UNIVERSIDAD MICHOACANA DE
SAN NICOLAS DE HIDALGO

FACULTAD DE CONTADURIA Y
CIENCIAS ADMINISTRATIVAS

RECUPERACION DE DATOS MEDIANTE LA INFORMATICA FORENSE

TESIS

PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA ADMINISTRATIVA

PRESENTA

IRVING RICARDO GUTIÉRREZ VILLEGAS

ASESOR

M.A. BRUNO RAMOS ORTIZ

MORELIA MICHOACAN, OCTUBRE DEL 2020

RESUMEN

El presente trabajo habla sobre la informática forense, enfocada en la Recuperación de datos a trasvés de la Informática forense, comenzando por los conceptos básicos como el de Informática Forense que es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal. Teniendo como objetivo explicar el estado actual de un artefacto digital.
Existe un número de principios básicos que son necesarios al examinar un computador o un cadáver. Como son: Evitar la contaminación, Actuar metódicamente y Controlar la cadena de evidencia.
La informática forense no es una sola actividad, utiliza muchas disciplinas. Involucra la aplicación de tecnología de la información para la búsqueda de la evidencia digital y comprende, entre otras, las siguientes tres actividades:
Análisis de soportes y dispositivos electrónicos.
Análisis de la comunicación de datos.

Se ven 3 perspectivas: la del intruso, esta es una forma de aproximarse a ver como estos piensan, actúan y operan, para desarrollar el olfato y la pericia para predecir y analizar los posibles rastros y acciones que se desarrollen en medios tecnológicos. Algunos ejemplos de los intrusos serian, Hacker, Cracker, Phreaker, Delincuente informático.

el administrador, en este rol el Informático Forense debe comprender los conceptos de protección y control de tecnologías de la información, no solo para detallar las medidas tecnológicas de seguridad y control configuradas, sino para identificar y analizar las diferentes formas de alerta, detección, registro y monitoreo que la infraestructura tiene definidas para prevenir algún tipo de incursión no autorizada.

el investigador, es un profesional científico, formal en los procedimientos y el uso de las herramientas disponibles, que no busca otra cosa que las relaciones y causales que pudieron llevar a materializar el caso.

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización y como objetivo a proteger, son tres elementos: Información, Equipos que la soportan y Usuarios.

El derecho informático Es un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática.

Se muestran algunos artículos dedicados a los delitos informáticos.

Y a través del marco metodológico encontraran información como el correcto uso de los procesos como la metodología para el análisis forense, el cual muestra las fases y el buen ejercicio para el correcto análisis.

En el esquema del proceso de respuesta ante incidentes, muestra el proceso de respuesta ante algún incidente.
Y se dan a conocer los pasos a seguir para un adecuado inicio de la informática forense, con algún dispositivo a analizar.

ABSTRACT

Y por último algunas recomendaciones para proteger contra virus, gusanos y troyanos.
This paper talks about forensic computing, focused on data recovery through forensic computing, starting with basic concepts such as forensic computing, which is the application of specialized scientific and analytical techniques to technological infrastructures that allow to identify, preserve, analyze and present valid data within a legal process. Aiming to explain the current state of a digital artifact.
There are a number of basic principles that are necessary when examining a computer or a corpse. As they are: Avoid contamination, Act methodically and Control the chain of evidence.
Computer forensics is not a single activity, it uses many disciplines. It involves the application of information technology to search for digital evidence and comprises, among others, the following three activities:
Analysis of electronic media and devices.
Analysis of data communication.

3 perspectives are seen: that of the intruder, this is a way of approaching to see how they think, act and operate, to develop the sense of smell and the skill to predict and analyze the possible traces and actions that are developed in technological means. Some examples of the intruders would be, Hacker, Cracker, Phreaker, Computer criminal.

The administrator, in this role, the Computer Forensic must understand the concepts of protection and control of information technologies, not only to detail the technological security and control measures configured, but to identify and analyze the different forms of alert, detection, registration and monitoring that the infrastructure has defined to prevent any type of unauthorized incursion.

The researcher is a scientific professional, formal in the procedures and the use of the available tools, who does not look for anything other than the relationships and causes that could lead to the case materializing.

Computer security consists of ensuring that the resources of the information system (computer material or programs) of an organization are used in the way that was decided and that access to the information contained there, as well as its modification is only possible to people. that are accredited and within the limits of their authorization and as an objective to protect, are three elements: Information, Equipment that supports it and Users.

Computer law It is a set of principles and rules that regulate the legal effects arising from the interrelation between law and computer science.

Some articles dedicated to cybercrime are shown.

And through the methodological framework you will find information such as the correct use of processes such as the methodology for forensic analysis, which shows the phases and the proper exercise for the correct analysis.

In the incident response process outline, show the incident response process.

And the steps to follow for a proper start of forensic computing are disclosed, with a device to be analyzed.
And finally, some recommendations to protect against viruses, worms and Trojans.

PALABRAS CLAVE: Seguridad informática, Informática Forense, Evidencia Digital, Información, Delitos Informaticos

Tabla de contenido

INTRODUCCIÓN

Hoy en día vivimos en un mundo sumergido en un constante y acelerado devenir, por lo que somos testigos de los avances que las tecnologías de comunicación y computación han tenido, y esto lo podemos constatar en la gran cantidad de personas que hace uso de una de sus aplicaciones llamada Internet.

Internet ha venido revolucionando la vida del hombre, lo que le ha provocado el cambio en materia de legislación en muchos países esto debido al nacimiento de nuevas formas de delinquir, ha dado paso al nacimiento de nuevas ciencias como la informática forense de la cual se desprenden la computación forense y redes forenses.

El problema que existe en México, es que se sabe muy poco al respecto, tendríamos que modificar desde la legislación, preparar al personal para que lleve a cabo esta labor de una manera eficiente. Y adoptando esta forma de vida para obtener todas las ventajas que propiciaría el tener el control al respecto.

Ya que la mayor cantidad de los delitos informáticos son cometidos dentro de las mismas empresas, como el acceso no autorizado a información, espionaje industrial o comercial, atentar contra la privacidad de las personas, robo de información, suplantación de identidad, acosos vía mail, entre los más importantes.

Los motivos por los que no existe denuncia en este tipo de casos son: Inicialmente se desconoce que estas actividades pueden ser probadas y denunciadas, porque no tienen a quien acudir y por no saben cómo tratar este tipo asuntos el personal legal y de sistemas de sus instituciones.

Todo delito informático es investigable y probable, muchos quienes cometen este tipo de delitos tienen una idea errada, piensan que su escudo más grande es una computadora, un correo electrónico, un foro de internet, un chat, etc.

A raíz del auge delictivo informático, nacieron los llamados detectives digitales o policía cibernética que usando técnicas de informática forense pueden contrarrestar y dar con los causantes del delito.

Estos detectives también utilizan estas técnicas para recuperar información dentro de las empresas u organizaciones, dicha información que simplemente se perdió por el daño de algún equipo o a causa de robo.

En nuestro país, vemos que nos va ganado terreno el cibercrimen organizado. Una de las más grandes vías de comunicación que poseemos como lo es el Internet esta desprotegida totalmente.

Pocos conocen de Informática forense, que es una disciplina de las ciencias forenses, que procura descubrir o interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso.

El presente proyecto ofrecerá información referente al tema de informática forense, así como la metodología a seguir por el informático forense en la realización de su labor.

CAPÍTULO I. PROTOCOLO DE INVESTIGACIÓN

RECUPERACIÓN DE DATOS MEDIANTE SOFTWARE FORENSE

Introducción.

En la actualidad se han visto de muchas maneras que las empresas o instituciones a nivel mundial han sido víctimas de varios delitos informáticos en el que se demuestra que en realidad se debería realizar estudios que garanticen seguridad y confiabilidad de la información que se encuentran almacenado en dispositivos de almacenamiento como son discos duros, CD, pendrives, memorias extraíbles entre otros.

México no está exento de este problema ya que de la misma manera han existido varios casos de fraudes informáticos. Esta tesis está realizada en base a datos reales del tema, consiste en un estudio de herramientas de análisis forense y recuperación de información en los dispositivos de almacenamiento, tomando en cuenta que la investigación es de mucha importancia porque se analizará y demostrará que diferentes herramientas de análisis forense ayudará a recuperar información, sean cual fueren las causas de dichas perdidas como robo, alteración o borrado de información que se encuentran almacenados en diferentes dispositivos de almacenamiento. El trabajo investigativo realizado tendrá impacto en el desarrollo tanto de laboratoristas, estudiantes, docentes ya que servirá de soporte científico y sobre todo que sirva para solucionar el problema.

Objetivos.

OBJETIVO GENERAL
Realizar un estudio referente a la ciencia de la informática forense y confirmar el problema planteado, mediante un método que permita una mayor eficacia.

OBJETIVOS ESPECÍFICOS
Definir el papel del profesionista informático forense.
Mostrar la metodología y las técnicas de la informática forense.
Exhibir la importancia del trabajo de la informática forense.
Señalar el trabajo de la Legislación Mexicana en informática forense.
La recuperación de información y su importancia.

Justificación.

El presente proyecto se enfoca a la tarea de investigar en que consiste la metodología de la informática forense para la recuperación de la información perdida o robada, cuáles son sus beneficios, su importancia así como los requerimientos de capacitación para los profesionistas, herramientas a usar de la informática forense, así como la legislación existente relacionada con los delitos

informáticos para orientar a las personas sobre la importancia de la seguridad de la información y su manejo.

Cabe mencionar que la información que se pierde puede ser recuperada en un 80 y 90%, mediante la metodología y sus diferentes herramientas.

Hipótesis.

El uso de software forense ofrece hasta un 90% de éxito en la recuperación de información perdida por ataque, intrusión o fallo de equipo de cómputo.

Definición de las variables

Software que se maneja y porcentaje de efectividad.
Recuva: tiene entre un 80 y 90 %
Easy Recovery: tiene entre un 80 y 90 %

Metodología procedimientos que se emplearon.

La metodología desarrollada se divide en cinco fases. Estas son:

1. Identificación
2. Preservación
3. Análisis
4. Documentación y presentación de las pruebas

CAPÍTULO II. MARCO TEÓRICO

II.1 INFORMÁTICA FORENSE

DEFINICIONES

a. Se iniciará con el término computer forensics, cuya traducción por lo general se hace como computación forense. Esta expresión se podría interpretar de dos maneras: (1) disciplina de las ciencias forenses que, considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información de los medios informáticos para establecer los hechos y formular la hipótesis relacionadas con el caso; o (2) como la disciplina científica y especializada que, entendiendo los elementos propios de las tecnologías de los equipos de computación, ofrece un análisis de la información residente dichos equipos.

b. Es una rama de la ciencia forense relacionada con la ley y con las pruebas encontradas en las computadoras y medios de almacenamiento digital, las técnicas de forense son la aplicación de una técnica de investigación metódica para reconstruir una secuencia de eventos.

c. La Informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información. Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

PREGUNTAS SOBRE INFORMÁTICA FORENSE

Sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información.

Consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas.

Su finalidad en una empresa contrata servicios de Informática forense puede perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se han producido.

Las distintas metodologías forenses incluyen la recogida segura de datos de diferentes medios digitales y evidencias digitales, sin alterar los datos de origen. Cada fuente de información se cataloga preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recabadas permiten elaborar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis que en él se barajan a partir de las pruebas recogidas.

Todo el procedimiento debe hacerse tenido en cuenta los requerimientos legales para no vulnerar en ningún momento los derechos de terceros que puedan verse afectados. Ello para que, llegado el caso, las evidencias sean aceptadas por los tribunales y puedan constituir un elemento de prueba fundamental, si se plantea un litigio, para alcanzar un resultado favorable.

OBJETIVOS DE LA INFORMÁTICA FORENSE

El objetivo de la informática forense es explicar el estado actual de un *artefacto digital.* El término artefacto digital puede incluir un sistema de computadoras, un medio de almacenamiento (como un disco duro o CD-ROM), un documento electrónico (por ejemplo, un mensaje de correo electrónico o Imagen JPEG) o incluso una secuencia de paquetes se desplazan a través de una red informática.
La explicación puede ser tan sencilla como "¿qué información está aquí?" y tan detallada como "¿cuál es la secuencia de eventos responsable de la situación actual?"
Hay muchas razones para emplear las técnicas de informática forense:
En casos legales, técnicas forenses se utilizan con frecuencia para analizar los sistemas informáticos pertenecientes a los acusados (en los casos penales) o los litigantes (en los casos civiles).
Para recuperar los datos en el caso de una falla de hardware o software.
Para analizar un sistema después de una pausa-en, por ejemplo, para determinar la forma en que el atacante tuvo acceso y lo que hizo el atacante.
Para reunir pruebas contra un empleado de una organización que desea terminar.
Para obtener información acerca de los sistemas informáticos de trabajo con el propósito de depurarlos, optimizar su rendimiento, o ingeniería inversa.

Para que la empresa tenga conocimiento de lo que sus empleados están haciendo con los equipos y sistemas informáticos, así como son su información e incluso, con fugas de información, robo de propiedad industrial, etc.

Por otro lado, cuando la seguridad de la empresa ya ha sido vulnerada, la informática forense permite recoger rastros probatorios para averiguar, siguiendo las evidencias electrónicas, el origen del ataque (si es una vulneración externa de la seguridad) o las posibles alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno de la empresa para determinar las actividades realizadas desde uno o varios equipos concretos.

Las técnicas de forense digital son el arte de recrear que ha pasado en un dispositivo digital. Existen dos aspectos de estas técnicas:

- Que ha hecho la gente en su computador, esto incluye:
    - La recuperación de archivos eliminados
    - Des encriptación elemental
    - Búsqueda de cierto tipo de archivos
    - Búsqueda de ciertas fases
    - Observación de áreas interesantes del computador
- Que ha hecho un usuario remoto en la computadora de alguien más. Esto incluye:

- Leer archivos de registro
- Reconstruir acciones
- Rastrear el origen

PRINCIPIOS FORENSES

Existe un número de principios básicos que son necesarios al examinar un computador o un cadáver. Estos principios son:

a. Evitar la contaminación
b. Actuar metódicamente
c. Controlar la cadena de evidencia, es decir, conocer quien, cuando y donde ha manipulado la evidencia

a. Evitar la contaminación

En televisión salen los examinadores forenses ataviados con batas blancas y guantes, cogiendo todas las pruebas con pinzas y poniéndolas en bolsa de plástico selladas. Todo ello es para prevenir la “contaminación”.

b. Actuar metódicamente

En cualquier cosa que se haga, si tuvieras que ir a un juicio, necesitarías justificar todas las acciones que hayas tomado. Si actúas de una manera científica y metódica, tomando cuidadosas notas de todo lo que haces y cómo lo haces, esta justificación es mucho más fácil.

c. Cadena de Evidencias

Siempre se debe mantener lo que se denomina la “Cadena de Evidencias”. Esto Significa que, en cualquier momento del tiempo, desde la detección de la evidencia hasta la presentación final en el juicio, puedes justificar quién ha tenido acceso y dónde ha sido. Esto elimina la posibilidad de que alguien haya podido sabotearlo o falsificarlo de alguna manera.

ACTIVIDADES DE LA INFORMÁTICA FORENSE

La informática forense no es una sola actividad, utiliza muchas disciplinas. Involucra la aplicación de tecnología de la información para la búsqueda de la evidencia digital y comprende, entre otras, las siguientes tres actividades:

- **Análisis de soportes y dispositivos electrónicos.**

El análisis de soportes de almacenamiento, como los discos, almacenamientos removibles (por ejemplo, disquetes, discos ZIP, CD, DVD, etc.), requiere una comprensión completa de la estructura física y del funcionamiento de los medios almacenamiento, así como, la forma y la estructura lógica de cómo se almacenan los datos. Mucha de la complejidad de esta actividad se ha simplificado gracias a la aplicación de herramientas de recuperación

de datos muy eficaces e inteligentes. Cuando mencionamos a los "dispositivos electrónicos" nos referimos a cualquier dispositivo capaz de guardar información que posea valor como evidencia, incluyendo teléfonos celulares, agendas y organizadores electrónicos y distintos dispositivos de comunicaciones de red como los routers y hub's.

- **Análisis de la comunicación de datos.**

Este párrafo abarca dos actividades separadas:

- Intrusión en una red de computadoras o mal uso de la misma.
- Interceptación de datos.
- La intrusión en una red de computadoras o mal uso de la misma es la actividad de la informática forense principal cuando el análisis se hace sobre estructuras de esta naturaleza. Consiste en las funciones siguientes:
- Detección de la intrusión.
- Detectar la evidencia, capturarla y preservarla.
- Reconstrucción de la actividad específica o del hecho en sí.

El descubrimiento de la intrusión generalmente involucra la aplicación de software especializado y en algunos casos hardware, para supervisar la comunicación de los datos y conexiones a fin de identificar y aislar un comportamiento potencialmente ilegal.

La captura de la evidencia y su preservación, generalmente tiene lugar después del descubrimiento de una intrusión o un comportamiento anormal, para que la actividad anormal o sospechosa pueda conservarse para el posterior análisis.

La fase final, la reconstrucción de la intrusión o comportamiento anormal, permite un examen completo de todos los datos recogidos durante la captura de la evidencia.

Para llevar a cabo con éxito estas funciones, el investigador forense debe tener experiencia en comunicación de datos y el apoyo de ingenieros de software.

REGLAS DE LA INFORMÁTICA FORENSE

Esencialmente, las reglas de la informática forense son:

Regla 1—Minimizar el Manejo del Original

La aplicación del proceso de la informática forense durante el examen de los datos originales se deberá reducir al mínimo posible. Esto puede considerarse como la regla más importante en la informática forense. Cualquier análisis debe dirigirse de manera tal que minimice la probabilidad de alteración. Cuando sea posible, esto se logra copiando el original y examinando luego los datos duplicados.

La duplicación de evidencia tiene varias ventajas:

Primeramente, asegura que el original no será alterado en caso de un uso incorrecto o inapropiado del proceso que se aplique.

Segundo, le permite al examinador aplicar diferentes técnicas en casos dónde el mejor resultado no está claro.

En tercer lugar, les permite a varios especialistas de informática forense trabajar en los mismos datos, o en partes de los datos, al mismo tiempo.

Aunque hay ventajas al duplicar la evidencia, hay también desventajas.

Primeramente, la duplicación de evidencia debe realizarse de forma tal y con herramientas, que aseguren que el duplicado es una copia perfecta del original. El fracaso para autenticar el duplicado apropiadamente, producirá un cuestionamiento sobre su integridad, lo que lleva inevitablemente a preguntar por la exactitud y fiabilidad del proceso del examen y los resultados logrados. Segundo, duplicando el original, nosotros estamos agregando un paso adicional en el proceso forense. Se requieren más recursos y tiempo extra para facilitar el proceso de duplicación. Más aun, la metodología empleada debe extenderse para incluir el proceso de la duplicación. Finalmente, la restauración de datos duplicados para recrear el ambiente original puede ser difícil.

Regla 2—Documentar los cambios.

Cuando ocurren cambios durante un examen forense, la naturaleza, magnitud y razón para ellos debe documentarse apropiadamente, puede ser necesario durante cualquier examen alterar el original o el duplicado.

Durante el examen forense este punto puede parecer insignificante, pero se vuelve un problema crítico cuando el examinador está presentando sus resultados en un juicio. Aunque la evidencia puede ser legítima, las preguntas acerca de las habilidades del examinador y conocimiento pueden afectar su credibilidad, así como la confiabilidad del proceso empleado.

Regla 3—Cumplir con las Reglas de Evidencia

Para la aplicación o el desarrollo de herramientas y técnicas forenses se deben tener en cuenta las reglas pertinentes de evidencia. Uno de los mandatos fundamentales de informática forense es la necesidad de asegurar que el uso de herramientas y técnicas no disminuye la admisibilidad del producto final. Por consiguiente, es importante asegurar que la manera como son aplicadas las herramientas y técnicas, cumplan con las reglas de evidencia. Otro factor importante en cuanto a la obediencia de las reglas de evidencia es la manera en que la misma se presenta

Regla 4—No exceda su conocimiento

El especialista en informática forense no debe emprender un examen más allá de su nivel de conocimiento y habilidad. Es esencial que el perito sea consciente del límite de su conocimiento y habilidad. Llegado este punto, tiene varias opciones:

- Detener cualquier examen y buscar la ayuda de personal más experimentado;
- Realizar la investigación necesaria para mejorar su propio conocimiento, para que le permita continuar el examen.

CAMPOS DE APLICACIÓN DE LA INFORMÁTICA FORENSE

Prosecución Criminal:
Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

Litigación Civil:
Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.

Investigación de Seguros:
La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

Temas corporativos:
Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

Mantenimiento de la ley:
La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez que se tiene la orden judicial para hacer la búsqueda exhaustiva.

Investigación científica:
Academias y universidades aprovechan las bondades de la informática forense para realizar estudios de seguridad, vigilar la evolución de las amenazas e identificar las tendencias de los ataques informáticos, entre otros.

Usuario final:
Cada vez es más común que las personas usen herramientas de software para recuperar archivos borrados, encriptar documentos y rastrear el origen de un correo electrónico.

LA COMPUTACIÓN FORENSE, UNA PERSPECTIVA DE TRES ROLES (INTRUSO, ADMINISTRADOR E INVESTIGADOR)

- **El rol del intruso**

Esta es una forma de aproximarse a ver como estos piensan, actúan y operan, para desarrollar el olfato y la pericia para predecir y analizar los posibles rastros y acciones que se desarrollen en medios tecnológicos. Conocer la mente y actuar de los atacantes le ofrece al Informático Forense una ventaja estratégica y conceptual sobre el caso que revise, pues se pondrá en el lugar del infractor y tratara de ver como actuaría en un caso semejante.

Características	Intruso Interno	Intruso Externo
Psicológicas	• Generalmente motivados por situación personal o laboral. • Inestabilidad emocional. • Socialmente hábil para recabar información y conocer a sus víctimas.	• Generalmente motivado por reto tecnológico y compensación económica. • Sensación de control y poder sobre un tercero. • Relaciones basadas en conocimiento y logros.
Técnicas	• Conocimiento detallado de fallas de procedimientos y relaciones internas. • Conocedor y estudioso de la organización y su modelo de procesos y controles. • Conocedor de los mecanismos de seguridad y de control.	• Conocedor y estudioso de las fallas tecnológicas de los sistemas operativos. • Conocedor y usuario de técnicas de evasión de investigaciones. • Cuenta con un laboratorio de pruebas para verificar previamente sus acciones.

La mente de los intrusos

Según Furnell, existen diferentes consideraciones para concebir o para clasificar a los atacantes, así como las motivaciones que los mueven a actuar en una situación particular.

Motivaciones	Ciberterroristas	Phreakers	Scripts kiddies	Crackers	Desarrollo de virus	Atacante interno
Reto		X			X	X
Ego		X	X		X	
Espionaje				X	X	X
Ideología	X					
Dinero		X		X	X	X
Venganza	X		X		X	X

Tipos de intrusos

✓ **Hacker**

Hacker es una expresión idiomática inglesa cuya traducción literal al español tiene varios significados, siendo el más popular el atribuido a "una persona contratada para un trabajo rutinario" y que por la naturaleza del mismo su trabajo es tedioso, entregado, hasta se podría maniático.

✓ **Cracker**

Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan

programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en Internet.

- ✓ **Phreaker**

El phreaker es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

- ✓ **Delincuente informático**

Es la persona o grupo de personas que en forma asociada realizan actividades ilegales haciendo uso de las computadoras y en agravio de terceros, en forma local o a través de Internet. También es un delincuente informático el "pirata" que distribuye software sin contar con las licencias de uso proporcionadas por su autor o representantes, pues no solo atenta contra la propiedad intelectual, provocando la fuga de talentos informáticos, se enriquece ilícitamente y es un evasor de impuestos.

Tipos de delitos informáticos

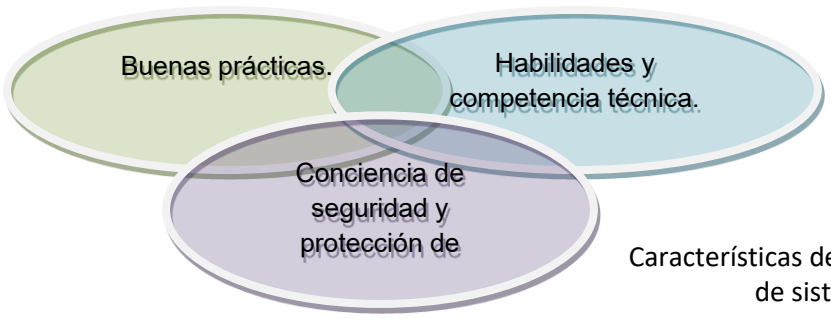
Es habitual encontrar nuevas amenazas para la seguridad informática, los delitos relacionados con la posesión, distribución, falsificación y fraude de información se realizan tras un escritorio, esto muestra un panorama complejo, en el cual los profesionales de las tecnologías de la información y los profesionales de la defensa de la ley deben cooperar y trabajar juntos en la defensa, detección y procesamiento de las personas que utilizan las nuevas tecnologías para realizar delitos informáticos.

Entre los delitos más habituales tenemos:

- ✓ **Protección al menor**: producción, distribución y posesión de pornografía infantil.
- ✓ **Fraude en las comunicaciones**: locutorios telefónicos clandestinos.
- ✓ **Dialers**: modificación oculta del número de teléfono de destino, Producción y distribución de decodificadoras de televisión privada.
- ✓ **Fraudes en Internet**: estafas, subastas ficticias y ventas fraudulentas.
- ✓ **Carding**: uso de tarjetas de crédito ajenas o fraudulentas.
- ✓ **Phising**: redirección mediante correo electrónico a falsas páginas simuladas trucadas (común en las mafias rusas).
- ✓ **Seguridad lógica**: virus, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico. Delitos de injurias, calumnias y amenazas a través del e-mail, news, foros, chats o SMS.
- ✓ **Propiedad intelectual**: piratería de programas de computadora, de música y de productos cinematográficos. Robos de código: como en el caso de los juegos Dark Age of Camelot, y Half-Life 2, o de los sistemas Cisco IOS y Enterasys Dragon IDS.

- **El rol del administrador**

Si bien el rol del intruso es interesante y atractivo, no es posible conocer los detalles de los rastros, si no nos adentramos en la mente del administrador, el profesional de tecnologías de la información a cargo de la administración y control de las maquinas que posiblemente están involucradas. En este rol el Informático Forense debe comprender los conceptos de protección y control de tecnologías de la información, no solo para detallar las medidas tecnológicas de seguridad y control configuradas, sino para identificar y analizar las diferentes formas de alerta, detección, registro y monitoreo que la infraestructura tiene definidas para prevenir algún tipo de incursión no autorizada.

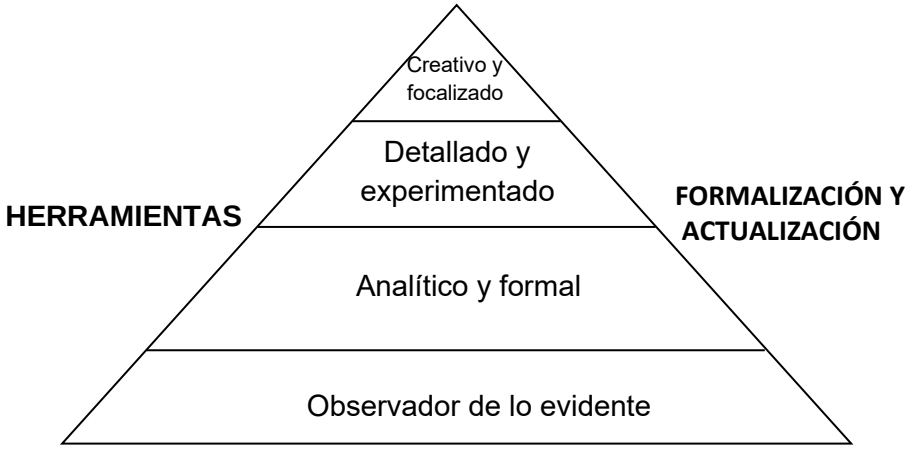


Características del administrador de sistemas

El intruso y el administrador son dos roles complementarios y requeridos dentro de la gestión de la inseguridad de la información, pero se requiere un rol adicional que, con mirada emergente y superior, descubra las relaciones y los móviles de lo ocurrido; siga los procedimientos exigidos y establezca las evidencias requeridas para construir la escena de lo anormal identificado.

- **El rol del investigador**

Este es escéptico de lo obvio, observador, detallista y riguroso. Es un profesional científico, formal en los procedimientos y el uso de las herramientas disponibles, que no busca otra cosa que las relaciones y causales que pudieron llevar a materializar el caso. Por lo general, este perfil se forma en la carrera de criminalista, que actualmente en los países latinoamericanos está confinada a profesionales y personas adscritas a instituciones militares, de policía o de administración de justicia.



El investigador en informática forense examina en detalle los datos, los elementos informáticos o de hardware que se recogieron en la escena del crimen, con el fin de extraer toda la información relevante para el caso, siguiendo para ello procedimientos de aseguramiento de la evidencia, control de los elementos probatorios, herramientas de hardware y software certificadas y las normas y regulaciones pertinentes al análisis en profundidad que debe desarrollar. Todo este trabajo se verá reflejado en informes periciales.

Consideraciones básicas sobre los informes periciales

Siguiendo lo establecido por Babitsky, S. y Mangraviti, Jr, J. (2002), un informe pericial persuasivo, comprensivo y formal debe considerar las pautas siguientes, que son complementarias a las prácticas presentadas anteriormente. En particular, las recomendaciones de los autores buscan darle mayor profundidad, credibilidad y poder al informe que se presenta:

- ✓ No especular o tratar de adivinar cosas.
- ✓ Evitar el uso de universales o absolutos como “siempre”, “nunca”, "para todos los casos".
- ✓ Evitar expresiones que sugieran vaguedad, aspectos equívocos o incertidumbre.
- ✓ Evitar el uso de lenguaje empático, signos de exclamación, uso de formatos, como negrita, itálicas y mayúsculas para enfatizar los hallazgos o las conclusiones.
- ✓ Usar lenguaje preciso sin jerga.
- ✓ Usar un lenguaje seguro, sin adornos literarios y evite las palabras como "se ve cómo", "podría", "aparentemente", "yo creo", “es probable que", entre otras.
- ✓ Definir todo término técnico propio del informe.
- ✓ Usar un lenguaje concreto sobre los hechos, y evite caracterizaciones subjetivas para describir la investigación, los hallazgos y las conclusiones.
- ✓ Explicar cualquier abreviatura utilizada.
- ✓ Evitar lenguaje argumentativo que pueda sugerir que el autor se inclina por un interés particular.
- ✓ Evitar comentarios sobre la credibilidad de los testigos y las pruebas.
- ✓ Mantener presente validar la consistencia de su informe, tanto dentro de su contenido, como su relación con otros casos donde se haya participado.

- ✓ Evitar cualquier sesgo en el informe.
- ✓ Enumerar las líneas del informe para que, en caso de requerirse alguna revisión de los resultados, se remitan de manera rápida al sitio en el mismo.

Estructura base de un informe pericial

1. Encabezado del informe.

Este encabezado identifica, de manera clara y concreta, qué se requiere hacer, quiénes participan, la identificación del caso, la clasificación del informe según su nivel de seguridad requerido y los investigadores participantes en el caso.

2. Introducción

En la introducción se detallan los aspectos base del caso que se investiga, basado en el expediente del mismo y en los datos que se ofrecen por parte bien sea de la fiscalía o de la defensa. En esta sección se describen la conducta que se investiga y los alcances de la pericia que se adelanta, con el fin de limitar los análisis y exploraciones a lo que se requiere para el caso particular.

3. Validación y verificación de la cadena de custodia

En esta sección se detalla y registra la evidencia con su formato de cadena de custodia, donde se especifica, qué se recibe, de quién, en qué fecha, las características de los objetos, sus marcas y seriales, los nombres de los peritos que reciben, la identificación del caso, entre otros aspectos.

4. Procedimientos de preparación y adecuación de la evidencia recibida

En esta sección se detallan los procedimientos relacionados con los medios informáticos que se tienen para adelantar las copias idénticas del material recibido, los programas informáticos requeridos para esta labor y su posterior análisis, las verificaciones de las copias y los detalles de los análisis que se van a realizar según lo especificado en la introducción.

5. Análisis de la evidencia

En esta sección se adelanta en el análisis detallado de las copias de la evidencia, utilizando los recursos de hardware y software disponibles, los cuales previamente han sido validados y verificados en la tapa anterior, según se requiera para evidenciar la confiabilidad y la calidad de los resultados que van obtener. Es importante, detallar las técnicas utilizada para identificar y extraer la información de los medios entregado para el análisis.

6. Hallazgos o hechos identificados

En esta sección se presenta, luego de la exploración de la evidencia realizada en la sección, lo que se encontró relevante para la materia de investigación. Se presenta tal como se indica en las herramientas, sin análisis ni opiniones al respecto. Esta es la exposición de los resultados de las herramientas que generalmente hablan de archivos, sitios en los medios, calidad de la información recuperada, entre otros aspectos.

7. Conclusiones

En esta sección se presentan los análisis de los hallazgos en el contexto del caso investigado, basados en las formalidades científicas y técnicas que puedan ser validadas por un tercero si así se requiere. Las afirmaciones que se hagan en esta sección deben corresponder a lo que la formalidad técnica establece, a las características de los objetos analizados y los hechos investigados.

8. Firma de los analistas o peritos

Esta sección es tan importante como las anteriores. Corresponde al momento en que el perito refrenda su ejercicio técnico y científico con su rúbrica, haciéndose responsable del contenido de informe y todo lo que allí se encuentre. Se recomienda que este profesional firme con una pluma con tinta especial y de color diferente al negro. Así mismo, es recomendable que el perito o analistas firmen todas las hojas, como medida de confiabilidad sobre el informe, que permita identificar con mayor certeza su informe, por si un tercero quisiera alterar el contenido del mismo, sin autorización.

ANÁLISIS FORENSE INFORMÁTICO

Frecuentemente se publica en internet, noticias y blogs de equipos de seguridad reportes sobre vulnerabilidades, fallas humanas, errores de procedimientos y mala configuración de los equipos y aplicaciones de seguridad que presentan un escenario perfecto para que se lleven a cabo incidentes y delitos informáticos. Los intrusos informáticos que causan cualquier tipo de daño en los equipos poseen diferentes motivaciones, alcances y estrategias que desconciertan a los administradores de los servidores y equipos, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro.

Definiciones asociadas con el análisis forense

Forense en redes. - Comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.

Forense digital. - Una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos.

Gestión de evidencias electrónicas

Evidencia ofrece servicios y asesoría en todas las fases de una investigación digital, con el objetivo de obtener y aportar prueba electrónica en los procesos judiciales:

Primera respuesta a incidentes informáticos

Los primeros instantes posteriores a la detección de un incidente informático son críticos para la preservación de la información digital, que se deteriora y sobrescribe con rapidez. Es importante identificar y asegurar correctamente cualquier fuente de información que pueda ser útil en una investigación posterior.

Definición de objetivos y estrategia

La parte más importante de un proyecto de investigación digital es definir unos objetivos alcanzables, y coordinados con los servicios jurídicos del cliente, y su éxito depende directamente de lo que técnicamente se puede conseguir con un análisis forense y de la calidad de la información digital a analizar.

La amplia experiencia de evidencia en resolución de conflictos donde interviene información digital es una garantía de la elección de la estrategia óptima que respetará la legislación vigente y los objetivos del cliente y de sus servicios jurídicos.

Adquisición de fuentes de información digital

La adquisición de las fuentes a analizar es un paso indispensable previo al análisis, que debe realizarse en unas condiciones específicas para asegurar la integridad de la información y las garantías legales de los resultados. Debe realizarse con herramientas y técnicas específicas en presencia de un fedetario público, que custodiará una copia para evitar la indefensión de la otra parte.

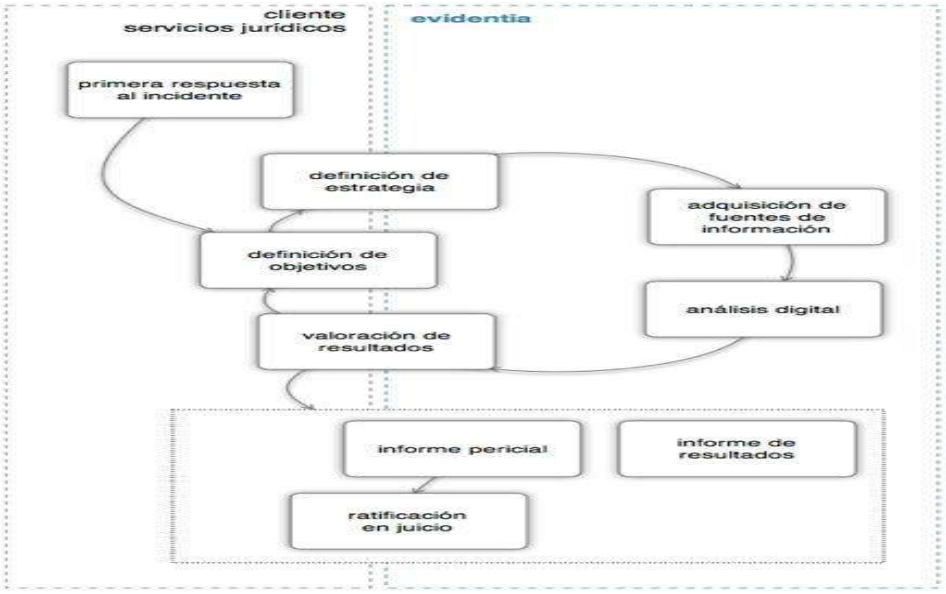
Investigación digital

Los técnicos de evidencia cuentan con herramientas y metodologías de acuerdo con el estado del arte de la informática forense, lo que permite recuperar información borrada u oculta, o analizar correo electrónico respetando la legislación vigente.

Redacción de informes periciales

Las evidencias digitales obtenidas por evidencia pueden utilizarse como medios de prueba en procesos judiciales mediante informes periciales claros y asequibles a perfiles no técnicos, pero que a la vez incluyen toda la información necesaria para hacer reproducibles los resultados.

Ciclo de vida de las evidencias electrónicas



INVESTIGACIÓN DIGITAL

Se puede realizar una investigación digital sobre casi cualquier dispositivo o medio que contenga información digital, por ejemplo:

1. Páginas web, foros de internet
2. Redes sociales (como facebook, twitter, etc.)
3. Correo electrónico
4. Computadoras personales y portátiles
5. Teléfonos móviles, PDA's y smartphones
6. Memorias USB, discos duros externos, CDs, DVDs,...
7. Servidores de empresa
8. Sistemas de almacenamiento corporativos
9. Sistemas de software comerciales o desarrollados propios

Un análisis forense en una investigación digital puede permitir obtener uno o varios de los siguientes resultados:

1. Localizar y extraer documentos respetando los derechos a la intimidad y al secreto de las comunicaciones de las personas implicadas.
2. Determinación de la autoría de un documento o una acción en un entorno digital.
3. Análisis de actividad, o determinación de la cadena de hechos previa o posterior a un suceso en un entorno digital.
4. Recuperación de archivos e información borrada, incluso después de varios formateados y reinstalaciones del sistema.
5. Certificación de información técnica, como procedencia de correos electrónicos o autoría de información publicada en internet.
6. Revelación de información oculta en un sistema digital, accidental o mal intencionadamente.
7. Investigación de hechos y recopilación de información en entornos digitales.

8. Peritajes de programas y sistemas informáticos.

Casos típicos objeto de una investigación digital

Los casos típicos donde un análisis forense digital puede resultar de gran utilidad suelen estar relacionados con conflictos como, por ejemplo:

1. Envíos de amenazas, insultos o información confidencial mediante correo electrónico o publicación en internet
2. Uso malintencionado de los sistemas de la empresa: borrado masivo o sobre escritura de información, sabotaje de los sistemas, modificación no autorizada de páginas web, suplantación de identidad.
3. Fraude: fraude económico o contable, fugas de información, competencia desleal, espionaje empresarial o industrial
4. Uso no autorizado de los privilegios de administración informática
5. Conflictos laborales: bajo rendimiento laboral, uso indebido de los sistemas.
6. Conflictos en proyectos de desarrollo de software o implementación de sistemas informáticos entre cliente y fabricante o instalador.

EVIDENCIA DIGITAL

Es el conjunto de datos en formato binario, esto es comprender los archivos, su contenido o referencias a estos (metadatos) que se encuentren en los soportes físicos o lógicos de un sistema comprometido por un incidente informático.
Fuentes de Evidencia Digital. Algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo, es necesario distinguir entre aparatos electrónicos como los celulares y PDAs y la información digital que estos contengan.

Fuentes de la evidencia digital
Las fuentes de evidencia digital pueden ser clasificadas en tres grandes grupos:

1.-**Sistemas de computación abiertos**, son aquellos que están compuestos de las llamadas computadores personales y todos sus perifericos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tienen la capacidad de guardar gran cantidad de información dentro de los discos duros, lo que los convierte en una gran fuente de evidencia digital.

2.-**Sistemas de comunicación**, estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.

3.-**Sistemas convergentes de computación**, son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

Alberto David Airala, Osvaldo Horacio Rapetti, (2003, Revista de derecho informático. A las puertas de una Nueva Especialización: La Informática forense. No 055) comentan al respecto de la evidencia digital:

1. La identificación de evidencia digital. Es el primer paso en el proceso forense. Sabiendo qué evidencia está presente, dónde y cómo se guarda, es vital determinar qué procesos serán empleados para efectuar su recuperación. Aunque muchas personas piensan que solamente las computadoras personales son el centro de la informática forense, en la realidad el concepto puede extenderse a cualquier dispositivo electrónico que sea capaz de almacenar información, como los teléfonos celulares, las agendas electrónicas y las tarjetas inteligentes.

2. Preservación de la evidencia digital. Es un elemento crítico en el proceso forense. Dado que los datos serán analizados minuciosamente en un juzgado, es indispensable que cualquier examen de los datos electrónicamente guardados se lleve cabo de la manera menos intrusiva posible.
Hay circunstancias dónde los cambios de datos son inevitables, pero es importante que se haga en la menor medida posible. En situaciones dónde el cambio es inevitable, es esencial que la naturaleza y razón del mismo pueda explicarse con detalle.

3. El análisis de la evidencia digital La extracción, procesamiento e interpretación de los datos digitales, se consideran generalmente como los elementos principales de la informática forense. Una vez obtenida, la evidencia digital, normalmente requiere de un proceso, antes que pueda ser comprendida por las personas. Por ejemplo, cuando se tiene la imagen de un disco, los datos contenidos dentro de la misma requieren un proceso (conversión) para que una persona los pueda interpretar.

4. La presentación de evidencia digital. Esto incluye la manera formal de la presentación, la especialización y calificaciones del perito y la credibilidad de los procesos que empleó para producir la evidencia que se está presentando ante el juzgado, árbitro o mediador que interviene.
El rasgo distintivo de la informática forense, que la diferencia de cualquier otra área de la tecnología de información, es el requisito que el resultado final debe derivarse de un proceso que sea legalmente aceptable.

La evidencia digital puede ser dividida en tres categorías:

1. Registros almacenados en el equipo de tecnología informática (P.e. correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.)
2. Registros generados por los equipos de tecnología informática (registros de auditoria, registros de transacciones, registros de eventos, etc.)
3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática. (Hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.).

Características de la evidencia digital

La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad:
1. Es volátil

2. Es anónima
3. Es duplicable
4. Es alterable y modificable
5. Es eliminable.

	LICENCIA	IMAGEN	CONTROL INTEGRIDAD	ANÁLISIS	ADMON CASO
ENCASE	si	si	si	si	si
FORENSIC TOOLKIT	si	si	si	si	si
WINHEX (Forensic edition)	si	si	si	si	si

Herramientas para la recolección de evidencia

El uso de Herramientas sofisticadas se hace necesario debido a:

1. La gran cantidad de datos que pueden estar almacenados en un computador.
2. La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
3. La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
4. Limitaciones de tiempo para analizar toda la información.
5. Facilidad para borrar archivos de computadores.
6. Mecanismos de encriptación, o de contraseñas.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas para conocimiento general, que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática:

Si bien las herramientas detalladas anteriormente son licenciadas y sus precios oscilan entre los 600 y los 5000 dólares, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código abierto.

Estás últimas a pesar de que son utilizadas con frecuencia como estrategia de validación en el uso de otras herramientas, vienen haciendo una importante carrera en la práctica de la informática forense, con lo cual no se descarta en un futuro próximo que éstas estén compitiendo mano a mano con las licenciadas mencionadas anteriormente.

El equipo de seguridad también debe contar con un conjunto de utilitarios que permitan dar una oportuna atención a incidentes que pudieran presentarse, en esta sección se presentan algunas herramientas que serán de gran ayuda y que se las encontrar fácilmente en internet.

Herramientas para el monitoreo y/o control de computadoras

Algunas veces se necesita información sobre el uso de las computadoras, por lo tanto, existen herramientas que monitorean el uso de los computadores para poder recolectar información. Existen algunos programas simples como *keyloggers* o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente.

- **KeyLogger**

Es un ejemplo de herramientas que caen en esta categoría. Es una herramienta que puede ser útil cuando se quiere comprobar actividad sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por *e-mail*. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

- **Herramientas de Marcado de documentos**

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente. El foco de la seguridad está centrado en la prevención de ataques. Algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes.

- **Técnicas forenses en una máquina individual**

Esta es probablemente la parte más común en las técnicas de forense digital. El examinador forense puede estar buscando evidencia de fraude, como hojas financieras dispersas, evidencia de comunicación con alguien más, e-mail o libretas de direcciones o evidencia de una naturaleza particular, como imágenes pornográficas. En los discos duros, se puede buscar tanto en los archivos del usuario como en archivos temporales y en caches. Esto permite al examinador forense reconstruir las acciones que el usuario ha llevado a cabo, a que archivos han tenido acceso, y más.

Hay muchos niveles a los que puede ser examinado un disco duro, existen utilidades que por ejemplo, observar que contenía un disco antes de una formateada. Muchos de los archivos que se detectan no pueden ser leídos inmediatamente, muchos programas tienen sus propios formatos de archivo; sin embargo, también existen utilidades que permiten saber cuál tipo de archivo es.

- **Técnicas forenses en una red**

Las técnicas forenses en una red se usan para saber dónde se localiza un computador y para probar si un archivo particular fue enviado desde un computador particular. Estas técnicas son muy complicadas, pero se puede investigar utilizando dos herramientas básicas:

- Registros de firewalls
- Encabezados de correo

- **Post-Mortem**

He aquí la palabra que encauza el título de nuestro artículo, el análisis post-mortem se realiza mayoritariamente para la recuperación de datos con los que poder trabajar posteriormente, obviamente para no tener que acudir a este recurso se aconsejan las copias de seguridad periódicas.

Se puede decir que un disco duro ha "muerto" cuando su parte mecánica interna no funciona correctamente o cuando se quema, moja, deforma, rompe, etc. Es decir, deja de ser operativo.

Cuando esto sucede no hay más que una solución posible, y esa es el análisis post-mortem. Para ello se lleva a cabo un volcado completo del soporte digital en una "cámara blanca". Los platos del disco antiguo se extraen y se insertan en un nuevo conjunto mecánico para su correcta lectura de datos.

- **Hardware**

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se han diseñado varias herramientas como DIBS las cuales son las que nos permiten poder recuperar la información sin alterar los datos. Pero seguimos teniendo el inconveniente de que cuando encendemos la computadora se modifican los registros de la misma.

Destrucción de la evidencia.

Este método busca modificar físicamente el objeto que contiene la evidencia requerida, de tal forma que no sea posible conseguirla de manera confiable o real. Cuando se habla de eliminar la fuente de la evidencia, significa neutralizar el sistema o la técnica utilizada por el sistema para dejar los rastros; al contrario, esta técnica o proceso no existirá la evidencia y, por tanto, no habrá trazas que seguir en una evidencia.

Si el atacante no ha podido materializar los dos métodos anteriores, puede optar por esconder la evidencia o falsificarla. En la primera, la evidencia se dispersa en el medio que la contiene, se oculta en el mismo, o en el sistema donde se encuentra, limitando los hallazgos del investigador en su proceso. En la segunda, crea o invalida la evidencia residente en el sistema para limitar las conclusiones y análisis que adelante el investigador (ídem).

A manera de resumen y como elemento de análisis, se adjunta un cuadro resumen y analítico de las técnicas antiforenses (cuadro 5.1).

Propósito	Tipo	Nivel de esfuerzos requeridos
Destrucción	Lógica: borrado seguro de datos	Bajo
	Física: desmagnetizador (degaussers)	Alto
Ocultar	Aplicaciones: Criptografia, esteganografia, rootkits	Medio
	Sistemas de archivos: Unidades de datos, metadata, archivos cifrados	Medio
	Medios de almacenamiento: HPA (Host Protected Area)	Alto
Eliminar la fuente	Memoria física	Medio
	Desactivar sistemas de monitoreo	Medio
Falsificar	Sistema de archivos: metadata	Medio
	Sistemas de logs y auditoria	Medio

Complementando la propuesta efectuada por Harris, Garfinkel (Garfinkel 2007, pp. 78-80) detalla algunas técnicas tradicionalmente utilizadas para materializar los métodos previamente presentados, entre los cuales mencionamos la sobreescritura de datos y metadatos, así como la utilización de técnicas criptográficas y esteganográficas.

La sobreescritura de datos y metadatos está asociada con la modificación física de la información residente en los medios de almacenamiento, y sus sistemas de archivo. Es una manera para dejar inconsciente una posible recuperación de información, o una forma de construir entradas falsas en las tablas de asignación de archivos que generen la aparición de archivos inexistentes. Como se puede observar en este segmento, las técnicas anti forenses están evolucionando para confrontar los procedimientos y esfuerzos en informática forense, de tal forma que los atacantes tengan a su favor la duda razonable, y la impunidad haga su aparición en los procesos vinculados con informática. En este contexto, se requiere un compromiso decidido de la industria, de la academia, del gobierno y de todos los actores sociales para abrir nuevas posibilidades de colaboración y construcción conjunta frente a esta realidad de la delincuencia informática organizada, no sólo para enfrentar la amenaza planteada, sino para edificar relaciones de cooperación organizada de largo plazo.

Confiabilidad de las herramientas forenses en informática

Por un lado, las herramientas licenciadas, establecen un nicho de negocio que exige de los investigadores forenses en informática importantes inversiones, tanto en hardware como en software, para darles mayor formalidad y certeza a las partes involucradas en un caso de la evidencia digital.

De otra parte, se encuentran las herramientas forenses de código abierto, las cuales aún son cuestionadas en muchos tribunales y poco se recomiendan como herramientas de uso formal para presentar en audiencias, por su condición de herramientas revisadas y analizadas por una comunidad de la cual poco se conoce de sus pruebas, de las personas que adelantan las mismas, ni del control de los errores. Sin embargo, otra corriente defiende estas herramientas (Carrier 2003) frente a las licenciadas, diciendo que en el mundo de código abierto todo está para el escrutinio de un tercero, que las pruebas se pueden adelantar con mayor confianza que en las abiertas, y que el nivel de confiabilidad es mayor, dado que son muchos “ojos” los que están tratando de mejorarla.

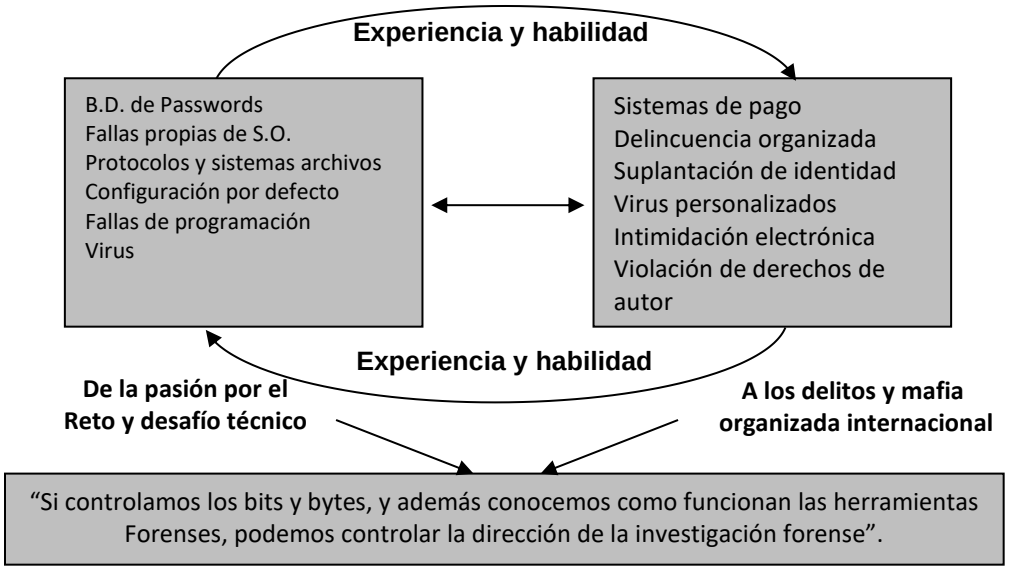
Algunas herramientas licenciadas	VS	Algunas herramientas de código abierto
ENCASE – Guidance software. FORENSIC TOOL KIT – Access data. WINHEX FORENSICS - X - ways. PRODISCOVER TOOLS – Techno-logy pathways. COMPUTER FORENSICS SOFTWARE TOOL SUITE- New		THE SLEUTH KIT. THE CORONER TOOL KIT. DCFL-DD. LIVEVIEW. NETCAT. CRYPTCAT. PASCO.

Herramientas forenses en informática: Licenciadas vs código

El test de Daubert (Dixon y Cill 2001) es un conjunto de reglas extraídas de la sentencia de la Corte Suprema de Justicia Estadounidense, en el caso de Daubert versus Merrell Dow Pharmaceutics, Inc., 509 US. 579 de 1993, donde se clarifican los estándares que los jueces federales deben tener en cuenta a la hora de admitir o no la evidencia entregada por expertos en un caso. Si bien no es un estándar universalmente seguido, sí se ha considerado en muchas iniciativas normativas sobre el tema a nivel internacional. Las reglas que establece la prueba de Daubert son:

- La técnica o el programa utilizados han sido probados en condiciones reales y no sólo en los laboratorios.
- La técnica o el programa han sido sometidos a revisión de pares académicos o científicos y publicaciones especializadas.
- Se conoce el nivel de error potencial del programa o técnica.
- Existe un estándar o un referente para el control y la revisión del programa o técnica.
- La técnica o programa son generalmente aceptados dentro de la comunidad científica relevante a la misma.

En este sentido, los programas o las herramientas de computación forense requieren estudios y análisis detallados para contar con un nivel de adaptación de los mismos, bien sea licenciados o de código abierto. Mientras más pruebas formules se tengan, mayor exposición a la verificación de sus niveles de error, mejores condiciones habrá para el fortalecimiento de las mismas tanto a nivel jurídico en un caso, como a nivel profesional en el uso de la misma.



Evolución de los atacantes

Dificultades del investigador forense

El investigador forense requiere de varias habilidades que no son fáciles de adquirir, es por esto que el usuario normal se encontrará con dificultades como las siguientes:

1. Carencia de software especializado para buscar la información en varios
2. Computadoras.
3. Posible daño de los datos visibles o escondidos, aún sin darse cuenta.
4. Será difícil encontrar toda la información valiosa.
5. Es difícil adquirir la categoría de 'experto' para que el testimonio personal sea válido ante una corte.
6. Los errores cometidos pueden costar caro para la persona o la organización que representa.
7. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.
8. Falta de experiencia para mostrar, reportar y documentar un incidente
9. Computacional.
10. Dificultad para conducir la investigación de manera objetiva.

RETOS Y RIESGOS EMERGENTES PARA LA INFORMÁTICA FORENSE

El cibercrimen, como elemento emergente en el escenario de un mundo interconectado, tiene elementos que los hacen imperceptibles y característico de una "sorpresa predecible".

- La gente piensa que eso es un invento de "los paranoicos" y que, si pasara, no sería tan grave.
- Se tienen datos y noticias relacionados con este tema, pero dispersos y poco difundidos.
- Los gobiernos no tienen tiempo para mirar esto, porque existen otros temas más prioritarios para sus naciones.

Adicionalmente a estos elementos planteados, se suman las falsas alarmas, las cuales crean inmunización y fatiga en los analistas, que disminuyen su atención en los problemas potenciales emergentes, generando una falla estructural en el sistema de inteligencia de las naciones que no permite reconocer una amenaza real cuando esta llega.

La inseguridad informática es una sorpresa predecible, algo con lo cual se convive y, aun así, sus manifestaciones, cada vez más silenciosas y estratégicamente concebidas, no nos alertan sobre los efectos que puede traer al adecuado funcionamiento de las organizaciones (Parker 2007). Esta situación genera una resistencia natural a estar atentos por algo que no podemos evitar, pero que, si podemos intentar comprender, y no sólo identificar.

Por tanto, la formación de investigadores forenses en informática, como esos garantes de la justicia ahora en los medios digitales e informáticos, requiere atención especial para establecer los referentes mínimos del plan de estudios que lleve a la profesionalización de estos nuevos investigadores. A continuación, se presenta algunas iniciativas en este sentido.

II.2. SEGURIDAD INFORMÁTICA

El término **seguridad** proviene de la palabra *securitas* del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia. La seguridad es un estado de ánimo, una sensación, una cualidad intangible. Se puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria.

DEFINICIÓN

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad**: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad**: La información sólo debe ser legible para los autorizados.
- **Disponibilidad**: Debe estar disponible cuando se necesita.
- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

TÉRMINOS RELACIONADOS CON LA SEGURIDAD INFORMÁTICA

- **Activo**: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- **Amenaza**: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Impacto**: medir la consecuencia al materializarse una amenaza.
- **Riesgo**: Es la probabilidad de que suceda la amenaza o evento no deseado
- **Vulnerabilidad**: Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.
- **Ataque**: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Desastre o Contingencia**: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

OBJETIVO DE LA SEGURIDAD INFORMÁTICA

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

Información

Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

Equipos que la soportan.

Software, hardware y organización. También computadores.

Usuarios

Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

Addison Wesley Longman nos dice que es importante considerar altamente los siguientes aspectos:

Seguridad Externa. Consiste en la seguridad física y seguridad de operación. La seguridad física incluye la protección contra desastres y la protección contra intrusos. Los mecanismos de detección son importantes para la seguridad física; los detectores de humo y los sensores de calor pueden proporcionar un aviso temprano en caso de incendio; los detectores de movimiento pueden determinar si ha entrado un intruso en una instalación de cómputo.

Seguridad de operación se compone de las diversas políticas y procedimientos puestos en práctica por los administradores de la instalación de cómputo. La autorización determina qué acceso se otorga a qué entidades.

Seguridad interna. Se ocupa de los diversos controles integrados al equipo y al sistema operativo con el fin de garantizar el funcionamiento confiable y sin corrupción del sistema de cómputo y la integridad de los programas dados.

Vigilancia. Se ocupa de supervisar el sistema y realizar auditorías de él, y de verificar la identidad de los usuarios.

Supervisión de amenazas. Cuando hay supervisión de amenaza los usuarios no pueden obtener acceso directo a los recursos, esto solo pueden tenerlo unos programas llamados programas de vigilancia.

Auditoria. Se utiliza por lo general en sistemas manuales a posteriori, la auditoria en sistemas de cómputo puede implicar un procesamiento inmediato en el computador para revisar las transacciones que se acaban de realizar.

Una bitácora de auditoría. Es un registro permanente de eventos importantes que ocurren en el sistema de cómputo, se produce automáticamente cada vez que sucede un evento así y se almacena en un parea protegida del sistema, si el sistema se ve comprometido, la bitácora de auditoría deberá permanecer intacta.

Protección por contraseña hay tres clases de elementos para la verificación de autenticidad con los cuales puede establecerse la identidad de una persona:

- Algo característico de la persona. Esto incluye huellas dactilares, patrones de voz, fotografías y firmas
- Algo que posee la persona. Esto incluye credenciales, tarjetas de identificación y claves.
- Algo que sabe la persona. Esto incluye contraseñas, combinaciones de candados y el apellido de soltera de la suegra.

La criptografía es el empleo de transformaciones de los datos a fin de hacerlos incomprensibles para todos con excepción de sus usuarios autorizados. El problema de intimidad se ocupa de evitar la extracción no autorizada de información de un canal de comunicación. El problema de verificación de autenticidad se ocupa de evitar que algún enemigo modifique una transmisión o inserte datos falsos en una transmisión. El problema de disputa se ocupa ofrecer al receptor e un mensaje una prueba legal de la identidad del remitente, o sea, el equivalente electrónico de una firma escrita.

Criptoanálisis. Es el proceso de intentar regenerar texto simple a partir de texto cifrado, pero sin conocer la clave de desciframiento; tal es la tarea normal del espía. Si este último, llamado también criptoanalista, no puede obtener el texto simple a partir del texto cifrado (sin clave), el sistema criptográfico será seguro.
Sistema de clave pública Un sistema criptográfico es tan seguro como lo sean sus claves.

Firmas digitales. Los criptosistemas de clave pública ofrecen una forma de llevar a la práctica las firmas digitales. El remitente utiliza la llave privada para crear un mensaje firmado y el receptor utiliza la clave pública del receptor para descifrar el mensaje. El receptor conserva el mensaje firmado para usarlo en la aclaración de disputas.

IMPORTANCIA DE LA SEGURIDAD

Para el INEGI la seguridad es importante por la existencia de personas ajenas a la información, también conocidas como piratas informáticos, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos.
Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70 por ciento de las Violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Los servicios de *ethical hacking*

Ethical Hackers son redes de computadoras y expertos que atacan sistemas informáticos en nombre de sus propietarios, con los mismos métodos que sus homólogos, en busca de posibles fallas de seguridad con la finalidad de brindar un informe de todas las vulnerabilidades encontradas que podrían ser aprovechadas por los piratas informáticos.

Para tales fines los ethical hackers han desarrollado lo que se conoce como pruebas de penetración, (PEN-TEST por sus siglas en inglés).

Tests de intrusión.

Una prueba de penetración es un paso previo natural a todo análisis de fallas de seguridad o riesgo para una organización. A diferencia de un análisis de vulnerabilidades, una prueba de penetración se enfoca en la comprobación y clasificación de las mismas; y no en el impacto que estas tienen sobre la organización.

Tipos de Tests de intrusión.

Las empresas que se dedican a realizar pruebas de penetración, luego de analizar las necesidades del cliente, las enfocan en las siguientes perspectivas:

- **Tests de intrusión con objetivo:** se busca las vulnerabilidades en componentes específicos de los sistemas informáticos que son de mayor importancia para la empresa.
- **Tests de intrusión sin objetivo:** a diferencia de la prueba de penetración con objetivo esta prueba examina la totalidad de los componentes en los sistemas informáticos presentes en la empresa.

Tests de intrusión ciega: se utiliza únicamente la información pública disponible sobre la empresa. Esta prueba de penetración trata de simular los ataques de un ente externo a la empresa.

- **Tests de intrusión informada:** se utiliza información privada, otorgada por la empresa, sobre sus sistemas informáticos. Esta prueba de penetración trata de simular ataques hechos por un ente interno a la empresa y con cierto grado de información privilegiada.
- **Tests de intrusión externa:** se realiza de manera externa a las instalaciones de la empresa. La motivación de esta prueba es evaluar los mecanismos perimetrales de seguridad informática de la empresa.
- **Tests de intrusión interna:** es realizada dentro de las instalaciones de la empresa con el motivo de probar las políticas y los mecanismos internos de seguridad de la empresa.

El resultado de este servicio le brinda al cliente un documento con una lista detallada de las vulnerabilidades encontradas y certificadas (eliminación de falsos positivos). Adicionalmente el documento provee una lista de recomendaciones a aplicar, sobre la cual los responsables de seguridad de la organización pueden apoyar su programa de control.

Seguridad en el Nivel de Red

Implementar la seguridad en el nivel de red tiene muchas ventajas. La primera de todas es que las cabeceras impuestas por los distintos protocolos son menores ya que todos los protocolos de transporte y de aplicación pueden compartir la infraestructura de gestión de claves provista por esta capa. La segunda sería que pocas aplicaciones necesitarían cambios para utilizar la infraestructura de seguridad, mientras que si la seguridad se

implementara en capas superiores cada aplicación o protocolo debería diseñar su propia infraestructura. Esto resultaría en una multiplicación de esfuerzos, además de incrementar la probabilidad de existencia de fallos de seguridad en su diseño y codificación.

ANÁLISIS DE RIESGO INFORMÁTICO

El activo más importante que se posee una organización es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de *barreras y procedimientos* que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Los medios para conseguirlo son:

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Elementos de un análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:
1. Construir un perfil de las amenazas que esté basado en los activos de la organización.
2. Identificación de los activos de la organización.
3. Identificar las amenazas de cada uno de los activos listados.
4. Conocer las prácticas actuales de seguridad
5. Identificar las vulnerabilidades de la organización.

- Recursos humanos
- Recursos técnicos
- Recursos financieros

6. Identificar los requerimientos de seguridad de la organización.
7. Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.
8. Detección de los componentes claves
9. Desarrollar planes y estrategias de seguridad que contengan los siguientes puntos:

- Riesgo para los activos críticos

- Medidas de riesgos
- Estrategias de protección
- Planes para reducir los riesgos.

Técnicas para asegurar el sistema

- Codificar la información: Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.
- Vigilancia de red. Zona desmilitarizada
- Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

Hardware y software

Desde el punto de vista de soluciones tecnológicas, una arquitectura de seguridad lógica puede conformarse (dependiendo de los niveles de seguridad) por: software antivirus, herramientas de respaldo, de monitoreo de la infraestructura de red y enlaces de telecomunicaciones, firewalls, soluciones de autentificación y servicios de seguridad en línea; que informen al usuario sobre los virus más peligrosos y, a través de Internet, enviar la vacuna a todos los nodos de la red empresarial, por mencionar un ejemplo.

Organismos oficiales de seguridad informática

Existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el **CERT/CC** (*Computer Emergency Response Team Coordination Center*) del *SEI* (Software Engineering Institute) de la Carnegie Mellon University el cual es un centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.

Mecanismos de trampa

Privilegios. En algunos sistemas, son demasiados los programas que tienen demasiados privilegios. Esto va contra el principio de menor privilegio.

Confinamiento de programas. Un programa prestado por otro usuario puede actuar como caballo de Troya; podría robar o alterar los archivos de quien lo pidió prestado.

Residuos. Muchas veces el penetrador puede encontrar una lista de contraseñas con sólo examinar un cesto de basura. En ocasiones se dejan residuos en almacenamiento después de ejecutarse una rutina del sistema. La información confidencial siempre deberá reemplazarse o destruirse antes de liberar o desechar el medio (almacenamiento, papel, etcétera) que ocupa. Los desmenuzadores de papel gozan de popularidad para el propósito.

Blindaje. Una corriente en un alambre genera un campo magnético alrededor de éste; los penetradores pueden intervenir de hecho una línea de transmisión o un sistema de cómputo sin hacer contacto físico. El blindaje eléctrico puede servir para evitar estas “instrucciones invisibles”.

Valor del umbral. El propósito de éstos es refrenar intentos repetidos de entrar en el sistema, por ejemplo. Después de un cierto número de intentos de entrada no válidos, ese usuario (o la Terminal desde la cual se está intentando entrar) deberá bloquearse, notificando al administrador del sistema. Muchos sistemas no cuentan con esta característica.

Algunas afirmaciones erróneas comunes acerca de la seguridad

- *Mi sistema no es importante para un cracker*

Esta afirmación se basa en la idea de que no introducir contraseñas seguras en una empresa no entraña riesgos pues ¿quién va a querer obtener información mía? Sin embargo, dado que los métodos de contagio se realizan por medio de programas *automáticos*, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes, etc. Por tanto, abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.

- *Estoy protegido pues no abro archivos que no conozco*

Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.

- *Como tengo antivirus estoy protegido*

En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún.

- *Como dispongo de un firewall no me contagio*

Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un firewall) y otras de conexiones que se realizan (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los firewalls de aplicación (los más usados) no brindan protección suficiente contra el spoofing.

- *Tengo un servidor web cuyo sistema operativo es un Unix actualizado a la fecha*

Puede que esté protegido contra ataques directamente hacia el núcleo, pero si alguna de las aplicaciones web (PHP, Perl, Cpanel, etc.) está desactualizada, un ataque sobre algún script de dicha aplicación puede permitir que el atacante abra una shell y por ende ejecutar comandos en el unix.

II.3 DERECHO INFORMÁTICO

DEFINICIÓN

"Un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática".

CUESTIONES TÉCNICAS Y LEGALES DE LA INFORMÁTICA FORENSE

Para realizar un adecuado análisis de Informática forense se requiere un equipo multidisciplinario que incluya profesionales expertos en derecho de las TI y expertos técnicos en metodología forense. Esto es así porque se trata de garantizar el cumplimiento tanto de los requerimientos jurídicos como los requerimientos técnicos derivados de la metodología forense, cómo actuar mediante la Informática forense ante delitos informáticos e infracciones dentro de la empresa.

La informática y los elementos informáticos pueden constituirse, en ocasiones, como un medio de comisión de una pluralidad de delitos e infracciones. Se abre una nueva realidad muy compleja para cometer actos criminales e infracciones vinculadas a las nuevas tecnologías. La Informática Forense o Forensic detecta las evidencias de la vulneración de la seguridad de los sistemas de información de las empresas y resulta, al tiempo, un método de prevención para evitar este tipo de intrusiones.

REGULACIÓN LEGAL DEL DELITO INFORMÁTICO

Nuestro código penal no recoge una regulación específica de delito informático. Si entendemos como tal, una regulación autónoma de acciones u omisiones penadas por la Ley en las que sirva para la comisión de los delitos un elemento o servicio informático. No obstante, varios de los artículos de la Ley se refieren a distintos tipos delictivos que se pueden cometer con el uso de elementos informáticos, entre otros:

-Delitos relativos a la propiedad intelectual e industrial.
-Delitos relativos al mercado y a los consumidores.
-Estafas.
-Delitos societarios.
-Descubrimiento y revelación secretos.
-Delitos contra el patrimonio y el orden socioeconómico.
-Delitos contra la intimidad y el derecho a la propia imagen.

Puesto que las empresas necesitan los sistemas de información para el desarrollo de sus funciones, son ellas las que más sufren estas acciones y sus consecuencias.

ARTÍCULOS DEDICADOS A LOS DELITOS INFORMÁTICOS

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería está regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa. Como ahí no están

LEGISLACIÓN FEDERAL (VIGENTE AL 1 DE ABRIL DE 2010)

Código penal federal, libro segundo, título noveno. Revelación de secretos y acceso ilícito a sistemas y equipos de informática.
Capítulo ii. Acceso ilícito a sistemas y equipos de informática

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

Artículo 211 bis 2. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
a quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el distrito federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 3. Al que, estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
Al que, estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
A quien, estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el distrito federal. si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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

Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

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

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

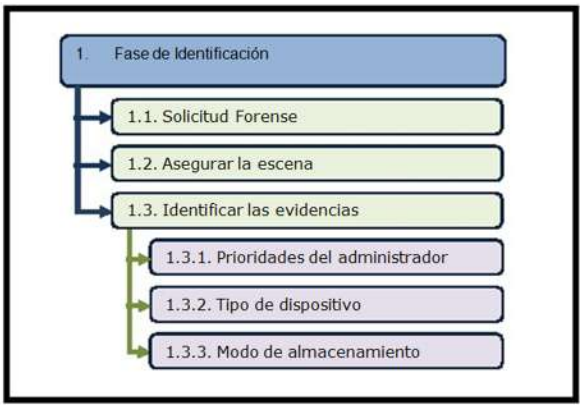
CAPÍTULO III. MARCO METODOLÓGICO

III. 1. METODOLOGÍA PARA EL ANÁLISIS FORENSE

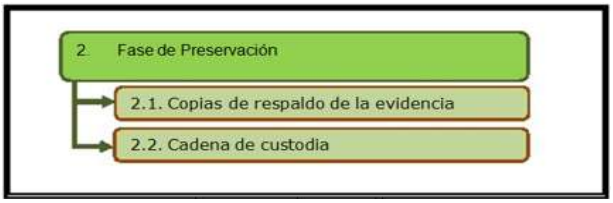
La metodología desarrollada se divide en cuatro fases. Estas son:

1. Identificación
2. Preservación
3. Análisis
4. Documentación y presentación de las pruebas

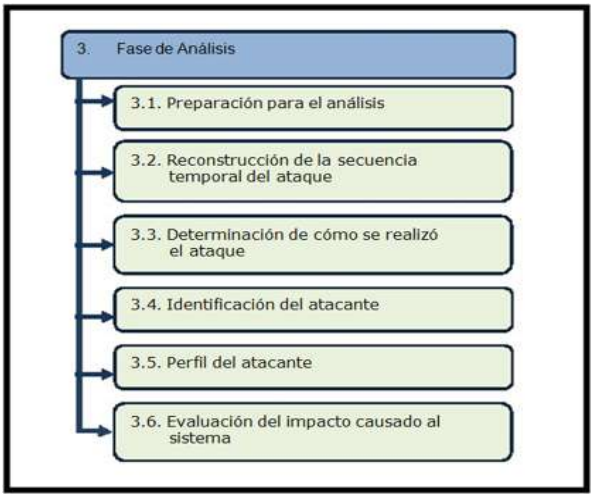
Fase de Identificación



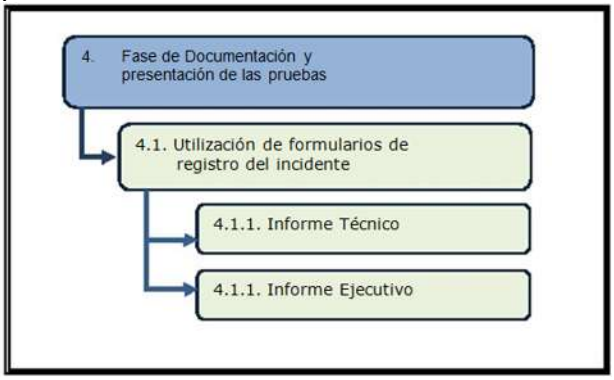
Fase de Preservación



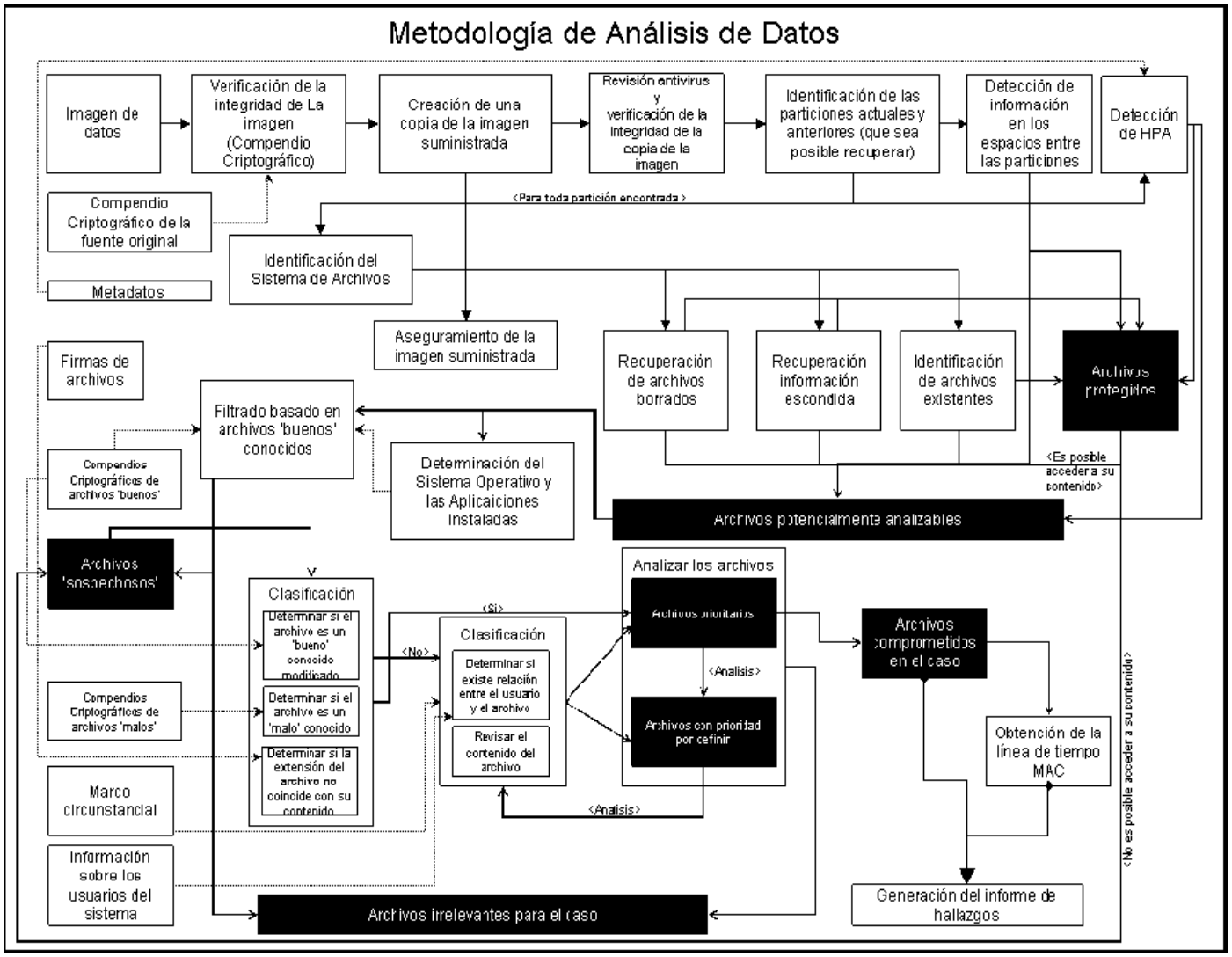
Fase de Análisis



Fase de Documentación y presentación de pruebas



III.2. ESQUEMA DEL PROCESO DE RESPUESTA ANTE INCIDENTES.



III.3. PASOS A SEGUIR DE LA INFORMÁTICA FORENSE

1. Esterilidad de los medios de informáticos de trabajo

Los medios informáticos utilizados por los profesionales en esta área, deben estar certificados de tal manera, que éstos no hayan sido expuestos a variaciones magnéticas, ópticas (láser) o similares, so pena de que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. Un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de las causas de la muerte del paciente.

2. Verificación de las copias en medios informáticos.

Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas. La verificación de éstas debe estar asistida por métodos procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia. Para esto, se sugiere utilizar algoritmos y técnicas de control basadas en firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia.

3. Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados.

El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona externa pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al investigador.

4. Mantenimiento de la cadena de custodia de las evidencias digitales

Este punto es complemento del anterior. La custodia de todos los elementos allegados al caso y en poder del investigador, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

5. Informe y presentación de resultados de los análisis de los medios informáticos.

Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones.

Generalmente existen dos tipos de informes, los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias.

6. Administración del caso realizado

Los investigadores forenses en informática deben prepararse para declarar ante un jurado o juicio, por tanto, es probable que en el curso de la investigación o del caso, lo puedan llamar a declarar en ese instante o mucho tiempo después. Por tanto, el mantener un sistema automatizado de documentación de expedientes de los casos, con una adecuada cuota de seguridad y control, es labor necesaria y suficiente para salvaguardar los resultados de las investigaciones y el debido cuidado, diligencia y previsibilidad del profesional que ha participado en el caso.

7. Auditoria de los procedimientos realizados en la investigación

Finalmente y no menos importante, es recomendable que el profesional investigador mantenga un ejercicio de autoevaluación de sus procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses, de tal manera que el ciclo de calidad: PHVA - Planear, Hacer, Verificar y Actuar, sea una constante que permita incrementar la actual confiabilidad de sus procedimientos y cuestionar sus prácticas y técnicas actuales para el mejoramiento de su ejercicio profesional y la práctica de la disciplina.
Conflictos donde se ve involucrada información digital, incluyendo:

• Amenazas, insultos, envío anónimo de correos electrónicos.
• Robo de cuentas de correo, redes sociales, servicios de internet.
• Publicación de información sin autorización.
• Suplantación de identidad.
• Competencia desleal.
• Fuga de información.
• Espionaje, espionaje industrial.

III.4. PROCEDIMIENTO PARA RECUPERAR DATOS DE DIFERENTES DISPOSITIVOS

Como en todo proceso de análisis existe una metodología a seguir que nos marca los pasos a desarrollar de forma que siempre acabaremos con los cabos bien atados y con unos resultados altamente fiables.

Estudio preliminar:
En el primer paso se planteará la situación en la que nos encontramos: estado físico del disco, causas del posible fallo, sistema operativo, topología de la red, etcétera. Esta es la toma de contacto y de aquí saldrá, a priori, el camino a seguir para llegar a buen puerto.

Adquisición de datos:
En esta fase obtenemos una copia exacta del disco duro a tratar para poder trabajar con ellos en el laboratorio.
Para esta fase la forma más común de realizarlo es mediante el comando `dd' de Linux, que nos realiza un volcado de un disco a otro. Si el disco está dañado físicamente entonces

no tenemos más remedio que recurrir al uso de la cámara blanca. En esta fase ha de estar presente un notario para dar fe de los actos realizados.

Análisis

Procedemos 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.

Presentación

Después de un trabajo duro llega el momento de la entrega de los resultados obtenidos al cliente. Si éste requiere presentar una denuncia judicial aportando como pruebas las conclusiones obtenidas, se le realiza un informe judicial para su exposición ante el juez.

CAPÍTULO IV. DESARROLLO DEL PROYECTO

HERRAMIENTAS DE SOFTWARE

- ✓ **Recuva**

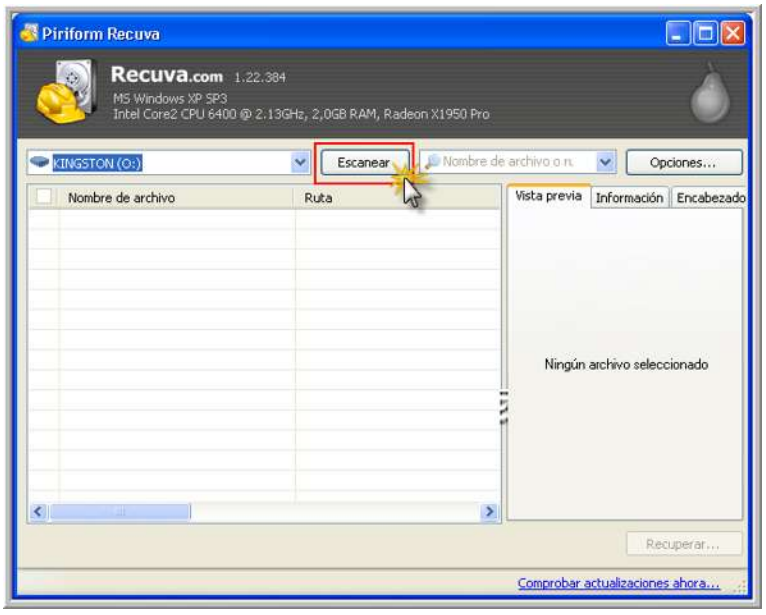
Es un programa de licencia gratuita, desarrollado por Piriform, para Microsoft Windows, fue lanzado el 7 de agosto de 2007, pero la versión más estable fue hasta el 8 de Junio de 2016. Es capaz de restaurar archivos que han sido permanentemente borrados y que han sido marcados por el sistema operativo como espacio libre. El programa también puede ser usado para restaurar archivos borrados de memorias Flash/USB, tarjetas de memoria o reproductores MP3.
Al igual que otros programas de recuperación de datos, Recuva trabaja buscando datos no referenciados, pero si el sistema operativo ha escrito nuevos datos sobre un archivo borrado, la restauración del archivo no será posible.

Arrancamos Recuva y nos saldrá la pantalla del asistente.

Para salir del asistente basta con pulsar el botón cancelar.

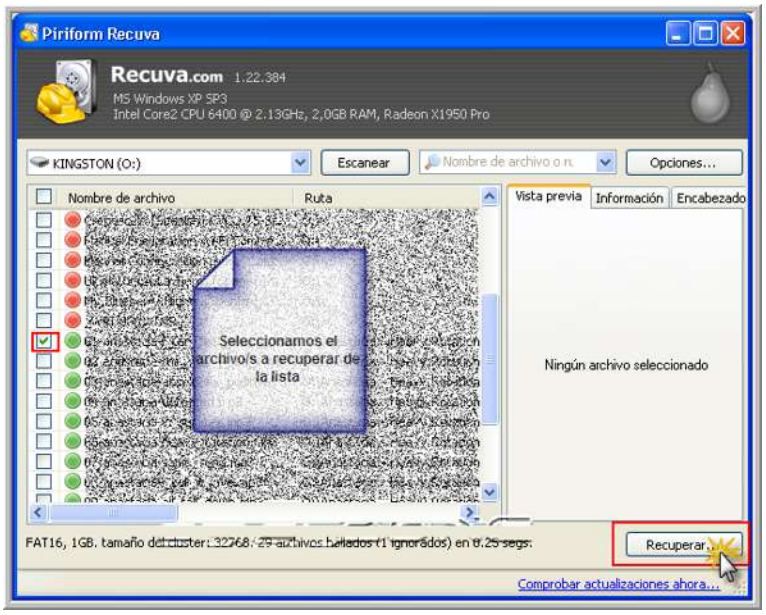
Una vez que salgamos del asistente nos aparecerá la siguiente pantalla:

Para comenzar a buscar los archivos borrados seleccionamos donde se encuentran.



Una vez tenemos seleccionada la ruta donde deber buscar **Recuva** solo tenemos que pulsar Escanear.
A la derecha se encuentra el botón opciones, si pulsamos en él podremos cambiar diferentes preferencia u opciones del programa (no explicare las opciones porque no revierten ninguna dificultad).

Al seleccionar **Escanear** Recuva buscará y nos mostrará todos los archivos que ha encontrado y que se puede intentar recuperar:



Seleccionamos en el listado el archivo o archivos a recuperar. Hay que recordar que si está en rojo se supone que no se puede recuperar o que es difícil de recuperar, aunque muchas veces estos se recuperan sin problemas. Si está en verde el archivo se recupera fácilmente. También podéis ver información referente al archivo seleccionado en el cuadro de la derecha del listado.
Una vez que marquemos el archivo a recuperar pulsamos el botón recuperar.

Seleccionamos el lugar donde queremos que Recuva nos mande los archivos recuperados y listo.

Archivo recuperado !!!!

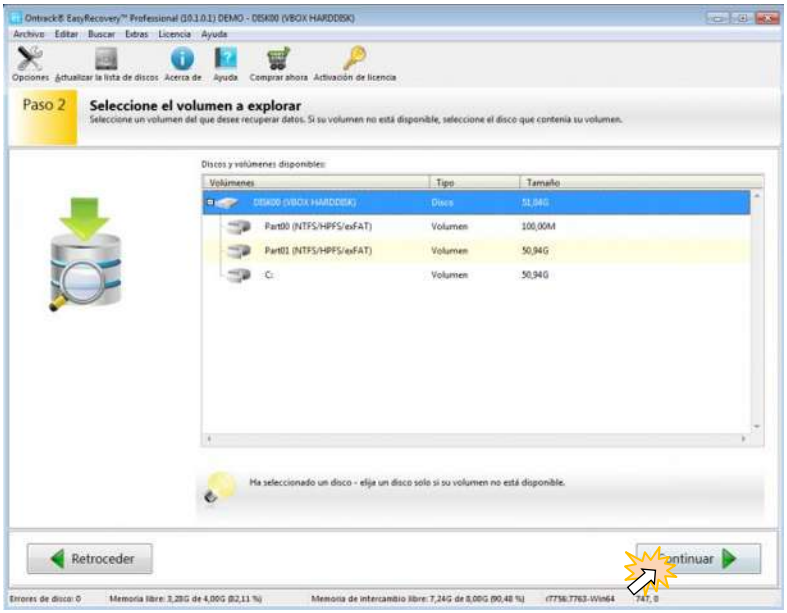
EASY RECOVERY

Es una aplicación de pago desarrollada por Kroll Ontrack,disponible para las plataformas Windows y Mac OSX.

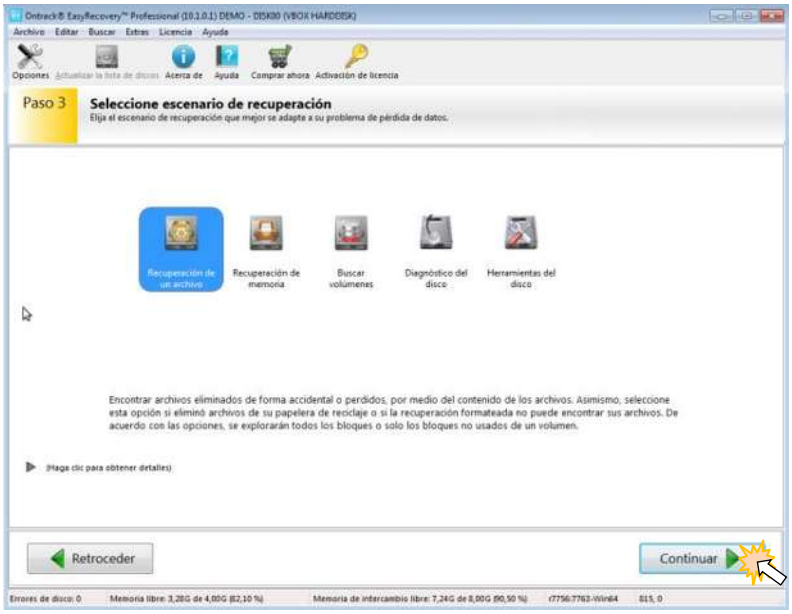
Abrimos el programa, y a continuación podremos ver la pantalla principal del programa.

Para comenzar a buscar los archivos debemos hacer click sobre el botón «continuar» de la parte inferior derecha. El programa nos preguntará sobre el medio desde el que vamos a recuperar los archivos. Como dato a destacar, permite la recuperación de archivos de medios ópticos como CDs y DVDs. En nuestro caso vamos a recuperar archivos desde un disco duro.

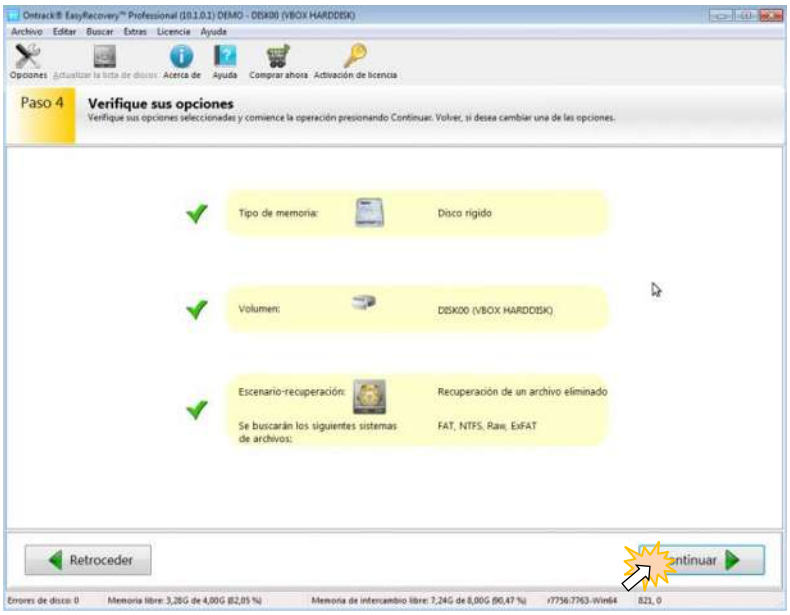
En el próximo paso vamos a seleccionar el dispositivo de dónde vamos a recuperar los archivos.



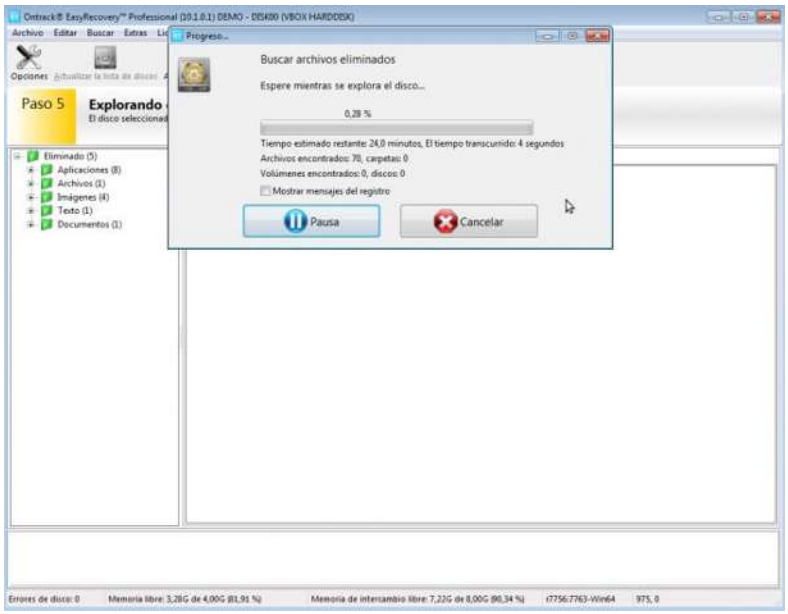
A continuación, elegiremos el tipo de recuperación. Podemos elegir si queremos recuperar archivos recién eliminados, archivos eliminados por un formateo, buscar particiones o mostrar un diagnóstico del estado del disco.



Antes de empezar nos mostrará un resumen de las acciones a realizar según lo que hayamos seleccionado.

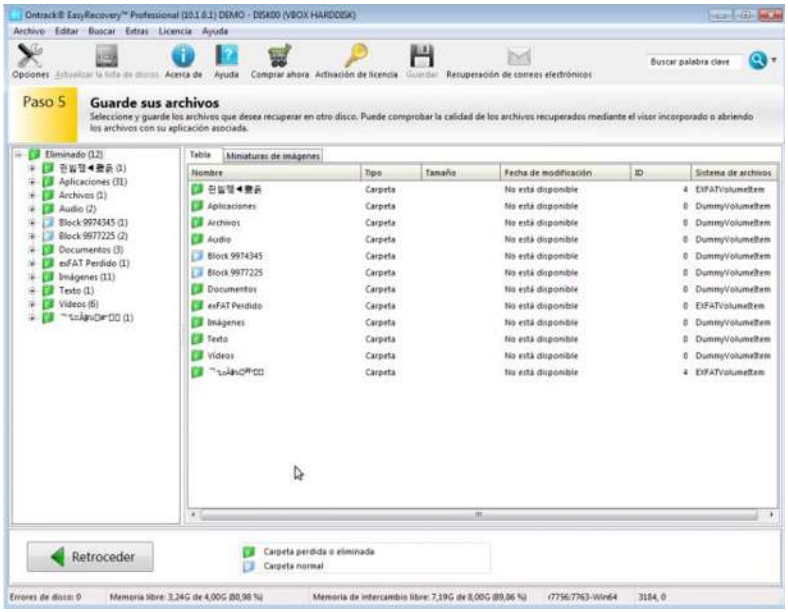


Al pulsar sobre continuar comenzará la búsqueda de archivos. La búsqueda que realiza es



profunda por lo que le llevará su tiempo. Paciencia.

Una vez finalizada la búsqueda de archivos nos aparecerán en la aplicación ordenados por tipos (imágenes, documentos, audio, vídeo etc.)



Desde aquí podemos buscar el archivo que queremos recuperar según su tipo y extensión.

Seleccionaremos el archivo que vamos a recuperar y pulsamos el botón «guardar» de la parte superior. Seleccionamos el directorio donde los guardaremos y ya tendremos nuestro archivo recuperado, sin más dificultad.

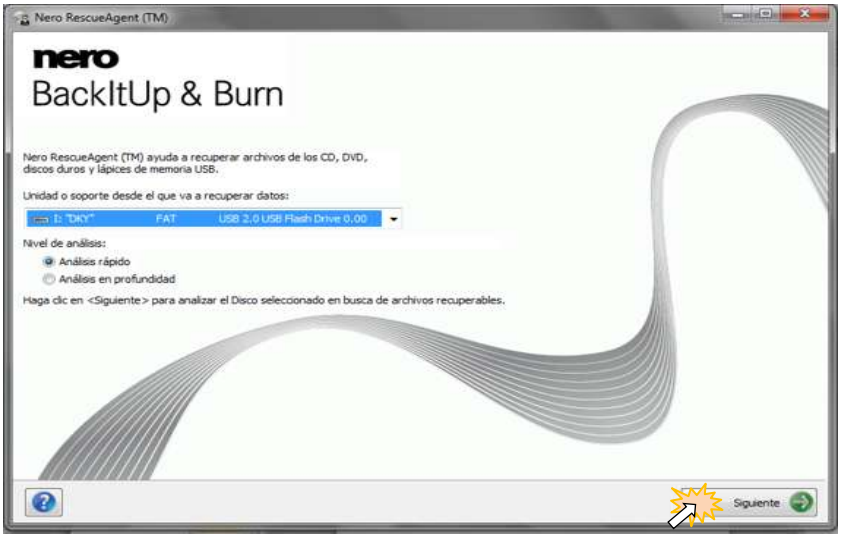
Archivo recuperado !!!!

Nero RescueAgent

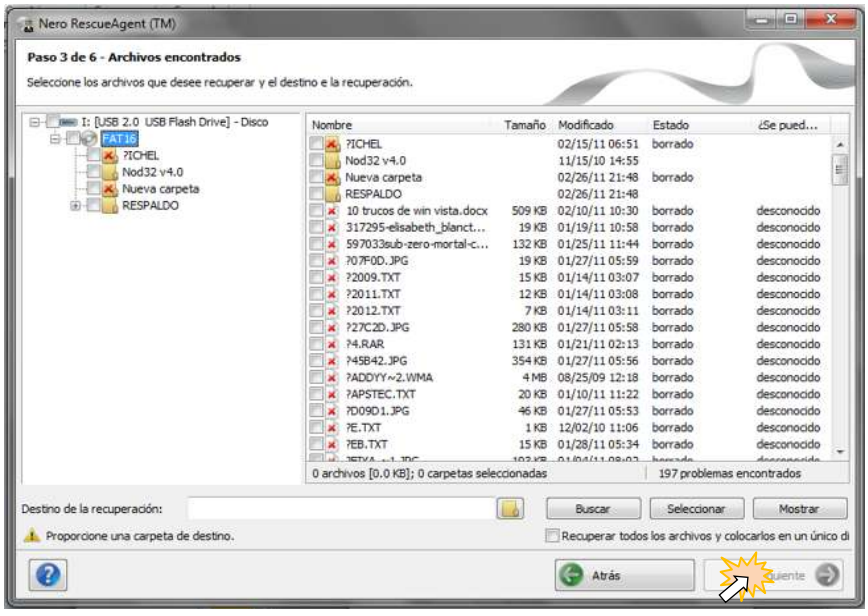
Es un software de pago, desarrollado por Nero AG, para Microsoft Windows y GNU/Linux, fue lanzado en el año 1997, pero la versión más estable fue hasta el 4 de marzo de 2013. puede recuperar de forma rápida y sencilla archivos del soporte de almacenamiento que, por ejemplo, se hayan rayado o no se puedan leer correctamente debido al envejecimiento. Los siguientes soportes de almacenamiento son compatibles con Nero RescueAgent.

Para los discos de varias sesiones y discos con formato para el sistema de archivos UDF capaces de grabar paquetes, Nero RescueAgent también ofrece la opción de recuperar archivos borrados y versiones de archivos antiguos.

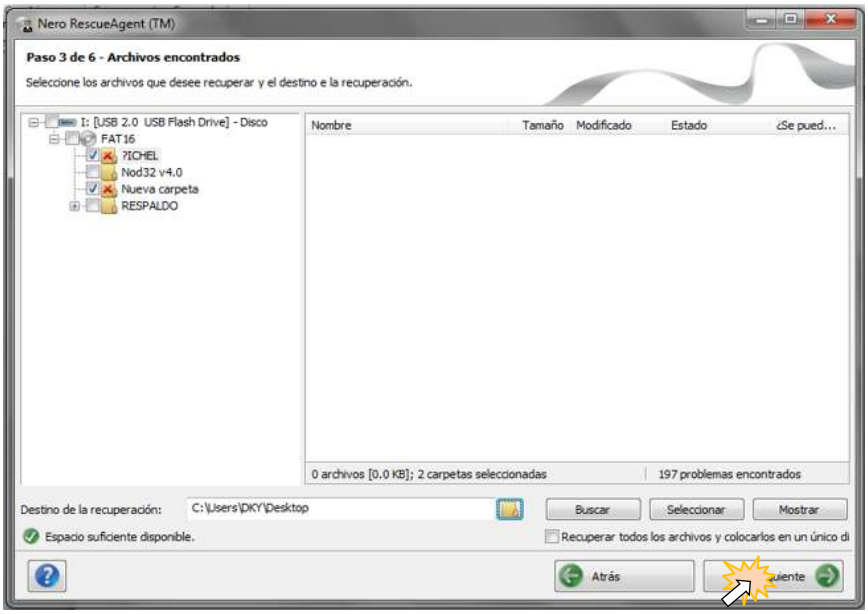
Abrimos el programa Nero RescueAgent.



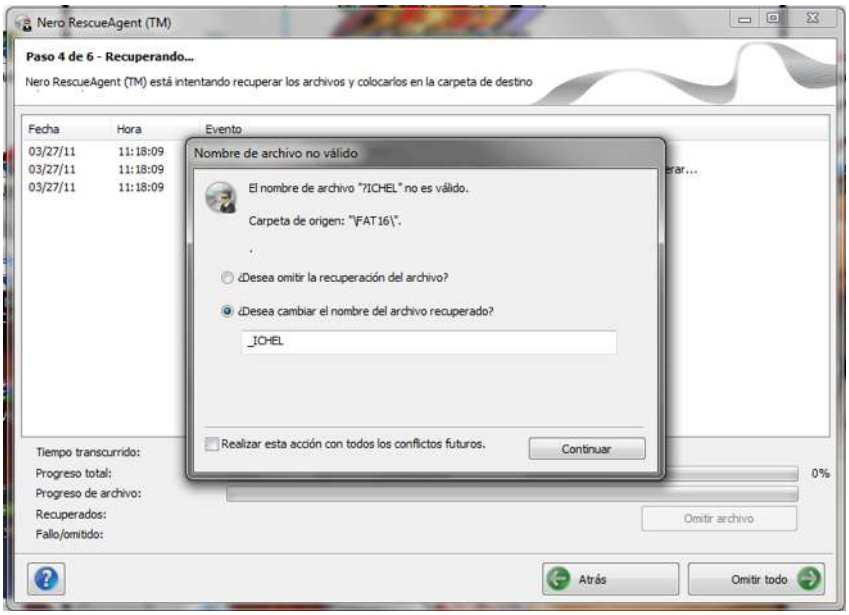
En la pantalla de inicio de Nero RescueAgent, puede seleccionar el medio de almacenamiento del que desea restaurar los datos. Además, puede elegir entre un análisis rápido o en profundidad.



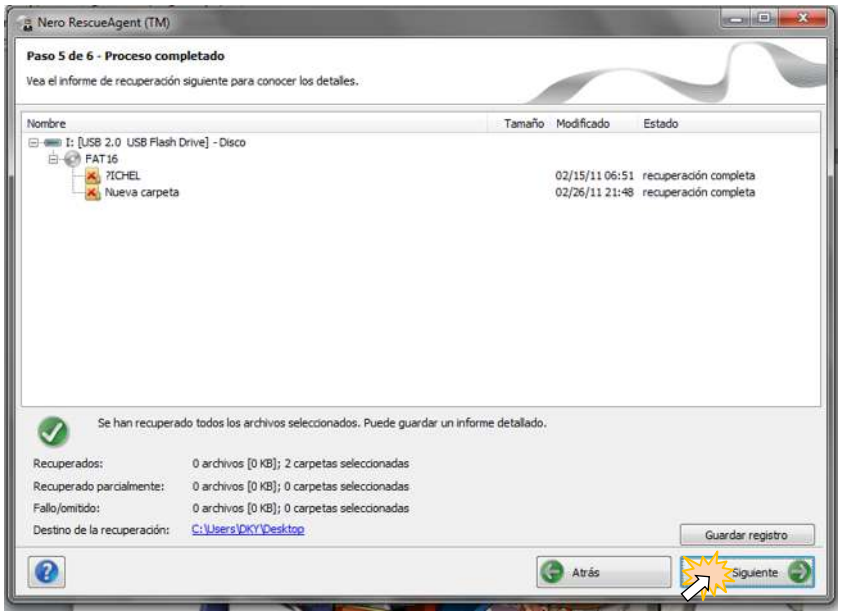
La pantalla Archivos encontrados, muestra todos los archivos que se pueden restaurar. Si los archivos solo pueden recuperarse en parte, se marcan en amarillo. Si existe tan solo una mínima posibilidad de que los archivos se puedan restaurar, se marcan en rojo.



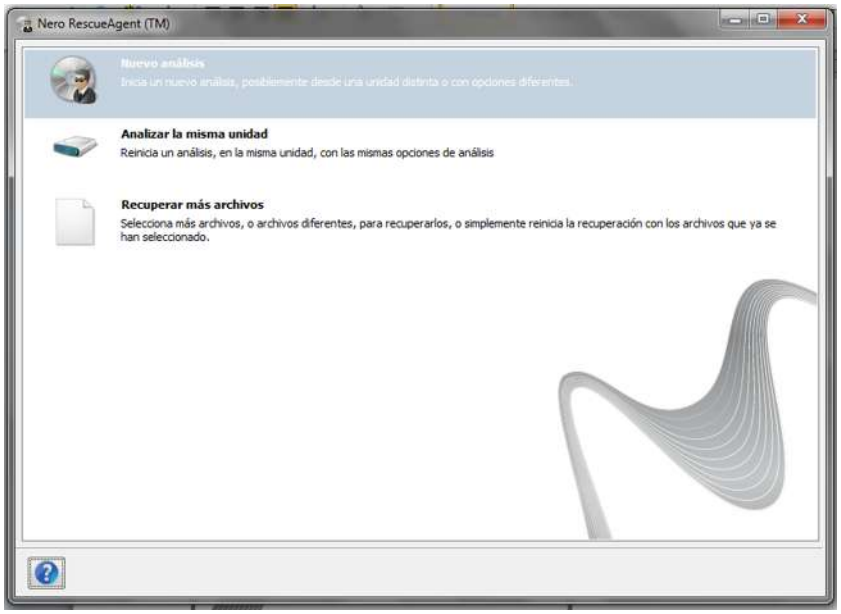
La pantalla Archivos encontrados, con los archivos o carpetas seleccionadas para la recuperacion,



En la pantalla Recuperando, nos muestra el avance dela recuperación de datos y en el caso de haya algún problema con un archivo, nos permite decidir si se cambia el nombre u omitimos la recuperación del mismo.



Todos los archivos recuperados aparecen en la pantalla Proceso completo. La pantalla también indica el número de archivos que no se pudieron recuperar. Puede guardar un archivo de registro como resumen de la recuperación realizada.



En la pantalla final puede iniciar un nuevo análisis, analizar el mismo soporte de almacenamiento de nuevo o restaurar más archivos.

CONCLUSIONES Y RECOMENDACIONES

En la actualidad el valor de la información está en aumento, con ello debemos de preocuparnos más por protegerla. La informática forense nace a raíz de esta preocupación, buscando tanto la prevención como la reacción y corrección a problemas que puedan afectar los sistemas de información.

Para la buena aplicación preventiva de la informática forense es necesaria la realización de auditorías continuas en los sistemas, y la corrección de los errores encontrados en los mismos.

También se necesita establecer políticas de seguridad para usuarios y para el uso de los sistemas de información, con el fin de minimizar la posibilidad de infiltraciones por alguna negligencia por parte de los usuarios o alguna falla en los procedimientos. Ya que las aplicaciones que utilice para hacer las pruebas solo recuperaron entre el 80 y 90%, dependiendo de las condiciones de los dispositivos de almacenamiento.

Por otro lado, en cuanto a la parte reactiva de la informática forense se necesita el uso de programas para la detección de la intrusión en el sistema de información y los cambios realizados a la información (manipulación o borrado). Así como un equipo multidisciplinario para poder cubrir de manera efectiva las áreas que traspasadas durante el ataque y poder rastrear los daños y al atacante.

Para que todo lo realizado en la informática forense sea exitoso, es necesario que se tengan regulaciones jurídicas que penalicen a los atacantes y que pueda sentenciárseles por los crímenes cometidos. Cada país necesita reconocer el valor de la información de sus habitantes y poder protegerlos mediante leyes. De manera que todos los crímenes informáticos no queden impunes.

Una investigación de este tipo nos hace capaces de acercarnos a problemas reales de las empresas y al mismo tiempo cooperar para solucionarlos.

En el presente trabajo se establecieron los métodos necesarios para la solución de uno de los problemas que más frecuentemente se presentan en empresas tanto públicas como privadas.

Durante la realización de esta investigación descubrí la importancia que tiene la informática forense, en la recuperación de información, así como también todo el método que influye para lograr este objetivo, también pude comprobar todos los beneficios que trae consigo este método. Por tanto, fue muy importante, para mi desarrollo tanto personal como personalmente, ya que me permitió conocer este tema que es de gran importancia para mi carrera.

En todas las épocas del año se dan circunstancias climatológicas que pueden provocar los discos duros se estropeen y no se pueda acceder a los datos.
A continuación, se ofrecen una serie de consejos para evitar una pérdida de datos:

En algunos casos esto suele ser debido a los contrastes de temperaturas o lo que los especialistas en recuperación de datos llamamos “descompensación térmica”, que provoca desajustes en las piezas internas del disco duro impidiendo el acceso a la información.
Además, las tormentas eléctricas tan habituales y la inestabilidad del suministro provocan subidas, bajadas o picos de tensión, cortocircuitos, apagones, etc. provocando fallos electrónicos en los discos duros.

A continuación, se ofrecen una serie de consejos para evitar que tanto los contrastes de temperaturas como las incidencias eléctricas conlleven una pérdida de datos:

FRENTE A LOS CONTRASTES DE TEMPERATURAS:

- ✓ Mantener la zona del ordenador a temperatura estable.
- ✓ Colocar un ventilador en el frontal de la caja del ordenador para que meta aire y otro en la trasera para que saque el aire interior.
- ✓ No tener el ordenador en sitios cerrados.
- ✓ Colocar los discos duros en el ordenador en alojamientos NO contiguos con espacio entre ellos para que circule el aire y el calor que desprende uno no afecte al otro.

FRENTE A LAS INCIDENCIAS ELÉCTRICAS:

- ✓ Instalar un SAI (Sistema de Alimentación Ininterrumpida) capaz de mantener funcionando su ordenador generando energía instantáneamente ante cualquier apagón.
- ✓ Instalar regletas protectoras de tensión que le ofrecerán protección frente a picos de tensión, evitarán que se quemen sus equipos, y el envejecimiento progresivo (por fatiga y sobrecalentamiento) de sus componentes integrados, entre ellos el disco duro.

En ambos casos: realizar Copias de Seguridad periódicas, bien sea mediante backup online o copias locales.
Si todo falla, ante una Pérdida de Datos:
- No pierda la calma, no se precipite.
- No reinstale el Sistema Operativo ni introduzca más datos.
- No utilice software de recuperación de datos.
- Apague el sistema (sin reiniciar) y desconecte el dispositivo ante cualquier síntoma de avería.
- No abra nunca el disco duro.
- Contacte con especialistas en recuperación de datos.

MEDIDAS PARA AUMENTAR LA POSIBILIDAD DE LA RECUPERACIÓN DE DATOS

- No guardar los archivos en el directorio raíz.
- Desfragmentar regularmente las unidades.
- No guardar archivos importantes en unidades chicas.
- Desfragmentar el disquete luego de utilizarlo.
- No utilizar la unidad que va ser recuperado para nada para no estropear el proceso de recovery.
- Es preferible tener el Disco duro con más particiones, dejando uno exclusivamente para el uso del sistema y el resto para otras.

PROTECCIÓN CONTRA VIRUS, GUSANOS Y TROYANOS

Aunque los virus, los gusanos y los troyanos tienen características muy distintas, existen tres formas principales para protegerse de todos ellos.

- **Paso 1:** nunca abra un archivo adjunto de correo electrónico de un desconocido.
- **Paso 2:** nunca abra un archivo adjunto de correo electrónico de alguien que conozca a menos que sepa exactamente qué es el archivo adjunto.
- **Paso 3:** mantenga siempre el software antivirus actualizado.
- **Paso 4:** mantenga el software de Microsoft actualizado con estos recursos en línea.

A continuación, se ofrecen 10 sugerencias rápidas para mantener un entorno informático seguro con software habitual en el lugar de trabajo:

1. Asegúrese de que cuenta con las actualizaciones más recientes. Instale actualizaciones y revisiones de seguridad en todos los servidores, equipos de sobremesa y portátiles.

* Para obtener las últimas actualizaciones de su sistema operativo Windows, software y hardware, vaya a Windows Update. Este recurso explora el equipo para determinar qué actualizaciones se necesitan; luego permite descargarlas todas o sólo las que se desee.

* Para mejorar el nivel de seguridad y estabilidad del software de Microsoft Office, vaya a Office Update y siga el vínculo de búsqueda de actualizaciones.

2. Reduzca el riesgo de virus. Hay muchas cosas que se pueden hacer para proteger el equipo y la red frente a los virus. Lo primero es utilizar software antivirus y mantenerlo actualizado; pero tiene la posibilidad de hacer más:

* Utilice la configuración de seguridad predeterminada de Office 2003, que es la versión más segura de Office publicada hasta la fecha.

* Visite el sitio Office Update para obtener las últimas actualizaciones y revisiones

* No abra nunca mensajes de correo electrónico ni archivos adjuntos que le parezcan sospechosos; aproveche el filtro de correo no deseado para enviar los mensajes sospechosos directamente a la carpeta de correo electrónico no deseado.

3. Use el Centro de seguridad de Windows para administrar las configuraciones. La vista unificada que le proporciona el Centro de seguridad de Windows le ofrece una perspectiva clara de la configuración de seguridad de su PC. Ajuste la configuración según sea necesario para establecer el nivel de seguridad deseado. La configuración de protección del PC se aplica automáticamente a los archivos y al contenido procedente de Internet, lo que contribuye a salvaguardar datos confidenciales de la empresa.

4. Cifre la información delicada del equipo portátil. Si en los viajes utiliza un portátil con Windows 2000 Professional o Windows XP Professional, protéjalo para prevenir el robo de datos. Utilice el Sistema de archivos cifrados (EFS) para cifrar carpetas y archivos confidenciales. En caso de robo del portátil, los archivos y las carpetas estarán protegidos, porque sólo será posible el acceso a los mismos con una clave especial de descifrado.

5. Descargue únicamente archivos de Internet de fuentes en las que confíe. Si tiene dudas acerca de si los archivos que desea descargar son seguros, considere la posibilidad de transferirlos primero a un soporte distinto de la unidad de disco duro; por ejemplo, un

disquete o un CD. Después puede explorar los archivos con un programa de detección de virus.

6. Utilice cifrado de contraseñas para proteger los archivos de Office. La tecnología de cifrado mejorada ha reforzado la seguridad de las contraseñas en Word 2003 y Excel 2003 y amplía el cifrado de contraseñas a PowerPoint 2003. Busque en el menú Herramientas de cada uno de estos tres programas para activar la protección con contraseñas. Constituye un medio eficaz para restringir el acceso a información confidencial de la empresa.

7. Limpie el disco duro antes de deshacerse de un PC. Si cambia de equipo de sobremesa o portátil y el antiguo se va a desechar, asegúrese de eliminar antes todos los datos personales o confidenciales de la empresa antes de que se lo lleven. Eso no significa limitarse a eliminar los archivos y vaciar la Papelera de reciclaje. Deberá volver a formatear el disco duro o adquirir software que elimine los datos definitivamente.

8. Utilice un servidor de seguridad. Si la empresa utiliza una banda ancha para una conexión ininterrumpida a Internet, instale un servidor de seguridad como línea básica de defensa frente a intrusos. Hay dos tipos básicos: 1) un servidor de seguridad de software como el Servidor de seguridad de conexión a Internet de Microsoft que se incluye en Windows XP Professional protege el equipo en el que se ejecuta; 2) un servidor de seguridad de hardware que bloquea todo el tráfico entre Internet y la red, excepto el de remitentes en los que se confía específicamente.

9. No navegue nunca por Internet desde un servidor. Por su calidad de centro de control de la red de la empresa, en un servidor suele almacenarse información crítica para el negocio. Si se pone en peligro la seguridad del servidor, también lo estarán la de los datos y la red.

10. Sea avispado con respecto a las contraseñas. Utilice siempre contraseñas seguras de al menos ocho caracteres, compuestas de mayúsculas y minúsculas, números y símbolos. No utilice de forma reiterada la misma contraseña y acostúmbrese a cambiar las contraseñas con frecuencia. Si tiene dificultades para recordar las contraseñas, considere la posibilidad de utilizar una frase clave o de paso; Windows 2000 y Windows XP ofrecen esa posibilidad. Una frase de paso podría ser "El martes comí pizza".

BIBLIOGRAFÍA

LIBROS

Autor: Jeimy J. Cano M.
Julio 2009, COMPUTACION FORENSE, Descubriendo los rastros.
Editorial Omega.
Pág. 344
Primera Edición.

Autor: Julio Téllez Valdés.
2008, Derecho Informático.
Editorial McGraw Hill.
Pág. 344
Cuarta Edición.

Autor: Federico G. Pacheco.
2009, Hackers al descubierto.
Manual Users.
Pág. 352.
Primera Edición.

ENLACES WEB

Microsoft, (2016). Entorno Seguro. Recuperado de http://www.microsoft.com/business/smb/es/temas/recursos_tecnicos/entornoseguro.mspx

UNAM-CERT(18/01/2018). ¿Qué es el phishing?. Recuperado de https://www.cert.org.mx/que-es-el-phishing-2

UNAM (2017). Vulnerabilidades. Recuperado de http://www.seguridad.unam.mx/vulnerabilidadesDB

Alerta Antivirus (2016). Busca vulnerabilidades. Recuperado de http://www.alerta-antivirus.es/seguridad/busca_vulns.php

UNAM CERT (2018). Boletines de seguridad. Recuperado de http://www.cert.org.mx/boletin/

VNUNET (2016). Sistemas de protección. Recuperado de http://www.vnunet.es/Seguridad/Sistemas_de_protecci%C3%B3n

Cristian Borghello, (2013). Ciberseguridad Nacional Argentina. Recuperado de https://www.segu-info.com.ar/boletin/boletin-194-130915.htm

(IN)SECURE Magazine (2006). Computer forensics vs. electronic evidence. Recuperado de https://www.helpnetsecurity.com/insecuremag/issue-8-september-2006/

BORRMART (2003). Revista Red Seguridad. Recuperado de http://www.borrmart.es

RNP CAIS (2017). Seguridad. Recuperado de http://www.rnp.br/cais

Robert A (2209). Metasploit Decloaking Engine obtiene el IP real del usuario. Recuperado de http://www.cgisecurity.com

Cgisecurity.com (2002). Anatomy of the Web Application Worm. Recuperado de www.cgisecurity.com/articles/worms.shtml

Ausejo Prieto, Rafael (2004). Análisis forense. Recuperado de http://www.ausejo.net/seguridad/forense.htm.

Raymondorta (2008). Delitos Informáticos Programa Acceso Máximo. Recuperado de https://www.youtube.com/watch?v=vqu5vR7_Od0

Forensics Wiki (2017). Forensics Wiki. Recuperado de http://www.forensicswiki.org/

López Oscar y Amaya Haver y León Ricardo (2002). Informática forense: Generalidades, aspectos técnicos y herramientas. Recuperado de http://www.criptored.upm.es/guiateoria/gt_m180b.htm

Pérez Gómez Elena (2008). ¿Qué es la informática forense o Forensic? https://seguinfo.wordpress.com/2008/06/09/%C2%BFque-es-la-informatica-forense-o-forensic/

Dan Farmer and Wietse Venema (1999). The Coroner's Toolkit. Recuperado de http://www.porcupine.org/foren-sics/tct.html