la acción que se realiza al momento de conectar un nuevo hardware al computador, (ver glosario).
[27] Es el espacio de uso que se le asigna en un disco duro, (ver glosario).

Es importante: Si en el paso 5 no coinciden los checksum se debe repetir el proceso antes de saltar a la siguiente etapa.

Al momento de realizar la clonación del dispositivo investigado se puede utilizar software especial para la creación del clonado o imagen así como un hardware especial para dicha función.

Es importante: El hecho de utilizar diferente herramientas tanto de Hardware como Software ya sea por la variedad de tiempo, precio o uso, los resultados deben de ser los mismo, es decir la clonación debe ser bit por bit[28] el mismo sin importar que herramienta se utilizó.

Caso de estudio

Una vez obtenido los datos del incidente proporcionados por el administrador del sistema se procedió a montar en el equipo servidor una herramienta para la clonación de disco y una unidad de almacenamiento masivo, se efectuó un checksum previo al sistema y luego se realizó la clonación del dispositivo para obtener una imagen del sistema y posteriormente se verifico con otro checksum que la información de la copia de la imagen coincidiera con el checksum del sistema original para garantizar la integridad de la evidencia.

Recuperación

Para realizar esta etapa se necesita la ayuda de instrumentos especialmente diseñados para la recuperación, borrados o perdidas de datos localizados en los dispositivos a analizar.

Es recomendable realizar la recuperación de datos utilizando más de un instrumento, ya que de esta forma existe mayor garantía que los datos del dispositivo se recuperen en su totalidad; la cantidad de instrumentos de

[28] Se trata de un copiado, (ver glosario).

recuperación a utilizar va en dependencia del formato del dispositivo a analizar así como la inclinación dela persona que está realizando el análisis.

Caso de estudio

Una vez obtenida la imagen del disco del servidor para recuperar la información se optó a utilizar la herramienta VMware Workstation (ver tabla.2.) para montar la imagen obtenida del sistema creando varios entornos de trabajo para garantizar que los datos de los dispositivos recuperados se recuperen en su totalidad.

- Entorno Linux red hat (ver tabla.2.) para utilizar las herramientas de análisis forense Sleuthkit (ver tabla.2.) y Autopsy (ver tabla.2.) para tener otra perspectiva de la recuperación de archivos.
- Entorno Windows Server 2003 SP1 (ver tabla.2.) para tener acceso a las distintas aplicaciones y así avanzar en el análisis del sistema identificado en la imagen.

Análisis

Es el procedimiento de utilizar técnicas científicas y analíticas una vez que sé que se realizó la clonación o duplicación de datos a los dispositivos en los cuales se almaceno la copia mediante el proceso forense para encontrar evidencias que ayuden a entender ciertos eventos o conductas criminales o fuera de lo establecido.

Se puede realizar diferentes tipos de búsquedas dependiendo la necesidad y lo se desea encontrar:

- Cadenas de caracteres, fechas, horarios, palabras clave, etc.

- Acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB[29] (marca, modelo).

- Búsqueda de archivos específicos.

- Recuperación e identificación de correos electrónicos.

- Recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet[30], etc.

- Búsquedas realmente avanzadas mediante el uso de scripting[31] si se está auditando desde un sistema Linux[32] como puede ser Backtrack[33].

- Buscar en logs[34] generados y guardados en servidores[35], dispositivos, servicios y bases de datos[36] mostrara información relevante.

Caso de estudio

Se procede a arrancar el sistema pero aún se desconoce la contraseña de las cuentas se decide modificar la clave de administrador utilizando el programa chntpw (ver tabla.2.).

Una vez que se logra entrar al sistema se procede a configurar la información dela zona y hora antes de continuar con cualquier otro detalle de la evidencia, mediante el System Event Log (ver tabla.2.).

[29] Universal serial bus, (ver glosario).
[30] Es una colección de información de las actividades de internet, (ver glosario).
[31] Lenguaje guion, es un conjunto de instrucciones de programación pequeño, (ver glosario).
[32] Es un conjunto de programas que administra los recursos del computador, (ver glosario)
[33] Distribución de Linux diseñada en livecd, (ver glosario).
[34] Es un registro de eventos del sistema, (ver glosario).
[35] Es una computadora que forma parte de una red, (ver glosario).
[36] Es un conjunto de información, (ver glosario).

Luego se procedió a extraer una lista de los ficheros del sistema, lista de los ficheros borrados e intentar recuperar aquellos que sea posible, tiempo de acceso, creación y modificación de ficheros mediante el uso de la herramienta EnCase (ver tabla.2) y Autopsy (ver tabla.2) para listar la información de un sistema de fichero.

Se realiza una evaluación en caliente del sistema para obtener la lista de cuentas de usuarios y llama la atención una cuenta que diferente a las demás por ser la única sin nombre completo asociado y dentro de los caracteres vocales por números un habido usado por delincuentes informáticos así como la utilización de proactive password auditor (ver tabla.2) para recuperar la contraseña de dicha cuenta sospechosa.

Luego se procedió a buscar virus usando el antivirus panda titanium 2006 (ver tabla.2.), rootkits[37] logrando encontrar cookies[38] considerados espías pero sin afectar ningún fichero.

Se revisó también la lista de servicios y programas auto arrancables en el inicio del sistema con la herramienta autorun[39], así como el análisis de los puertos tcp[40] y udp[41] abiertos en el sistema usando la herramienta tcpview (ver tabla.2) los cuales se obtuvo que no había ninguna alteración de los mismos.

Llamo la atención el puerto tcp 3389 correspondiente a un servicio del protocolo de acceso remoto y el cual estaba configurado para tener acceso al sistema, se presume que el atacante activo este servicio.

Analizando los ficheros temporales del sistema se logró obtener que el usuario sospechoso genero una cuenta de correo electrónico que con la ayuda de EnCase

[37] Programa que permite un acceso de privilegio continuo, (ver glosario).
[38] Es un registro que se guarda en el navegador de internet, (ver glosario).
[39] Son componentes del sistema operativo Microsoft Windows, (ver glosario).
[40] Protocolo control de transporte, (ver glosario).
[41] Protocolo de diagrama de usuarios, (ver glosario).

(ver tabla.2) se obtuvo el nombre de la cuenta de correo electrónico relacionado con el sospechoso.

Con esta información se pudo averiguar cómo y cuándo se creó la cuenta sospechosa y a partir de ahí se siguió las actividades que tuvieron lugar en el ataque.

Presentación

En esta etapa se realiza un informe donde una vez realizado el análisis de todos los datos recuperados se presentara todo el proceso que se realizó explicando paso a paso los acontecimientos y evidencias encontradas utilizando una metodología.

Se recomienda realizar el informe de tal manera que sea fácil de leer y comprender, esto se debe a que un informe forense podrá ser leído en un futuro en un proceso judicial[42] y de su interpretación será una pieza clave para tomar una decisión durante el juicio legal.

Caso de estudio

Al terminar la investigación se pude obtener los siguientes puntos a considerar:

- Se puede establecer que hubo un cómplice involuntario que es usuario del sistema ya que mediante un correo electrónico que fue recibido en su cuenta el atacante logro obtener acceso.

- Luego de acceder en el servido el atacante creo una cuenta administrador en la cual se dedicaba a leer y copiar los archivos que se encontraban y generaban dentro del sistema.

[42] Es un proceso que se realiza para hacer ejercer el derecho de las personas, (ver glosario).

- A pesar que él es sistema estaba bien protegido el ataque ocurrió al uso indebido de las funciones del servidor, al utilizar el internet en actividades no relacionadas a lo profesional.

- Al identificar el correo electrónico del transgresor se pudo utilizar una herramienta para recuperar claves.

- Se accedió a la cuenta del correo del sospechoso relacionado con el usuario desconocido en el sistema y en ella encontrar la información personal que indica la persona que cometió el delito así como los datos que usurpo.

En consecuencia al ataque se recomienda:

- Reinstalar una versión del sistema operativo desde cero.
- Deshabilitar servicios que no sean necesarios durante su funcionamiento.
- Instalar todos los sistemas de seguridad requeridos.
- No obviar las alertas de la seguridad que notifica el sistema operativo.
- Realizar respaldo de información de los usuarios así como verificar los permisos relacionados con estos.
- Realizar un cambio de todas las contraseñas y una vez realizado esto proceder a conectar la red con el mundo exterior.
- Guardar de manera cifrada la información más importante y confidencial para evitar o minimizar un posible robo de la misma.

Destrucción segura del bien clonado

En el dado caso que la evidencia clonada que se utilizó para su análisis durante el proceso forense no permanezca bajo una custodia o no sea reclamado por la empresa, se recomienda su perfecta destrucción y certificarla.[43]

[43] http://es.slideshare.net/Fundaciocatic/analisis-forense-busca-de-evidencias

LA MEJORE PRÁCTICA EN CÓMPUTO FORENSE PROPUESTAS POR EL SWGDE (SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE)[44]

Incautación de evidencia.

a. Preguntar al oficial de policía encargado de la investigación el kit de herramienta de cómputo forense (ver glosario) necesaria para llevar a la escena.

b. Verificar la orden judicial legal que permita incautar la evidencia con sus respectivas limitaciones establecidas, en el caso que la evidencia que se desea confiscar no esté dentro de los parámetros establecidos, buscar la forma de su aprobación.

c. En la necesidad en la cual la evidencia no pueda confiscarse de la escena del crimen, realizar una copia o clonación que vaya de acuerdo a los procesos locales.

d. Confirmar que ninguna persona que estuvo en contacto con la escena del crimen no posea evidencias y garantizar el alejamiento inmediato de las personas de la escena.

e. Entrevistar a los sospechosos, testigos y administradores de red para solicitar información que ayude a saber que tanto conocimiento tienen del sistema, por ejemplo, contraseñas, sistemas operativos, direcciones de correo, etc.

f. Asegurarse de realizar una exhaustiva revisión de la escena del crimen, con el objetivo de obtener cualquier mínimo de información que represente una evidencia, de tal forma la persona que realice la investigación debe de tener muy claro los tipos de evidencias que pueda encontrar.

Imagen.5. Incautación de evidencia.

[44] Best Practices for Computer Forensics; "Scientific Working Group on Digital Evidence"; Version 1.0; Noviembre 2004, https://www.swgde.org/documents/Archived%20Documents/2004-1115%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20v1.0

Manipulación de evidencia.

Si se encuentra que la computadora esté apagada, no encender el equipo.

a. Antes de apagar un equipo, asegurarse que no exista ningún software de cifrado de datos (ver glosario), en el dado caso que se encuentre instalado alguno, recolectar primero la información requerida antes del apagado de la máquina.

b. Asegurar que en el lugar de la escena del crimen se cuenta con todas las necesidades de alimentación de energía requerida por los dispositivos con memoria volátil (ver glosario) y seguir con las reglas establecidas para poder manipular el dispositivo.

c. Documentar las condiciones en que se encuentra la evidencia, tomando fotografías legibles, por ejemplo de la pantalla, vista frontal y trasera del equipo, alrededores, además de realizar un croquis de las conexiones de la computadora, poniendo énfasis en los componentes externos.

d. Tomar nota y documentar cualquier daño a la evidencia.

e. Al encontrarse con una computadora con o sin conexión de red, se debe quitar el cable de alimentación directamente del equipo y sellar este conector con algún tipo de cinta.

f. En el caso de servidores, se debe tomar en cuenta la cantidad de información que puede ser necesario capturar, ya que este tipo de equipos son fuente de mucha información, en caso de ser necesario se deben capturar los datos volátiles (ver glosario) y de requerirse apagar el equipo se debe realizar empleando los comandos adecuados.

g. Toda evidencia obtenida se debe proteger de los cambios y es necesario mantener la cadena de evidencia de acuerdo a las políticas de la organización, un empaque apropiado para la evidencia puede incluir:

- Bolsas de papel o plástico.
- Sellar con cinta de evidencia los puntos de acceso y conectores de la computadora.
- Los dispositivos con memoria volátil deben empacarse apropiadamente, de tal manera que el dispositivo se encuentre alimentado.

h. Tener cuidado con el transporte de la evidencia digital para evitar daños físicos, vibraciones y los efectos de los campos magnéticos, estática, y los cambios bruscos de temperatura y humedad.

Imagen.6.Manipulacion de la Evidencia

Preparación de equipo.	a. Para asegurar el buen funcionamiento del equipo, este debe de estar vigilado y documentado. b. Se debe utilizar solamente equipos que estén en buen funcionamiento. c. Se recomienda poseer el manual de operación (ver glosario) del fabricante del equipo. d. Validar que el software de análisis/clonado brinde buenos resultados antes de usarlo.

Imagen.7.Preparación de equipos

Imágenes Forenses.

a. Documentar las condiciones actuales de la evidencia.

b. Tomar las precauciones necesarias para evitar que la evidencia entre en contacto con sustancias o materiales dañinos.

c. Evitar que le evidencia sea modificada, haciendo uso del hardware o software bloqueador de escritura (ver glosario).

d. Se debe emplear hardware o software que tenga capacidades de obtener copias bit a bit de los medios originales.

e. La evidencia que haya sido remitida para su análisis debe tratarse de tal modo que se preserve su integridad.

f. Se debe contar con medios preparados adecuadamente para cuidar que al realizar las copias de la evidencia, estos no se mezclen con información de otros casos.

g. Las imágenes forenses deben guardarse en dispositivos de almacenamiento, de acuerdo con las políticas organizacionales y las leyes aplicables.

Imagen.8.Imagenes forenses.

Análisis forense.

a. El analista debe contar con la debida capacitación en investigación forense.

b. Es necesario que el analista revise con detalle la documentación proporcionada por el solicitante para poder determinar las etapas a realizar para el análisis, así como las aprobaciones legales necesarias.

c. Tomar en cuenta la urgencia y prioridad del solicitante respecto a los resultados del análisis, así como otros tipos de análisis forense que pudieran ser requeridos.

d. Acordar una estrategia de análisis entre el solicitante y el investigador.

Imagen.9.Analis forense.

Documentación.

a. Copia de la autorización legal.

b. Cadena de custodia.

c. La cuenta inicial de la evidencia que será analizada.

d. Información relacionada a los paquetes y condiciones de la evidencia una vez que han sido recibidos por el analista.

e. Una descripción de la evidencia.

f. Comunicaciones relacionadas al caso.

h. Toda la documentación debe conservarse de acuerdo a las políticas de la organización.

g. La documentación del análisis debe ser específica del caso y contener los detalles suficientes que permitan a otro analista forense que se ha realizado y los hallazgos encontrados.

Imagen.10.Documentación.

Reportes.

a. Los reportes de resultados del análisis forense deben cumplir con los requerimientos que marque la política de la organización.

b. Los informes emitidos por el analista deben abordar las necesidades del solicitante.

c. El informe es para proporcionar a quien lo lea la información relevante al caso, de una manera clara y concisa.

Imagen.11.Reportes.

Revisión.

a. La organización debe contar con una política escrita en la que se establezcan los protocolos de revisión (ver glosario) por pares/técnica y administrativa.

b. La organización debe contar con una política para determinar las líneas de acción a seguir en caso de que el analista y el revisor no lleguen a un acuerdo.

Imagen.12.Revisión.

Crímenes y evidencia digital.

A continuación se muestra una lista de delitos que pueden estar relacionados a una computadora u otros dispositivos electrónicos, así como las posibles pruebas que pueden obtenerse de varios tipos de evidencia digital.[45]

Investigaciones de Fraude Computacional.	
• Datos de las cuentas de subastas en línea. • Contabilidad de software y archivos. • Libreta de direcciones. • Calendario. • Registros de chat.	• Información de clientes. • Datos de la tarjeta de crédito. • Bases de datos. • Software de cámara digital. • Correos, notas y cartas. • Registros financieros de bienes.
Investigación de Pornografía y Abuso Infantil.	
• Registro de chats. • Software de cámara digital. • Correos, notas y cartas. • Juegos. • Software de edición de gráficos.	• Imágenes. • Registro de actividad en internet. • Archivos de vídeo. • Usuario que creó el directorio y nombres de archivos de imágenes.
Investigación de Intrusiones de Red.	
• Libreta de direcciones. • Archivos de configuración. • Correos, notas y cartas. • Programas ejecutables. • Registro de actividad en internet	• Direcciones y nombres de usuario de protocolos de internet. • Registros de chat. • Código fuente. • Archivos de texto con nombres de usuario y contraseñas.
Investigación de Homicidios.	
• Libreta de direcciones. • Correos, notas y cartas. • Registro de activos financieros.	• Números telefónicos. • Diarios. • Mapas.

[45] http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/7879/1/2386_tesis_Diciembre_2010_933405487.pdf

• Registros de actividad en internet. • Documentos legales y testamentos. • Registros médicos.	• Fotos de la víctima o sospechoso. • Fotos de trofeos.
Violencia Doméstica.	
• Libreta de direcciones. • Diarios. • Correos, notas y cartas.	• Registros financieros. • Registros telefónicos.
Fraudes Financieros y Falsificación.	
• Libreta de direcciones. • Calendario. • Imágenes de moneda corriente. • **I**mágenes de orden de pago y cheques. • Información de clientes. • Correos, notas y cartas. • Identificaciones falsas.	• Registro de estados financieros. • Imágenes de firmas. • Registros de actividad en Internet. • Software bancario en línea. • Imágenes de falsificación de monedas. • Registros del banco. • Números de tarjetas de crédito
Amenazas de correo electrónico y acoso.	
• Libreta de direcciones. • Diarios. • Correos, notas y cartas. • Registros de activos financieros. • Imágenes.	• Registros de actividad en internet. • Documentos legales. • Registros telefónicos. • Victimas. • Mapas de ubicación.
Investigaciones en Drogas.	
• Libreta de direcciones. • Calendario. • Bases de datos. • Recipientes de droga. • Correos, notas y letras.	• Identificaciones falsas. • Registros de activos financieros. • Registros de actividad en internet. • Imágenes de procedimientos de elaboración.
Piratería de Software.	
• Registros de chat.	• Números de serie de software.

• Correos, notas y cartas. • Archivos de imagen de licencias de software. • Registros de actividad en internet.	• Utilerías para crack de software[46]. • Nombres de archivo y directorios creados por el usuario que clasifiquen el software propietario.
Fraude en Telecomunicaciones.	
• Software de clonación. • Bases de datos de clientes. • Números de serie electrónicos. • Números de identificación móvil.	• Correos, notas y letras. • Registros de activos financieros. • Registros de actividad en internet.
Robo de identidad.	
• Herramientas de hardware y software (Backdrops[47], lector/escritor de tarjetas de crédito, software de cámara digital, software de scanner). • Plantillas de identificaciones (Actas de nacimiento, chequeras, licencias de conducir, firmas electrónicas, registro de vehículos).	• Actividad en internet relacionada con robo de identidad (correos y noticias, documentos borrados, pedidos en línea). • Instrumentos de negocio (cheques, números de tarjetas de crédito, órdenes de pago, cheques personales).

Tabla.1.Tipos de delitos informáticos

Marco Legal para la Informática Forense

La informática forense como un fenómeno relativamente nuevo en los últimos tiempo, sus aplicaciones en todas las áreas del conocimiento humano incluye lo que es también el derecho.

La interrelación entre el derecho y la informática tiene dos vertientes fundamentales:

[46] Es una clave o registro que tiene como objetivo cambiar el comportamiento de un software original, (ver glosario).
[47] herramienta que se utiliza para cambiar el fondo de diferentes imágenes digitales, (ver glosario).

Una donde se utiliza la informática como una herramienta de diseño de entornos de compilación y almacenamiento de información a esta se le conoce como informática jurídica.

Por ejemplo creación, almacenamiento y recuperación de información jurídica como las leyes, documentos administrativos, expedientes judiciales, realización de gestiones de tipo jurídicos, como contratos, certificados, gestionar estudios jurídicos, administrar recursos humanos, consulta de legislación.

Una segunda donde la informática se utiliza como auxilio en el derecho para regular un marco regulador de las actividades ilícitas utilizando un dispositivo de computo o tecnológico para buscar y proteger cualquier tipo de información que sea objetivo de algún fraude o sospechas de robo, conocido como Derecho Informático.

El derecho informático es aquel que se caracteriza por principios y normas que regulan los efectos jurídicos que se han definido de la relación entre el derecho y la informática; no se dedica al uso de los dispositivos informáticos como auxilio al derecho.

Legislación informática

Conjunto de reglas jurídicas creadas para regular el procesamiento de la información

Es el conjunto de ordenamientos jurídicos creados para regular el tratamiento de la información.

En muchos países dentro de sus legislaciones se ha pronunciado normas jurídicas dirigidas a proteger la utilización abusiva e ilícita de la información. Tiene las siguientes características:

· Conductas criminales de cuello blanco[48], sólo un determinado grupo de personas tiene esos conocimientos.
· Son acciones ocupacionales
· Son acciones de oportunidad
· Ofrecen posibilidades de tiempo y espacio
· Presentan grandes dificultades para su comprobación

Legislaciones nacionales, regionales e internacionales

En los últimos tiempos dentro del ámbito internacional se ha llegado a acuerdos dentro de las valoraciones político – judicial de los problemas que se derivan del mal uso que se hace de las computadoras, dando lugar a que se modifiquen los derechos penales de los países.

Casi el 90% de los delitos informáticos que investiga el FBI en Estados Unidos tienen que ver con Internet. Esto nos enlaza directamente con los problemas de inexistencia de fronteras que aparecen constantemente cuando tratamos estos delitos: ¿Cuál es la ley a aplicar en multitud de casos? La solución pasa por una coordinación internacional, tanto a la hora de investigar como a la hora de aplicar unas leyes que deben contar con un núcleo común.

Tratados Internacionales

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

[48] Personas que cometen un delito en virtud de su status social, (ver glosario).

El GATT, se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), por consecuencia todos los acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes.

· El convenio de Berna
· La convención sobre la Propiedad Intelectual de Estocolmo
· La Convención para la Protección y Producción de Fonogramas de 1971
· La Convención Relativa a la Distribución de Programas y Señales

Legislación internacional

En algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender[49] ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. De ello surge la necesidad de adoptar medidas legislativas.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países tales como España, Francia, Chile, Alemania, Austria, Estados Unidos, Holanda, Reino Unido, Venezuela y Nicaragua.

En cuanto a Nicaragua Existe un anteproyecto de Ley Especial contra Delitos Informáticos, que el Consejo Nicaragüense de Ciencia y Tecnología (Conicyt) presentó a la Asamblea Nacional en 2005.

[49] Aprehender: Prender a una persona que ha cometido un delito: la policía ha aprehendido al asesino.

Para la elaboración de esta ley se montaron mesas de consulta en 2003. Al año siguiente estaba listo el primer borrador, y en 2005 fue presentado el anteproyecto a la Asamblea Nacional

En 2006 pasó a la Primera Secretaría del Poder Legislativo. Dos años después fue desechado. Algo lógico, porque ya las tecnologías le llevaban mil kilómetros de distancia.

La ley propuesta por el Conicyt fue discutida y desechada en plenario el 17 de septiembre de 2008 “porque esos delitos ya están tipificados en el Código Penal”, pero aún se queda corto.

Aunque el Código Penal vigente incorpora, al menos, seis artículos que penalizan los delitos informáticos, Sandra Barberena, asesora legal del Conicyt, considera que “esa clasificación resulta insuficiente para castigar todas las formas de delincuencia que se pueden cometer a través de medios tecnológicos” y que la ley es necesaria.

Campos de estudio del Derecho Informático:

1. Acceso a la información
2. Acceso a las TICs (Tecnologías de la información y las comunicaciones)
3. Administración de Justicia y Nuevas Tecnologías.
4. Banca y Dinero Digital
5. Censura en Internet. Libertad de Expresión online
6. Comercio Electrónico
7. Contratos Informáticos
8. Compras públicas mediante el uso de las NTIC (nuevas tecnologías de la información y las comunicaciones)
9. Correo electrónico
10. Defensa del consumidor
11. Delitos Informáticos
12. Derecho en la Era Digital
13. Derecho de las Telecomunicaciones
14. Derecho Laboral e Informática. Teletrabajo.

15. Documento Electrónico, mensajes de datos, EDI y Factura Electrónica
16. Editoriales online de Derecho.
17. E-government
18. e-Learning del Derecho y Nuevas Tecnologías
19. Firma Electrónica
20. Hábeas data
21. Impuestos e Internet
22. Informática jurídica
23. Manifestación de la Voluntad por Medios Electrónicos
24. Medidas Cautelares sobre Equipos
33. Protección de Datos de Carácter Personal
34. Publicidad e Internet
35. Relación entre el Derecho y la Informática
36. Seguridades informáticas
37. Sociedad civil e Internet
38. Sociedad de la Información
39. Software libre
40. Telefonía y Voz sobre IP
41. Wireless Application Protocol (WAP)[50]
51
Informáticos
25. Nombres de Dominio y Direcciones IP
26. Notas Bibliográficas y de Eventos
27. Notificación por Medios Electrónicos
28. Privacidad
29. Protección de datos
30. Profesionales del Derecho en la Era Digital
31. Propiedad Intelectual y Propiedad Industrial e Internet
32. Programas: Software Jurídico. Bases de datos y Gestión de Bufetes

[50] Es una regla segura que permite al usuario poseer información de forma instantánea, (ver glosario)
[51] Marco_Legal_para_la_Informatica_Forense.pdf

Herramientas Forenses

Durante el proceso de investigación forense informático o de cualquier otro proceso investigativo, la recolección y recuperación de la evidencia juega un papel muy importante que ayuda a encontrar pruebas se puedan almacenar y determina la mejor forma de encontrar al o los culpables del ataque informático.

La utilización de la mejor herramienta ayudara a realizar un proceso de investigación rápido, eficiente y veras; de esta manera se podrá sustentar la evidencia durante un juicio.

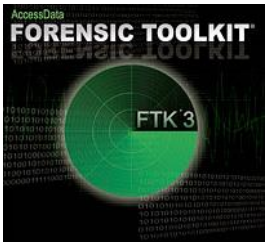
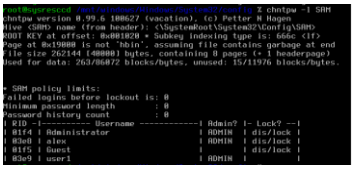
Tabla de herramientas

Instrumento forense	Descripción
The Sleuth Kit 	Es una colección de herramientas de análisis forense de volumen de sistema y archivos. Soporta particiones DOS[52], particiones BSD[53](etiquetas de disco), particiones Mac[54]) y disco GPT[55]. Con estas herramientas, se puede identificar donde se ubican las particiones y extraerlas, de manear que pueda ser analizadas con las herramientas de análisis del sistema de archivos.
Autopsy Forensic 	Es la mejor herramienta libre que existe para el análisis de evidencia digital. Su interfaz gráfica es un browser que basado en las herramientas en línea de comandos del Sleuth Kit, permite un análisis de diversos tipos de evidencia mediante una captura de una imagen de

[52] Sistema operativo de disco, (ver glosario).
[53] es un tipo de partición basado en el sistema de operativo UNIX, (ver glosario)
[54] Tipo de particiones creada por Apple, (ver glosario).
[55] Es un disco físico el cual posee una tabla de partición GUID (identificador globalmente único), (ver glosario)

	disco.
VMWare Workstation 	Es un sistema de virtualización por software. Este programa simula un sistema físico (un ordenador) con características de hardware determinadas, proporcionando un ambiente de ejecución similar a todos los efectos de un ordenador físico (excepto en el puro acceso físico al hardware simulado), con CPU[56] (puede ser más de una), BIOS[57], tarjeta gráfica[58], memoria RAM, tarjeta de red[59], sistema de sonido, conexión USB[60], disco duro (pueden ser más de uno), etc.
EnCase Forensic Edition 	Herramienta que permite determinar comportamientos en redes, acceso, manipulación o creación de datos y de dispositivos periféricos que se conecten a uno o varios computadores. Se especializa en la adquisición de imágenes forenses, capacidad para análisis concurrente de varios sistemas, Análisis de firmas de archivos , analizador de registro de eventos de Windows Documentos y archivos compuestos (por ejemplo, archivos comprimidos) búsquedas avanzadas, soporte para sistemas de archivos NTFS comprimidos, gestión de filtros compuestos, creación de “Logical Evidence Files” con autenticación MD5 y gestión del contenido de correos electrónicos, historial de internet y web caché.

[56] Unidad Central de Procesamiento, (ver glosario).
[57] Sistema Básico de Entrada/Salida, (ver glosario).
[58] Es una tarjeta de expansión de una computadora, (ver glosario).
[59] Es una tarjeta de expansión de una computadora la cual permite la comunicación, (ver glosario).
[60] Es el tipo de conexión capaz de comunicar, conectar y proveer de energía a los dispositivos USB, (ver glosario).

Hetman software 	Recupera archivos borrados de IDE / ATA / SATA / duro y unidades externas de disco SCSI, USB y dispositivos de almacenamiento FireWire, ZIP y discos de 3.5 “. El archivo de software de la recuperación puede UnErase archivos borrados de cualquier teléfono celular y tarjetas de memoria de cámaras de fotos.
AccessData Forensic ToolKit (FTK) 	Posee funciones eficaces de filtro y búsqueda de archivos. Los filtros personalizables de FTK permiten buscar en miles de archivos para encontrar rápidamente la prueba que necesita. También realiza análisis de correo electrónico.
R-Studio Network Edtion 	Se encarga de recuperación de datos más completo y la herramienta de restauración compatible con los sistemas de archivo FAT12/16/32, NTFS, NTFS5 (creado o actualizado por Win2000), Ext2FS (Linux) y que recupera archivos tanto en discos lógicos y físicos locales como en discos en ordenadores remotos sobre las redes, incluso si sus estructuras de partición están dañadas o eliminadas.
AccessData Mobile Phone Examiner Plus (MPE+) AccessData	Es la versión para análisis de dispositivos móviles del Access Data toolkit FTK.
Chntpw 	Change NT Password es un programa que nos permite quitar o modificar las contraseñas de usuario de los sistemas Windows NT, 2k, XP, Vista y Win7 accediendo al sistema de ficheros desde un sistema Linux.

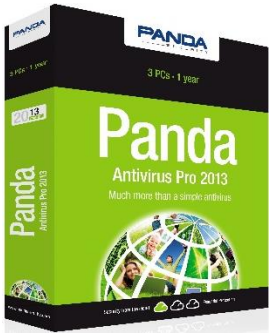
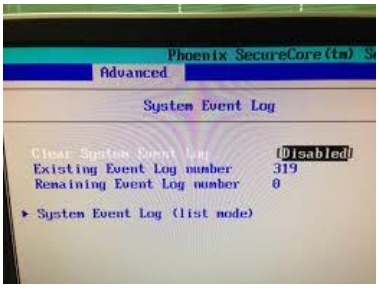
Tcpview 	Es un programa de Windows que muestra listados detallados de todos los extremos de TCP y UDP del sistema, incluidas las direcciones locales y remotas y el estado de las conexiones
Panda Antivirus y Antispyware 	Ofrece la seguridad completa para las amenazas en internet y virus.
System Event Log 	Función del Sistema operativo para mostrar datos de un registro de eventos de sistema.

Tabla.2.Herramientas

Ventajas y Desventajas de Algunas Herramientas Forenses

AccessData Forensic ToolKit (FTK)	
Ventajas	**Desventajas**
• Permite crear una imagen de disco en conjuntos la verificación de integridad devolviendo una cadena MD5. • Permite abrir once formatos diferentes de correos electrónicos. • Durante la búsqueda de archivos permite seleccionar criterio tales como tipo de archivo, tamaño reduciendo la cantidad de la extracción de información irrelevante. • Permite la elaboración de informes en formatos pdf, html, xml. • Función de búsqueda de archivos gráficos rastros de internet. • Compatibles con formatos de imágenes de EnCase, Smart y dd. • El análisis es automático. • Permite hacer imágenes de disco de todo el rango de memoria del sistema así como de uno o varios dispositivos. • Permite conexiones remotas a un único equipo y así poder realizar análisis forense de los datos activos en los equipos remotos desde el sistema del examinador. • Permite la adquisición de información	• La carga de la imagen de disco es un proceso no automático y esta tarda en realizar el montaje aproximadamente 30 min según el tamaño del dispositivo analizado. • La verificación de la cadena MD5 tarda más en comparación a otras herramientas.

de la red de forma segura y de un solo sistema, tales como dispositivos físicos, RAM etc. • Permite enumerar los procesos ocultos por los rootkits.	
Autopsy y The Sleuth Kit	
Ventajas	**Desventajas**
• El tiempo de verificación de cadena MD5 es mucha más rápido que otros programas. • Es una herramienta de acceso libre. • Permite visualizar los datos generados durante la búsqueda en forma de directorio. • Generación de informes.	• No genera una imagen de disco y necesita la ayuda de otra aplicación para poder realizar dicho propósito. • Únicamente soporta imágenes de discos creadas en .dd. • Es necesario estar en red todo el tiempo para su uso, provocando tiempos de interrupción durante el proceso del análisis, generado por la deficiencia de la conexión de red. • Durante el filtrado de los datos uno debe mantenerse posicionado en la ventana de búsqueda sino se perderá la información y se deberá iniciar de nuevo el filtrado desde cero.
R-Studio Network Edtion	
Ventajas	**Desventajas**
• Interfaz amigable. • Recupera datos en red. • Soporta los sistemas de archivos Fat 12, Fat 16, Fat 32, Ext 2.	• Durante el análisis se dilata mucho tiempo para poder finalizarlo así como un resultado no muy satisfactorio comparado con otras herramientas en cuanto a la cantidad de archivos recuperados.

Comparación entre Access Data Forensic ToolKit (FTK), Autospy e R-Studio Network Edtion
Basándose en las ventajas y desventajas de cada programa la experiencia de sus usos, FTK es el más óptimo para realizarse un análisis forense para obtener evidencias fiables, ya que permite crear imágenes de un dispositivo así como montar imágenes de diversos formatos en conjunto con la verificación de la integridad devolviendo una cadena MD5, así como el filtrado de información de archivos actuales, borrados, cifrados e incluso archivos de correos electrónicos, y su ejecución durante el análisis depende solo de la alimentación de energía.

Tabla.3.Ventajas y desventajas herramientas FTK, Autopsy e R-Studio

EnCase Forensic	
Ventajas	**Desventaja**
• Permite la interacción con VMware, Microsoft virtual pc, e imágenes .dd • Soporta discos de Windows 2000, Xp, 2003 Server. • Permite investigar múltiples partes de evidencias, clasificando los archivos en comprimidos o no en una gran cantidad de discos duros, extraíbles, zip y otros tipos de dispositivos de almacenamiento masivo. • Si la información recuperada es demasiada grande en tamaño, se puede colocar un disco duro más grande o incluso usar un servidor de red. • Permite buscar la información mediantes campos de ordenamientos ya sea por la fecha que se creó, última	• Disfrutar de todas las funciones del programa resulta costoso en comparación a otras herramientas.

modificación, nombre del archivo, extensiones etc. • Realiza análisis de archivos tipo Zip y adjuntos de correos electrónicos. • Soporta muchos tipos de sistemas de archivos desde Dos, Windows, Macintosh y Linux. • Genera el reporte del proceso de análisis forense automáticamente. • Permite visualizar las imágenes clasificada por tipo de archivo ya sea .gif o .jpg mediante la vista de galerías facilitando la apreciación de las fotos y escoger las imágenes más relevantes en el proceso investigativo.	
Hetman software	
Ventajas	**Desventaja**
• Soporta el sistema de archivo NTFS y FAT. • Recupera archivos eliminados de la papelera de reciclaje. • Recupera información en todos los formatos posibles así como archivos diseñados en Photoshop. • Recupera información de todos los tipos de tarjetas de memorias así como el soporte para dispositivos del tipo usb 3.0. • Es seguro y fácil de usar.	• Los diferentes beneficios que se pueden obtener al usar hetman es que cada uno de sus funciones está empaquetado de forma individual no como un paquete completo y resulta tedioso y algo costoso utilizarlo.

Comparación entre EnCase Forensic y hetman
Basándose en las ventajas y desventajas de cada programa la experiencia de sus usos, se considera más óptimo el uso de Encase Forensic ya que es una herramienta completa que le facilitara el trabajo y mejores resultados al investigador durante el proceso de análisis forense.

Tabla.4.Ventajas y desventajas herramientas EnCase Forensic y Hetman.

AccessData Mobile Phone Examiner Plus (MPE+)	
Ventajas	**Desventajas**
• Soporta dispositivos móviles que utilizan los sistemas Blackberry, iOs y Android. • Realiza reportes. • Soporta una variedad de formatos de imágenes y extensiones de archivos para exportar durante una búsqueda de datos.	• No facilita el análisis a dispositivos móviles con sistemas operativos o versiones Windows así como celulares anteriores a los nuevos celulares inteligentes.

Tabla.5.Ventajas y desventajas herramientas AccessData Mobile Phone Examiner.[61]

[61] Evaluación de herramientas para análisis forense orientado a discos duros.pdf

Desarrollo de la Aplicación

La información presentada en forma de texto se demostrara de manera interactivo utilizando un programa creado en adobe flash cs6 action script 2.0 con el propósito que la información llegue a los estudiantes de una forma didáctica y fácil de encontrar.

Para una mejor captación del uso de la herramienta interactivo de informática forense se podrá consultar el manual de usuario de forma texto y video tutorial.

Conclusiones

Con el trabajo realizado se presentan de forma interactiva las características fundamentales de la informática forense, así como las ventajas que tiene la utilización de la misma.

Se provee a estudiantes de la carrera de Ingeniería en Computación una herramienta sencilla y animada para conocer los conceptos básicos de la informática forense.

Con el manual interactivo se vincula la informática forense con las actividades educativas, ya que se hace uso de las tics para presentar la información y para la revisión de los conocimientos adquiridos se hace uso de un cuestionario.

Recomendación

Se recomienda hacer uso de videos, herramientas similares a la implementada en este trabajo, como alternativas de materiales en la docencia, enfocados al área de la informática forense.

Es importante hacer uso de videos donde se aborden situaciones o problemas reales donde se hace uso de la informática forense para la solución de los mismos, se sugiere que los estos sean analizados y además narrados, para la fácil comprensión por parte de los estudiantes.

Glosario

Activos y pasivos: Los activos son los bienes y derechos que le pertenecen a una organización y generan ingresos; los pasivos son estimaciones de gastos futuros formados por el conjunto de los recursos financieros**.**

Auditoria forense: Es un procedimiento donde se usan técnicas de investigación criminalística, conocimientos jurídicos procesales para hacer manifiesto las opiniones e información como evidencias o pruebas en los tribunales.

Autorun: Son componentes del sistema operativo Microsoft Windows que determinan qué acciones toma el sistema cuando una unidad es montada.

Backdrops: herramienta que se utiliza para cambiar el fondo de diferentes imágenes digitales.

Backtrack: Distribución de Linux diseñada en livecd creada para la auditoria de seguridad informática.

Bases de datos: Es un conjunto de información de forma organizada para un determinado uso que permite administrar datos.

BIOS: Sistema Básico de Entrada/Salida, Es un programa que controla el funcionamiento de la tarjeta madre y así como los componentes contenidas en ella.

Bit: Es el valor más pequeño que usa una computadora, el cual puede ser uno o cero en un formato digital.

Caché del navegador de Internet: Es una colección de información de las actividades de internet que se almacena temporalmente en la computadora.

Campos magnéticos: Es el fluido de la corriente eléctrica que fluye por un medio, el cual está presente en dispositivos de almacenamiento magnético que representan los dígitos binarios para leer, grabar información.

Centro computarizado: Son lugares donde existen equipos, programa y personal que se dedican a procesar datos de manera coordinada.

Checksum: Es un método con el objetivo de detectar que el proceso de copiado de disco se haya realizado de manera correcta garantizando la integridad de los datos, calculando el valor recibido con el valor enviado durante la transferencia de la información.

Clonación del dispositivo o bit por bit: Se trata de un copiado donde se asegura que desde la mínima cantidad de bit haya sido clonado de manera completa no obviando el mínimo detalle.

Cookies: Galleta informática, Es un registro que se guarda en el navegador de internet y es enviada por un sitio web con el objetivo de almacenar información sobre el usuario para que este al introducirse en la página web más de una ves no tenga la necesidad de introducirla de nuevo.

Conexión USB: Es el tipo de conexión capaz de comunicar, conectar y proveer de energía a los dispositivos USB.

CPU: Unidad Central de Procesamiento, es la parte central de un computador que se encarga de realizar los cálculos e interpretar las instrucciones de los programas y controlar los datos.

Crack de software: Es una clave o registro que tiene como objetivo cambiar el comportamiento de un software original y diseñado sin autorización del creador del programa.

Criminales de cuello blanco: Personas que cometen un delito en virtud de su status social, con la creencia que su status los ampara de dichos crímenes.

Datos volátiles: Es la información que solo existe en el computador cuando la computadora está encendida, una vez apagado o reiniciado el equipo se borran.

Disco GPT: Es un disco físico el cual posee una tabla de partición GUID (identificador globalmente único).

Dispositivos de USB: Universal serial bus, es un aparato que se utiliza para almacenar información digital el cual utiliza una memoria flash.

ERP: El sistema de planificación de recursos empresariales denominado ERP, siglas del nombre en inglés Enterprise Resource Planning, surgió de la necesidad de englobar todos los datos referentes a la totalidad de la cadena de producción de las empresas, con el fin de brindar información confiable en tiempo real.

Firma electrónica: Es el proceso que permite relacionar e identificar a un individuo o equipo informático durante la transmisión de documentos o mensajes electrónicos.

Hardware: Es todo aquello físico de la computadora que podemos ver y tocar.

Hardware o software bloqueador de escritura: Es un dispositivo ya sea físico o digital que se utiliza durante el proceso de adquisición de datos que no permite la escritura o modificación de los datos en un archivo que se desea proteger durante investigación.

Infraestructuras tecnológicas: Es la agrupación de dispositivos de hardware y software que integran una empresa con el objetivo de optimizar los recursos y aumentar las respuestas de demandas ante el mercado de usuarios.

Instrucciones de programación: Son órdenes diseñadas para que la computadora ejecute una orientación en particular deseada.

Ip: Es un número o identificación única que se le asigna a una computadora conectada a una red que se ejecuta en el Protocolo de internet.

Ip dinámica de la computadora: Es un número ip que se le asigna a un dispositivo durante cierto tiempo y este puede cambiar de un equipo a otro. Por lo general es asignado por los proveedores de internet mediante el DHCP (protocolo de configuración dinámica del host).

Información sensible. Datos claves (relativos a la misión) del negocio que, de comprometerse o exponerse, pueden alterar el funcionamiento y viabilidad de los procesos de la organización. Ejemplo: Estrategias de mercadeo, listado de clientes, claves de acceso a aplicaciones del negocio, etcétera.

Kit de herramienta de cómputo forense: Es un conjunto de artefactos o dispositivos que tanto hardware y software que ayudan al informático forense a realizar una investigación de manera más rápida y con mejores resultados.

Legitimidad: Es un término que hace referencia a que un objeto o situación se encuentra es un estado legitimo es decir que cumple con las leyes establecidas en la sociedad.

Lógica interna: Hace referencia a la lógica matemática aplicada en la computadora utilizada para realizar análisis y optimizar los recursos del computador.

Logs: Es un registro de eventos del sistema, estos hacen referencia a los registros de datos o información relacionado con lo que sucede en un dispositivo o programa cualquiera.

Manual de operación: Son instrucciones escritas en un documento formal que describen de manera detallada de cómo realizar una actividad o proceso en una empresa o programa desarrollado.

Memoria de computadora o RAM: Es un dispositivo importante dentro del funcionamiento de un computador ya que es la parte donde todos los datos o aplicaciones son almacenados.

Memoria flash: Es un tipo de memoria de lectura y escritura de múltiples posiciones de memoria en la misma operación, debido a su tecnología funciona a mayor velocidad comparada a las otras memorias.

Memoria volátil: Se hace referencia aquella parte de la computadora que almacena la información y si en un dado momento en el tiempo el fluido de energía eléctrica es cortado, dicha información se perdería.

Montaje del dispositivo: Es la acción que se realiza al momento de conectar un nuevo hardware al computador y para poder acceder a ellos se utiliza un directorio que permite entrar a dicho dispositivo.

Particiones del dispositivo: Es el espacio de uso que se le asigna en un disco duro; que se realiza en vista que el sistema operativo no trabaja con unidades físicas directamente sino con unidades lógicas.

Particiones BSD: Distribución de software Berkeley, es un tipo de partición basado en el sistema de operativo UNIX desarrollada en la Universidad de California en Berkeley para poder cumplir sus necesidades modificando el código fuente.

Particiones DOS: Sistema operativo de disco, se basa en la primera familia de sistemas operativos creados por Microsoft, original mente para primeras computadoras IBM PC.

Particiones MAC: Tipo de particiones creada por Apple para sus computadoras Mac Os tal como Mac Os Plus.

Particiones Linux: Particiones utilizadas para sistemas de ficheros Ext2, Ext3, Ext4 para sistemas operativos Linux.

Proceso judicial: Es un proceso que se realiza para hacer ejercer el derecho de las personas con el debido respeto y sus garantías establecidas en la constitución política de cada país.

Programas o software: Es la parte de la computadora que no se puede tocar, además es el conjunto de instrucciones que sirven para el hardware interactúe con el sistema.

Protocolo Ip: Es un protocolo que comunica datos a través de una red de paquetes de datos.

Protocolos de revisión: Es un conjunto de reglas, procesos y disposiciones legales establecidos en una empresa que rigen un procedimiento de verificación a seguir.

Puerto tcp: Protocolo control de transporte, éste tipo de puerto garantiza que la transferencia de flujo de bits se envíe de forma fiable, el propio protocolo se encarga de la gestión de los paquetes de datos durante la transferencia.

Puerto udp: Protocolo de diagrama de usuarios, este tipo de puerto suministra un transporte de datos no confiable ya que este envía mucha cantidad de datos lo cual no agrega toda la información.

Pulsos electrónicos: Son pulsos electromagnéticos que generan un voltaje ya sea alto 1 o bajo 0.

Pyme: Pequeña y mediana empresa, nombre que se le da a las empresas formadas por personas emprendedoras y que producen y ayudan a la economía del país.

Rootkits: Programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

Scripting: Lenguaje guion, es un conjunto de instrucciones de programación pequeño que se utiliza para automatizar algunas tareas.

Servidores: Es una computadora que forma parte de una red, administra el funcionamiento y da servicios a otras computadoras llamadas clientes.

Simulación: Es la acción de comprobar una hipótesis mediante el uso de modelos para lograr ver su comportamiento y posteriormente aplicarlo en la vida real.

Sistema Linux: Es un conjunto de programas que administra los recursos del computador y controla su funcionamiento bajo la plataforma Unix.

Sistemas de información: Es una agrupación de objetos que interactúan entre sí que permiten que la información éste disponible para satisfacer las necesidades en una empresa. Este consta de recursos de cómputo que facilitan el manejo y entendimiento de la información de parte de los usuarios.

Sistema operativo Conjunto de procesos requeridos para administrar los recursos disponibles en un sistema de cómputo como la memoria, los periféricos (impresoras, CD-Rom, zip drives, etc.), los dispositivos de comunicaciones (tarjetas de red, puerto serial, puerto paralelo, etc.) y los medios de almacenamiento. Ejemplos: Windows 95/98, Windows NT/2000/XP, UNIX y Linux.

Software de cifrado de datos: Es un programa que transforma la información legible mediante un algoritmo (conjunto de instrucciones que realiza una función dada) en información ilegible llamado secreto o criptograma.

Unidad almacenamiento masivo: Es un dispositivo electrónico en el cual se guarda durante mucho tiempo información creada por los usuarios.

Unix: Es el núcleo de un sistema operativo multiusuario y multitarea desarrollado en 1969.

Tarjeta gráfica: Es una tarjeta de expansión de una computadora, la cual se encarga de recibir la información proveniente del CPU y lograr procesarla y transmitirla mediante cualquier dispositivo de salida ya sea monitor, Tablet, televisor, etc.

Tarjeta de red: Es una tarjeta de expansión de una computadora la cual permite la comunicación y conexión de varias computadoras o cualquier otro dispositivo entre sí, estableciendo una red por medio del uso de dicha tarjeta.

Virus informático: Es un conjunto de instrucciones creadas de manera maliciosa para alterar el comportamiento normal del funcionamiento de un computador sin permiso o conocimiento del usuario.

Wireless Application Protocol (WAP): Es una regla segura que permite al usuario poseer información de forma instantánea a través de dispositivos inalámbricos tales como teléfonos móviles, tablets etc.

Bibliografía

Periódico el nuevo diario de Nicaragua 12 de noviembre de 2013, Sección Política, CSE y Telcor respaldan reforma a Constitución.

Periódico la prensa de Nicaragua 06 de noviembre de 2013, Sección Ámbitos, Telcor: en las redes sociales hay gente haciendo “cosas que no deben”.

Best Practices for Computer Forensics; “Scientific Working Group on Digital Evidence”; Version 1.0; Noviembre 2004
https://www.swgde.org/documents/Archived%20Documents/2004-1115%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20v1.0

DELITOS INFORMATICOS, Colección Seguridad de la Información, Lima, Mayo del 2001
http://hospitalbarranca.gob.pe/estadistica/files/normas/delitosinfromaticos.pdf

http://www.datarecovercenter.co/Servicios/Informatica-Forense/Auditoria-e-Investigacion-Forense/Historia-de-la-Informatica-Forense

https://sites.google.com/site/sykrayolab/historia-de-la-informatica-forense

http://ditumbeschullepe.galeon.com/aficiones2454509.html

http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp

http://www.slideshare.net/Fundaciocatic/analisis-forense-busca-de-evidencias

http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

The Sleuth Kit.
http://www.sleuthkit.org/sleuthkit/index.php

Autopsy Forensics Browser.
http://www.sleuthkit.org/autopsy/index.php.

Vmware workstation software.
http://www.vmware.com

Encase Forensic, de Guidance Software.
http://www.guidancesoftware.com

Panda Antivirus + Antispyware
http://www.pandasoftware.com